Design principles for creating digital transparency in government

Ricardo Matheus a, b, *, Marijn Janssen a, Tomasz Janowski b, c

a Delft University of Technology, the Netherlands
b Gdańsk University of Technology, Poland
c Danube University Krems, Austria

1. Introduction

Lack of transparency in government operations and decision-making processes is often connected to corruption scandals (Harrison & Sayogo, 2014), poor decision-making (Guillamón, Ríos, Guesuè, & Metallo, 2016), lack of accountability of public officials (Lourengo, 2015), and dysfunctional governance of government organizations (Kosack, 2016). Transparency is often viewed as one of the critical conditions for good governance and an essential mechanism for balancing power between the government and the public (Janssen & van den Hoven, 2015). Transparency increases the chances that wrongdoings are detected, abuses of power uncovered, and activities scrutinized.

Although easy to grasp intuitively, transparency is hard to define and even harder to realize. Various definitions and conceptualizations of transparency emphasize different aspects and formulate different expectations towards this concept. The latter include improved accountability (Peixoto, 2013), good governance (Ward, 2014), better decision-making (Navarro-Galera, Alcaraz-Quiles, & Ortiz-Rodríguez, 2016), less corruption (John C Bertot, Jaeger, & Grimes, 2010), and more openness (Frank & Oztoprak, 2015; Matheus & Janssen, 2015). At the same time, an argument is also advanced that the expectations towards digital transparency is opening government data to the public (Luna-Reyes, Bertot, & Melloul, 2014) through portals, dedicated apps or Application Programming Interfaces (APIs). An open data portal makes raw datasets available for human or machine use. An app provides an interface for exploring, analyzing, and visualizing data in this way, enabling the performance of tightly controlled operations on such data. Big data, data analytics, artificial intelligence (AI), and other data-driven algorithms that process and analyze available data and visualize the outcomes are behind such possibilities.

* Corresponding author.
E-mail address: R.Matheus@tudelft.nl (R. Matheus).
Jaffalaan 5, 2628 BX Delft, South Holland, The Netherlands.

Received 19 November 2020; Received in revised form 21 November 2020; Accepted 21 November 2020
Available online 9 December 2020
https://doi.org/10.1016/j.giq.2020.101550
Despite its merits and the availability of relevant digital tools, full transparency is difficult to achieve (Fung, 2013), and the practical realization of digital transparency is challenging. First, opening government data alone is insufficient (Janssen, Charalabidis, & Zuiderwijk, 2012) as many socio-technical barriers prevent the creation of digital transparency from such data (Conradi & Choenni, 2014). Second, while data can be opened and shared, it could create limited insights into government operations; more data might not automatically lead to more transparency. Third, as those in control commonly lead transparency initiatives, they base their decisions on available data but often fail to consider public needs (Janssen et al., 2012). Fourth, presenting selected and aggregated data, open government data portals might embed their designers’ viewpoints (Kitchin, Lauriault, & McArdle, 2015) while suppressing the diversity of views held by different groups in a pluralistic society. Hence, such data might be unsuitable for creating accountability and combating fraud and corruption. Fifth, despite the many tools available to open up aspects of government operations and organization, these tools have their limitations and there is no guidance on how to use them to consistently achieve the desired level of digital transparency across government structures and operations.

Given the challenges above, this article aims to provide guidance for creating digital transparency in government. This guidance is offered through a set of design principles for digital transparency. The principles are intended to overcome the various barriers hindering digital transparency and create a window for the public to view the internal functioning of government. The principles make part of a window theory (Matheus & Janssen, 2020), with many factors relevant to digital transparency and multiple windows offered to realize such transparency. According to Matheus and Janssen (2020, p. 3), such a window is required “to view government functioning, aimed at overcoming the information asymmetry between the government and the public”. The window metaphor captures different influences on who, how, and what we can inspect about government – users, conditions of use, data and system characteristics, etc. The metaphor also captures the fact that transparency goals should inform window design, but that no single window can deliver full transparency by itself.

The rest of this article is structured as follows. Section 2 presents the research approach. Section 3 identifies barriers to digital transparency, followed by design principles and how they help overcome the barriers in Section 4. Section 5 evaluates the principles using three case studies. A discussion of the principles and their use is carried out in Section 6. Finally, Section 7 provides some conclusions.

2. Design research approach

As our goal is to arrive at a set of design principles for digital transparency, we followed the Design Science Research approach (Chanson, Bogner, Bilgeri, Fleisch, & Wortmann, 2019). The approach is outlined in Section 2.1. Section 2.2 presents the Systematic Literature Review method, which is used to derive design principles, followed by the Case Study approach in Section 2.3, which is used to evaluate the design principles in different practical scenarios.

2.1. Design science research approach

According to Chanson, Bogner, Bilgeri, Fleisch, and Wortmann (2019, p. 1277), the focus of the design science is “on the creation of the artificial and accordingly the rigorous construction and evaluation of innovative artefacts”. Using the design science research methodology by Peffers, Tuunanen, Rothenberger, and Chatterjee (2007, p. 48), Chanson et al. (2019) created a design cycle to build design principles. The latter “instantiated by an explicit design feature can be understood as an explanation (design principle) of why a specified piece (design feature) leads to a predefined goal (design requirement)” (ibid. p. 1279). Chanson et al. (2019) aimed at deriving design principles for a sensor data protection system.

In contrast, the artefacts in our research are digital systems used by government organizations. By following the design principles for digital transparency, a window on government decisions and operations can be created. This set of coherent and generalizable design principles for digital transparency comprises our design theory, which assumes and supplements the window theory (Matheus & Janssen, 2020).

Whereas most design approaches take an inductive approach to derive general laws from particular instances, we opted for a deductive approach to derive specific instances from general laws. In particular, rather than analyzing concrete government systems to uncover barriers to digital transparency and develop design principles to overcome such barriers, we opted to discover such barriers and principles through literature. This decision was motivated by the many barriers and principles available in literature and their potential for generalizability. For the barriers and principles derived from working systems, achieving such generalizability is difficult. Furthermore, we opted to evaluate the principles using three case studies conducted in different countries and policy areas. The diversity of case studies aims to justify that the proposed design principles can be used to ensure digital transparency for various government organizations and their digital systems.

The research process, depicted in Fig. 1, consists of five steps. In Step 1, a Systematic Literature Review (SLR) was conducted to uncover barriers to digital transparency in government organizations. A similar SLR was carried out in Step 2 to identify a set of design principles for overcoming the barriers. The principles were mapped in Step 3 into the Data-Driven Transparency cycle to ensure consistency, facilitate usage and help confirm which principles are relevant (Matheus, Janssen, & Maheshwari, 2018, p. 8). Next, Step 4 demonstrated and tested the principles using three international case studies. Each case study concerned the development of a digital system for a government organization, aimed at making this organization more transparent. Each case study involved conducting semi-structured interviews with experts working on such systems. Finally, Step 5 discussed practical applications of the design principles for digital transparency.

2.2. Systematic literature review

According to Fink (2019, p. 6), a Systematic Literature Review is a “systematic, explicit, and reproducible method for identifying, evaluating, and synthesizing the existing body of completed and recorded work produced by researchers, scholars and practitioners”. Fink (2019, p. 6) also recommends conducting SLR through the seven following steps: 1) determine the research question, 2) identify literature sources, 3) define keywords and other search terms, 4) use explicit screening criteria to include or exclude papers, e.g., the papers that are written in specific language or published in particular years, 5) apply the screening criteria methodologically, here to identify the barriers and design principles to build digital systems for transparent government, 6) prepare reliable reviews of all selected articles using standardized forms to ensure consistency and replication, and 7) synthesize the result into the lists of barriers and design principles.

The SLR for the first step of this research was conducted using the search term: (“big data” OR “open data”) AND “barriers” AND “transparency”. In four scientific databases – Scopus, JSTOR, SpringerLink and Web of Science – serving as the literature sources. As the inclusion criterion, we limited the search to the top 25 journals in the fields of Public Administration (PA) and Information Systems (IS) with an average impact factor above 1.0 based on the Scientific Journal Rank (SJR - Scimago/Scopus) calculated in 2016. We also limited the publication years to the period between 2007 and 2018.

The result of the SLR, which was conducted between 1 April and 31 May 2019, is a list of 50 relevant articles that helped uncover 364 barriers to digital transparency. The articles are listed in Table A.1, and the barriers in Tables B.1 and C.1, the latter after categorizing them into political, economic, human and social, and technological areas. All three
Table 1 and described as follows:

- **Data quality** barriers include inaccessible or inaccurate data, information sharing or re-identification from combined data sets causing privacy violations, lack of unified ontologies and language misconceptions causing data misinterpretation, lack of centralized databases causing data quality issues, and difficulties of integrating data from heterogeneous sources.
- **Economic** barriers include high costs of maintaining big data infrastructures and tools for big data analysis, lack of reliable Return-on-Investment (ROI) studies, unreliable architecture plans leading to unpredictable cost increases, and limited organizational budgets.
- **Ethical** barriers deal with data bias and the resulting discriminatory decisions by data-driven algorithms as well as privacy issues related to uncovering human habits through mass surveillance, among others.
- **Human** barriers include lack of workforce able to handle big data and related projects, low quality of decision-makers and decision-making using big data analytics, and lack of data-driven and evidence-based work culture.
- **Organizational** barriers include lack of information sharing plans, unclear ownership of data, data quality issues causing mistakes or allowing misconduct by personnel, unavailable data, lack of information sharing policies causing information asymmetry, the opacity of algorithms and the inability to inspect them, and lack of awareness about the benefits of big data.
- **Political and legal** barriers include lack of privacy policies, mass surveillance causing lack of data protection, and lack of stable regulatory frameworks creating legal issues.
- **Technical** barriers include the need to process vast volumes of data; data volumes causing user overload; lack of methods for managing big data systems; difficult integration between big data and legacy technologies; untimely data delivery; underperformance of big data systems caused by bandwidth limitations and the lack of architecture plans; security breaches caused by the leakage or hacking of data; security risks caused by the unavailability of logs to carry out forensic analysis; data silos lowering data quality; problems with data accessibility; and lack of user-friendly big data tools.
- **Usage** barriers include difficulties in adapting visualizations to different audiences, and users’ information overload causing data quality issues.

### 4. Design principles for digital transparency

In this section, we propose a set of design principles that can help government organizations design and adopt digital systems through which they can become more transparent. Specifically, the principles are intended to overcome data quality, organization, and usage barriers, as these categories are central to building digital transparency portals and opening data for digital transparency. Although relevant, we excluded economic, ethical, human, political and legal, and technical barriers as these are not directly related to the organization and creation of digital transparency.

The rest of this section is structured as follows. Section 4.1...
formulates 16 design principles for digital transparency based on the Systematic Literature Review. Section 4.2 relates the 16 principles identified in Section 4.1 to the 42 barriers identified in Section 3. The resulting many-to-many mapping describes which principles help to overcome which barriers. Finally, Section 4.3 maps the design principles to different phases of the data-driven transparency cycle (Matheus et al., 2018; Matheus & Janssen, 2018), thus operationalizing the use of the principles in the engineering for data-driven transparency.

4.1. Deriving design principles

Richardson, Jackson, and Dickson (1990, p. 388) described design principles as “beliefs upon which the enterprise is created and the bases of its decisions”. Bharosa, van Wijk, Janssen, de Winne, and Hulstijn (2011, p. 1) defined design principles as a means “to guide stakeholders in proactively dealing with some of the transformation issues” that organizations might encounter.

The Open Group Architecture Framework (TOGAF) (2009, p. 1) prescribed that such principles should be easy to understand, complete, consistent, stable, and enduring. To support sound decision-making, they should also be robust and precise. According to the TOGAF template – a standard way of defining design principles, each principle should have a name, statement, rationale and implications. The inclusion of the rationale and implications promotes the understanding and acceptance of the design principles throughout the organization (TOGAF, 2009).

The design principles derived in this section aim at creating digital transparency. They are intended to help organizations make the right decisions when realizing digital transparency. As such, they should be generalizable to different situations in which such decisions have to be made. The principles are described using the TOGAF template in Table C.1 and summarized in Table 2 below.

4.2. Relating principles to barriers

The design principles for digital transparency, as described in Table 2, should help overcome the barriers to digital transparency, as described in Table 1. The matrix describing which principles address which barriers is presented in Table 3. According to this Table 3, most principles help overcome several barriers, and most barriers are addressed using multiple principles, which demonstrates the complexity involved with organizing and designing for digital transparency. Ignoring some design principles might limit our capacity to address specific barriers, thus lowering the level of digital transparency overall.

**Table 1**

<table>
<thead>
<tr>
<th>Category</th>
<th>Code</th>
<th>Barrier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Quality</td>
<td>DQ1</td>
<td>Privacy issues due to information sharing risks</td>
</tr>
<tr>
<td></td>
<td>DQ2</td>
<td>Data quality issues due to the lack of unified area ontologies</td>
</tr>
<tr>
<td></td>
<td>DQ3</td>
<td>Data quality issue due to heterogeneous (structured vs unstructured) data sources</td>
</tr>
<tr>
<td></td>
<td>DQ4</td>
<td>Data quality issue due to the lack of data accuracy</td>
</tr>
<tr>
<td></td>
<td>DQ5</td>
<td>Privacy issue due to re-identification caused by combining data sets</td>
</tr>
<tr>
<td></td>
<td>DQ6</td>
<td>Data quality issue due to the lack of centralized databases</td>
</tr>
<tr>
<td></td>
<td>DQ7</td>
<td>Data quality issue due to language misconceptions, e.g. usage and jargon</td>
</tr>
<tr>
<td>Economic</td>
<td>EC1</td>
<td>The high cost of creating and maintaining big data analysis infrastructures</td>
</tr>
<tr>
<td></td>
<td>EC2</td>
<td>Financial issues due to the lack of reliable Return-on-Investment (ROI) studies</td>
</tr>
<tr>
<td></td>
<td>EC3</td>
<td>Lack of low-cost analytical tools to carry out big data analysis</td>
</tr>
<tr>
<td></td>
<td>EC4</td>
<td>Lack of big data system architecture plans leading to unpredictable cost increases</td>
</tr>
<tr>
<td></td>
<td>EC5</td>
<td>Financial issues due to limited organizational budgets</td>
</tr>
<tr>
<td>Ethical</td>
<td>ET1</td>
<td>Prejudicial use of algorithms, e.g. discrimination based on ethnicity</td>
</tr>
<tr>
<td>Human</td>
<td>HT1</td>
<td>Lack of skilled workforce able to handle big data</td>
</tr>
<tr>
<td></td>
<td>HT2</td>
<td>Low quality of decision-makers and decision-making</td>
</tr>
<tr>
<td></td>
<td>HT3</td>
<td>Lack of data-driven and evidence-based culture</td>
</tr>
<tr>
<td></td>
<td>HT4</td>
<td>Lack of skilled workforce to lead big data projects</td>
</tr>
<tr>
<td>Organizational</td>
<td>OR1</td>
<td>Lack of information sharing plans</td>
</tr>
<tr>
<td></td>
<td>OR2</td>
<td>Data quality issue due to unclear ownership</td>
</tr>
<tr>
<td></td>
<td>OR3</td>
<td>Data quality issue leading to mistakes or allowing misconduct by personnel</td>
</tr>
<tr>
<td></td>
<td>OR4</td>
<td>Lack of or limited availability of data</td>
</tr>
<tr>
<td></td>
<td>OR5</td>
<td>Asymmetry of information due to the lack of information sharing policies</td>
</tr>
<tr>
<td></td>
<td>OR6</td>
<td>Lack of openness and constraints on inspecting algorithms</td>
</tr>
<tr>
<td></td>
<td>OR7</td>
<td>Organizational issues due to the lack of awareness about the benefits of data</td>
</tr>
<tr>
<td>Political and</td>
<td>PL1</td>
<td>Privacy issues caused by the lack of explicit privacy policies</td>
</tr>
<tr>
<td>Legal</td>
<td>PL2</td>
<td>Data protection issues caused by mass surveillance</td>
</tr>
<tr>
<td></td>
<td>PL3</td>
<td>Legal issues due to the lack of stable regulatory frameworks</td>
</tr>
<tr>
<td>Technical</td>
<td>TE1</td>
<td>Difficulties in processing vast volumes of data</td>
</tr>
<tr>
<td></td>
<td>TE2</td>
<td>The complexity of the integration between big data and legacy technologies</td>
</tr>
<tr>
<td></td>
<td>TE3</td>
<td>Lack of appropriate methods to deal with modern big data systems</td>
</tr>
<tr>
<td></td>
<td>TE4</td>
<td>Technical issue due to the volumes of big data, causing users’ data overload</td>
</tr>
<tr>
<td></td>
<td>TE5</td>
<td>Data quality issues due to the lack of timeliness in data delivery</td>
</tr>
<tr>
<td></td>
<td>TE6</td>
<td>Underperformance due to the lack of big data system architecture plans</td>
</tr>
<tr>
<td></td>
<td>TE7</td>
<td>Performance issues caused by bandwidth limitations</td>
</tr>
<tr>
<td></td>
<td>TE8</td>
<td>Security issues caused by the risk of data leakage or hacking</td>
</tr>
<tr>
<td></td>
<td>TE9</td>
<td>Data quality issues caused by existing data silos</td>
</tr>
<tr>
<td></td>
<td>TE10</td>
<td>Lack of data accessibility</td>
</tr>
<tr>
<td></td>
<td>TE11</td>
<td>Security issues due to the unavailability of logs to carry out forensic analysis</td>
</tr>
<tr>
<td></td>
<td>TE12</td>
<td>Technical issues due to the lack of user-friendly big data tools</td>
</tr>
<tr>
<td>Usage</td>
<td>US1</td>
<td>Visualizations that are hard to adapt to different audiences</td>
</tr>
<tr>
<td></td>
<td>US2</td>
<td>Data quality issues due to the users’ information overload</td>
</tr>
</tbody>
</table>

**Table 2**

<table>
<thead>
<tr>
<th>Code</th>
<th>Name</th>
<th>Short Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1</td>
<td>Separating privacy-sensitive and -insensitive data at the source</td>
<td>Privacy</td>
</tr>
<tr>
<td>P2</td>
<td>The openness of processes and actors</td>
<td>Openness</td>
</tr>
<tr>
<td>P3</td>
<td>Feedback mechanisms for improving transparency</td>
<td>Feedback Mechanisms</td>
</tr>
<tr>
<td>P4</td>
<td>Various levels of abstraction for data access</td>
<td>Data Abstraction</td>
</tr>
<tr>
<td>P5</td>
<td>Avoid any jargon or terms that the public does not understand</td>
<td>Comprehension</td>
</tr>
<tr>
<td>P6</td>
<td>Checking and rating data quality</td>
<td>Data Quality Rating</td>
</tr>
<tr>
<td>P7</td>
<td>Visualization of different views</td>
<td>Visualization</td>
</tr>
<tr>
<td>P8</td>
<td>Data access in different protocols</td>
<td>Data Access</td>
</tr>
<tr>
<td>P9</td>
<td>Use of standardized formats</td>
<td>Standardized Formats</td>
</tr>
<tr>
<td>P10</td>
<td>Ensuring that data is not altered or its history can be traced</td>
<td>Data Persistence</td>
</tr>
<tr>
<td>P11</td>
<td>Data and system interoperability</td>
<td>Interoperability</td>
</tr>
<tr>
<td>P12</td>
<td>Include metadata for data comprehension</td>
<td>Metadata</td>
</tr>
<tr>
<td>P13</td>
<td>Transparency-by-design (automatically opening data)</td>
<td>Transparency-by-Design</td>
</tr>
<tr>
<td>P14</td>
<td>Opening of raw data</td>
<td>Opening of Raw Data</td>
</tr>
<tr>
<td>P15</td>
<td>Assigning stewards responsible for digital transparency</td>
<td>Stewardship</td>
</tr>
<tr>
<td>P16</td>
<td>Supporting views with different level of details</td>
<td>Gradation of Detail</td>
</tr>
</tbody>
</table>
## Table 3
Relationships between barriers and design principles for digital transparency.

<table>
<thead>
<tr>
<th>DQ1</th>
<th>P1</th>
<th>P2</th>
<th>P3</th>
<th>P4</th>
<th>P5</th>
<th>P6</th>
<th>P7</th>
<th>P8</th>
<th>P9</th>
<th>P10</th>
<th>P11</th>
<th>P12</th>
<th>P13</th>
<th>P14</th>
<th>P15</th>
<th>P16</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DQ2</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DQ3</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DQ4</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DQ5</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DQ6</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DQ7</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EC1</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EC2</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EC3</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EC4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EC5</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ET1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ET2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HR1</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HR2</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HR3</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HR4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OR1</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OR2</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OR3</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OR4</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OR5</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OR6</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OR7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PL1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PL2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PL3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TE1</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TE2</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TE3</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TE4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TE5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TE6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TE7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TE8</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TE9</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TE10</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TE11</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TE12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>US1</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>US2</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**Fig. 2.** Data-Driven Transparency cycle with design principles adapted from Matheus and Janssen (2018, p. 36)
4.2.1.1. Transparency cycle enabled by design principles. To operationalize the development for digital transparency and the use of the design principles as part of it, we adopted the data-driven transparency cycle (Matheus et al., 2018; Matheus & Janssen, 2018). The cycle is depicted in Fig. 2, adapted from fig. 8 “OGI Tools and Working Flow” in Matheus and Janssen (2018, p. 36). The cycle consists of six phases: eliciting data, collecting data, publishing data, using data, sharing results, and determining actions; and two parts: one on publishing data (light color, dotted outline) and another on using data (dark color, solid outline). In line with the iterative nature of development, the phases are ordered into a cycle.

During different phases of the data-driven transparency cycle, various design principles can be used. The assignment of the principles to phases, also depicted in Fig. 2 and elaborated in Table 4, helps decide which principles should be used and when. Every phase has several principles assigned to it, and each principle can be mapped to different phases.

5. Demonstrating and testing design principles

In order to demonstrate and test their usefulness, the principles were employed in three case studies of government applications that aim at digital transparency. The case studies are outlined in Table 5, including the responsible organization, application name and purpose, what kind of transparency effect is expected, and who is the target of this effect.

As part of this research, we carried out semi-structured interviews with designers involved in developing the applications, aimed at evaluating the principles. The interviews included questions belonging to different areas: the relevance of the principles; if and how the principles were used in the cases; and to which phase of the transparency cycle each principle belongs.

Although all principles were used by at least one person in charge of application development in the case studies, who all found them coherent, the survey showed that the principles were used to various extent. Table 6 summarizes the percentage of the use of different principles by the nine interviewed designers.

All designers used the Privacy (P1) and Metadata (P12) principles; some principles were used occasionally, e.g., Stewardship (P15) at 33%, Comprehension (P5) at 44% or Transparency-by-Design (P13) at 56%; and some were not used at all. Interviews revealed that the reasons for this were that the principles primarily concerned organizational changes, whereas the projects were on application development. This disparity did not make them less relevant; on the contrary, the interviewees suggested that adhering to them is needed to create digital transparency.

Stewardship (P15) refers to the ownership of and responsibility for data quality. Adhering to this principle has considerable organizational consequences and requires organizational changes. An interviewee noted that following this principle would be “major, if well done”. Although application designers could hardly use this principle, it was found to be highly relevant. Often strategic projects commence as technical software development, having no mandate to change an organization. This observation suggests that policy-makers and managers need to listen better to their developers to create digital transparency. An interviewee mentioned that it is “easy to allocate responsibilities, but organizational change might be needed”. The evaluation even suggested that it is imperative to prepare an organization for transparency before developing systems. Following this suggestion should ensure that data is collected and becomes immediately available at the right quality and in the proper format. Organizing can be viewed as a precondition for creating digital transparency.

Comprehension (P5) is about avoiding jargon or technical terms to ensure that the public can understand them. Removing jargon requires

<table>
<thead>
<tr>
<th>#</th>
<th>Phase Name</th>
<th>Description / Justification</th>
<th>Related Principle Codes and Names</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Elicit data need</td>
<td>Any data created for whatever reason and the disclosure of this data is a transparency action.</td>
<td>P1 Privacy, P2 Openness, P3 Feedback, P4 Mechanism, P5 Data Abstraction, P6 Comprehension, P7 Data Quality, P8 Rating, P9 Visualization, P10 Data Access, P11 Standardized, P12 Formats, P13 Data Persistence, P14 Interoperability, P15 Metadata, P16 Transparency-by-Design, Stewardship</td>
</tr>
<tr>
<td>B</td>
<td>Collect data</td>
<td>Data must be collected in any form, from manual and physical (e.g. surveys), to automated and digital (e.g. networked sensors).</td>
<td>P1 Privacy, P2 Openness, P3 Feedback, P4 Mechanism, P5 Data Abstraction, P6 Comprehension, P7 Data Quality, P8 Rating, P9 Visualization, P10 Data Access, P11 Standardized, P12 Formats, P13 Data Persistence, P14 Interoperability, P15 Metadata, P16 Transparency-by-Design, Stewardship</td>
</tr>
<tr>
<td>D</td>
<td>Use data</td>
<td>Transparency cannot happen if nobody uses data. After disclosure, users must use and create insights from data, as enabled by transparency.</td>
<td>P1 Privacy, P2 Openness, P3 Feedback, P4 Mechanism, P5 Data Abstraction, P6 Comprehension, P7 Data Quality, P8 Rating, P9 Visualization, P10 Data Access, P11 Standardized, P12 Formats, P13 Data Persistence, P14 Interoperability, P15 Metadata, P16 Transparency-by-Design, Stewardship</td>
</tr>
<tr>
<td>E</td>
<td>Share results</td>
<td>Transparency can happen to only one person. However, the more people use data, the more will have insights enabled by transparency.</td>
<td>P1 Privacy, P2 Openness, P3 Feedback, P4 Mechanism, P5 Data Abstraction, P6 Comprehension, P7 Data Quality, P8 Rating, P9 Visualization, P10 Data Access, P11 Standardized, P12 Formats, P13 Data Persistence, P14 Interoperability, P15 Metadata, P16 Transparency-by-Design, Stewardship</td>
</tr>
<tr>
<td>F</td>
<td>After a group of people gained meaningful insights enabled by...</td>
<td></td>
<td>P2 Openness, P3 Feedback</td>
</tr>
</tbody>
</table>

(continued on next page)
everybody to agree to use the same terms and to provide these terms with the same meaning. However, principle P5 goes beyond the use of jargon. It also covers the harmonization of data collection to ensure that the data is understood and ready to be compared.

Fig. 3 plots the 16 design principles on two orthogonal dimensions – ease of use in practice and importance for creating digital transparency. Some principles, particularly Opening of Raw Data (P14), Data Abstraction (P4), Stewardship (P15), Visualization (P7), Data Access (P8), and Feedback Mechanisms (P3) are both essential and easy to use. Thus, organizations could adopt them with little effort and achieve significant progress towards digital transparency. However, to realize stewardship is more than just allocating responsibilities on a drawing board, it has important organizational implications.

In contrast, some principles were found to be less relevant and challenging to use. This category includes Standardized Formats (P9), Transparency-by-Design (P13), Data Quality Rating (P6), Comprehension (P5), Privacy (P1) and Transparency-by-Design (P13), all located in the bottom right quadrant of Fig. 3. The interviewees judged them as less important for the projects, difficult to put into practice and requiring much effort to do so. However, for the organizations they can be essential to ensure that high quality data is automatically opened and can be easily used. Transparency-by-Design (P13), for instance, is essential to create digital transparency and for automating the opening of data, but the projects are focused on patching rather than organizing for Transparency-by-Design. As such, these principles go beyond a single project and might be important for policymakers. For example, formatting all datasets in a standardized way is vital for comparison but is expensive and time-consuming for a single project. An interviewee pointed out that the ease-of-use is dependent on how data collection and processing are organized: “if these [formats] are available then it is easy, if they are not then first a standardization process is needed”. Also, Openness (P2) might be hard to adopt. According to one interviewee: “some agents are very reluctant to be exposed” and “it is not always easy to track who has done what”. The latter influences how easy it is to apply this principle in practice.

Fig. 4 plots the design principles against two other dimensions: impact on the organization and importance for achieving digital transparency. The top right quadrant includes all high-importance and high-impact principles, particularly: Privacy (P1), Stewardship (P15), Data Quality Rating (P6), Standardized Formats (P9), Transparency-by-Design (P13), Opening of Raw Data (P14), Openness (P2), Gradation of Details (P16), Data Access (P8) and Comprehension (P5).

For example, the General Data Protection Regulation (GDPR) was used as the primary motivation by one interviewee for ranking P1 as highly important and having a high impact on the organization. Another interviewee noted: “if not done properly, credibility is lost and as a result, none or fewer data will be opened”. Similar to P1, an interviewee noted about P6: “if the transparency portal has no data quality for some datasets,

Table 5
Overview of case studies in digital transparency.

<table>
<thead>
<tr>
<th>Country</th>
<th>Organization leader</th>
<th>Application name</th>
<th>Application purpose</th>
<th>The expected effect of transparency</th>
<th>Target groups</th>
<th>Number of respondents</th>
</tr>
</thead>
</table>
| Belgium | The Flemish Environment Agency | Flemish Environment Agency Linked Data App (FELAP) | To enhance environmental policy-making in terms of timely publication of the state of affairs related to the environment, to evaluate the policy of issuing permits, and to develop tools for benchmarking the pollution produced by companies in the same economic domain | Accountability | 1. National, regional and local government  
2. Enterprises  
3. Citizens | Three designers involved with the case study |
| England | Trafford’s Innovation and Intelligence Lab | OGI – Trafford pilot prototype | To help support decision-making related to unemployment | Decision-Making | 1. Department for Work and Pensions  
2. Trafford’s Economic Growth Team  
3. Greater Manchester Combined Authority | Three designers involved with the case study |
| Ireland | Marine Institute | Irish National Tide Gauge Network | To enhance the value of the marine data assets for scenario-building purposes by structuring and enriching the data with vocabularies and meanings to aid the extraction of scenario-related requirements | Co-Creation | | Three designers involved with the case study |
this reduces the trust of people, and they might not use the good quality data in the future. This reduces transparency.

The bottom-left quadrant in Fig. 4 comprises low-impact and low-importance principles, particularly Metadata (P12), Interoperability (P11), Data Persistency (P10), Feedback Mechanisms (P3) and Visualization (P7). It is surprising to see Metadata (P12) in this quadrant, as metadata is often found to be a key contributor. One interviewee pointed out that “Without proper metadata, it is quite difficult to understand the dataset. Sometimes we have access to data without metadata and is impossible to discover what the variables and observations mean”. This comment is contrasting with another interviewee who recommended following “ISO 19157 to achieve a high metadata quality”. Various reasons may explain different answers. In some domains, meta-data standards are available; in others, they are not. Another reason for the low scoring of
metadata is that digital transparency initiatives generally focus on a few datasets. In contrast, the more datasets are used, the more important metadata becomes to handle them. Concerning Feedback Mechanisms (P3), an interviewee considered this principle of low importance as “it depends on the data. So sometimes it is essential and sometimes not”, following a quest to monitor “what is done with the data”. The interviewee comments suggest that the design principles’ impact and importance are context-dependent. However, more research is needed to understand and explore this direction.

6. Discussion

6.1. Do the design principles always result in digital transparency?

Disclosing data does not by itself result in digital transparency, accountability, or openness (Matheus & Janssen, 2015). Therefore, this article proposes a set of 16 design principles that form a design theory that can help guide the development of systems for digital transparency. To ensure that their contribution to accomplishing digital transparency is well understood, the principles are described in Table C.1 (Appendix C) using the TOGAF template (TOGAF, 2009).

The principles should be interpreted and used depending on the context, particularly the organizational context. Creating digital transparency is not limited to technical issues associated with developing systems. It also includes organizational changes and creating organizational conditions for digital transparency. For instance, the Privacy (P1) principle of separating privacy-sensitive and -non-sensitive data will influence how personal and non-personal data are separately collected at the source. More research is needed about organizational conditions for digital transparency.

Creating transparency through digital systems can only succeed when such systems are used. While building systems for diverse groups of users consumes money, time, people, and other resources, it also increases the chances for them to be popular with many users who have different needs and expectations. To build such systems, implementing technical features is necessary. Regular users expect easy navigation, which utilizes the well-designed User Interface (UI) and User Experience (UX), related to Visualization (P7). Experienced users might also want to access data through different protocols related to Data Access (P8) and Standardized Formats (P9). This expectation, however, will influence the back-end organization, which must be ready for including this type of functionality in the front-end.

Adhering to the design principles might be more far-reaching for governments. Openness (P2) and Feedback Mechanisms (P3) connect systems for digital transparency with open data use. Feedback mechanisms will influence the front-ends of transparency portals, to include mailboxes or participation buttons for users to submit criticism and suggestions for improvement. It will also affect the back-end since the organizations must be open and ready to listen to users and promptly respond to complaints and suggestions. As a result, substantive organizational changes will be required.

6.2. Is full transparency possible or desired?

While full transparency is often viewed as impossible (Fung, Graham, & Weil, 2007), it might not be even needed or desirable. To make a decision transparent, we only need to know the information on which the decision is based and the rules applied to reach this decision. Providing other types of information about the decision-making process might not add value and instead can produce an information overload. In order to create the desired level of transparency, it is vital to open the right type of information, in the right way, and to the right audience.

Full transparency might conflict with other public values, like privacy or trust, and might easily result in the released information being used for other purposes than those intended. As a concept, transparency is multidimensional and might be highly subjective. Different users might have different expectations of how transparency should be implemented, with personality, experience, culture, social values, and other structural factors all influencing such expectations. For example, a Chilean case study (Gonzalez-Zapata and Heeks (2016) showed that previous decisions (experience) play a major role in how transparency initiatives are implemented.

Full transparency can also bring undesirable effects, including opportunities for large-scale surveillance, lack of accountability for the results of consequential decisions made by inscrutable algorithms, bias and discrimination against groups affected by such decisions, etc. To protect users against such effects, our design principles, particularly Privacy (P1), include the protection of personal data. However, when designing systems for public use, such protection might result in trade-offs between transparency and privacy (Janssen & van den Hoven, 2015). Some mechanisms, though, can simultaneously help release data and ensure privacy. Specific design principles for this possibility should be developed.

Another reason why digital transparency can have undesirable effects is the uncertainty about how transparency-generated information will be used. The paradox of digital transparency is that the data opened to make systems and organizations transparent can be used in opaque ways. For example, algorithms might be used to process open data and make decisions that are difficult or impossible to explain (Nograsek & Vintar, 2014), that discriminate certain social groups (Chander, 2016), that draw conclusions that are inaccurate or incorrect. Also, introducing abruptly high levels of transparency in organizations experiencing systemic corruption might destroy trust in them by their constituencies (Bannister & Connolly, 2011).

7. Conclusions

Creating digital transparency is a significant challenge faced by governments. Merely opening data does not result in digital transparency and might only result in information overload for those wanting to examine such data. In order to create digital transparency, a transparency window should be designed to enable looking at different aspects and from different perspectives of the organization.

This article proposes a set of 16 design principles for digital transparency, which can help overcome a set of well-recognized barriers to such transparency. The principles, organized into a six-stage transparency cycle to facilitate practical applications, can guide government organizations in how they can improve their levels of transparency by digital means. Some principles are relevant to projects, others to systems, yet others to entire organizations. The latter have long-term implications for the organizations and lay the foundations for their digital transparency.

The case studies provided several lessons about the use of such principles. Although all identified principles proved relevant for digital transparency, some were easier to adhere to than others, some were more important for digital transparency than others, and some had more impact on the organizations than others. All designers interviewed used the principles, like protecting privacy and providing metadata, in all case studies. Other principles, such as the opening of raw data, data abstraction, stewardship, visualization, data access, and incorporation of feedback mechanisms, proved both important and easy to use. Yet, other principles were scarcely used in the projects because they required organizational changes or technical foundations like data standardization and harmonization. This diversity of usage scenarios shows that creating digital transparency should be approached as an organizational challenge rather than a system development challenge only.

The design principles are generic and need to be contextualized for an organization intending to use them. In further research, the principles could be used as a kind of guide or even regulation. Furthermore, the set of principles could be refined by adding new principles and modifying existing ones, as new initiatives will likely create new insights and influences. Although the principles proposed in this article focus on
creating data-driven transparency, they could also be used as a basis for creating transparency using Artificial Intelligence (AI) tools. Future research could explore this possibility and refine and extend the principles to AI-driven transparency, considering both public and private sector application scenarios. The principles should also be tested in practice considering different economic, human, political, and legal contexts and barriers that were not considered in this research. Finally, the principles would likely be insufficient for achieving higher levels of digital transparency by themselves. Other factors, like willingness, leadership, capabilities, and resources, play important roles as well.

Acknowledgements

Part of this work is funded by the European Commission within the H2020 Program in the context of the project OpenGovIntelligence [www.opengovintelligence.eu under grant agreement [No. 693849]. Part of this work was funded by the European Commission within the ERASMUS+ Programme in the context of the project CAP4CITY [www.cap4city.eu under grant agreement [No. 598273-EPP-1-2018-1-AT-EPPKA2-CBHE-JP]. The authors would like to cordially thank all the experts who participated in the study.

Declaration of Competing Interest

The authors declare do not have any conflict of interest.

Appendix A. List of papers containing barriers to digital transparency

Table A.1
List of papers containing barriers to digital transparency.

<table>
<thead>
<tr>
<th>Paper ID</th>
<th>Source</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Alfarthi, Krotov, and Bowman (2017)</td>
<td>Lee (2017)</td>
</tr>
<tr>
<td>14</td>
<td>Fan et al. (2014)</td>
<td>Brayne (2017)</td>
</tr>
<tr>
<td>21</td>
<td>Fairfield and Shiein (2014)</td>
<td>(continued on next page)</td>
</tr>
<tr>
<td>22</td>
<td>Wang, Liu, Kumar, and Chang (2016)</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>Mittelstadt and Floridi (2016)</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>Zakim and Schwab (2015)</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>Roski, Bo-Linn, and Andrews (2014)</td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>Nativi et al. (2015)</td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>Fernández et al. (2014)</td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>Gil and Song (2016)</td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>Clarke (2016)</td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>Kruse, Goswamy, Raval, and Marawi (2016)</td>
<td></td>
</tr>
</tbody>
</table>

Appendix B. List of barriers to digital transparency

Table B.1
List of barriers to digital transparency.

<table>
<thead>
<tr>
<th>#</th>
<th>Category</th>
<th>Code</th>
<th>Barrier</th>
<th>Description</th>
<th>Cite Count</th>
<th>Sources</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Human resources</td>
<td>HR1</td>
<td>Lack of skilled people to work with big data</td>
<td>Organizations face a scarcity of talented people to work with big data.</td>
<td>27</td>
<td>1, 3, 4, 5, 6, 7, 11, 12, 18, 21, 22, 23, 24, 25, 26, 30, 31, 35, 39, 40, 44, 45, 46, 47, 48, 49, 50</td>
</tr>
<tr>
<td>2</td>
<td>Technical</td>
<td>TE1</td>
<td>Difficulties in processing vast amounts of data</td>
<td>The vast amounts of data is a technical barrier for dealing with big data analytics.</td>
<td>25</td>
<td>1, 2, 3, 5, 6, 10, 12, 13, 14, 15, 18, 20, 23, 24, 25, 26, 27, 28, 30, 31, 39, 43, 45, 46, 48</td>
</tr>
<tr>
<td>3</td>
<td>Economical</td>
<td>EC1</td>
<td>High cost to create and maintain big data analysis</td>
<td>There is still a high cost to create and maintain big data analysis.</td>
<td>25</td>
<td>1, 2, 4, 5, 11, 13, 14, 15, 18, 21, 22, 23, 24, 25, 26, 28, 30, 31, 32, 33, 34, 37, 38, 41, 49, 50</td>
</tr>
<tr>
<td>#</td>
<td>Category</td>
<td>Code</td>
<td>Barrier Description</td>
<td>Cite Count</td>
<td>Sources</td>
<td></td>
</tr>
<tr>
<td>----</td>
<td>-------------------</td>
<td>-------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Technical</td>
<td>TE2</td>
<td>Complex integration between legacy and big data technology</td>
<td>21</td>
<td>1, 2, 4, 5, 6, 10, 11, 14, 15, 20, 27, 28, 30, 33, 36, 37, 38, 39, 44, 46, 48</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Data Quality</td>
<td>DQ1</td>
<td>Privacy issue due to information sharing risks</td>
<td>13</td>
<td>23, 24, 25, 30, 33, 34, 35, 37, 38, 39, 43, 44, 50</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Human resources</td>
<td>HR2</td>
<td>Low quality of decision-makers</td>
<td>13</td>
<td>1, 6, 8, 10, 12, 13, 15, 16, 20, 30, 31, 39, 50</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Data Quality</td>
<td>DQ2</td>
<td>Data quality issues due to the lack of unified ontologies</td>
<td>11</td>
<td>6, 7, 10, 11, 14, 15, 16, 28, 30, 33, 47</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Usage</td>
<td>US1</td>
<td>Hard to adapt visualization to a wide audience</td>
<td>11</td>
<td>3, 7, 13, 15, 19, 20, 21, 23, 26, 32, 33</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Human resources</td>
<td>HR3</td>
<td>Lack of data-driven culture</td>
<td>11</td>
<td>1, 2, 3, 5, 6, 18, 31, 41, 49, 50</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Data Quality</td>
<td>DQ3</td>
<td>Data quality issues due to multiple types of data sources – unstructured vs structured datasets</td>
<td>11</td>
<td>1, 5, 30, 37, 38, 40, 41, 45, 46, 49, 50</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Data Quality</td>
<td>DQ4</td>
<td>Data quality issue due to lack of accuracy</td>
<td>10</td>
<td>2, 30, 32, 34, 37, 38, 43, 44, 45, 49</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Economical</td>
<td>EC2</td>
<td>Financial issues due to the lack of reliable Return-on-Investment (ROI) studies</td>
<td>10</td>
<td>3, 4, 6, 12, 14, 15, 16, 18, 20, 35</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Data Quality</td>
<td>DQ5</td>
<td>Privacy issues due to re-identification combining datasets</td>
<td>10</td>
<td>1, 2, 5, 8, 14, 16, 41, 42, 44, 49</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Organizational</td>
<td>OR1</td>
<td>Lack of information sharing plans</td>
<td>9</td>
<td>1, 3, 4, 11, 12, 13, 31, 42, 47</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Organizational</td>
<td>OR2</td>
<td>Data quality issues due to ownership</td>
<td>8</td>
<td>2, 23, 25, 30, 37, 43, 45, 50</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Data Quality</td>
<td>DQ6</td>
<td>Data quality issues due to the lack of centralized databases</td>
<td>8</td>
<td>3, 4, 24, 40, 42, 43, 44, 45</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Political and</td>
<td>PL1</td>
<td>Privacy issues due to the lack of privacy policy</td>
<td>7</td>
<td>5, 8, 11, 12, 13, 14, 16</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Legal</td>
<td>TE3</td>
<td>Lack of appropriate methods to deal with modern Big Data systems</td>
<td>7</td>
<td>1, 4, 5, 6, 29, 37, 42</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Political and</td>
<td>PL2</td>
<td>Data protection issues due to mass surveillance</td>
<td>7</td>
<td>1, 6, 8, 17, 41, 42, 44</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Technical</td>
<td>TE4</td>
<td>Technical issues from big data volumes creating data overload to users</td>
<td>7</td>
<td>7, 11, 13, 14, 15, 37, 42</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>Technical</td>
<td>TE5</td>
<td>Data quality issues due to the timeliness</td>
<td>7</td>
<td>4, 30, 32, 37, 42, 43, 45</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>Organizational</td>
<td>OR3</td>
<td>Data quality issues leading to mistakes or misconducts</td>
<td>5</td>
<td>8, 14, 39, 42, 49</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>Economical</td>
<td>EC3</td>
<td>Lack of low-cost analytical tools for big data analysis</td>
<td>5</td>
<td>2, 5, 6, 34, 46</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>Technical</td>
<td>TE6</td>
<td>Lack of performance due to the lack of big data system architecture plans</td>
<td>5</td>
<td>5, 6, 42, 43, 45</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>Technical</td>
<td>TE7</td>
<td>Performance issues due to bandwidth projects</td>
<td>5</td>
<td>2, 5, 13, 14, 26</td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>Technical</td>
<td>TE8</td>
<td>Security issues due to chances of leaking and hacking</td>
<td>5</td>
<td>2, 5, 13, 14, 26</td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>Economical</td>
<td>EC4</td>
<td>Lack of big data system architecture plans leading to unpredictable cost increases</td>
<td>4</td>
<td>1, 6, 30, 35</td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>Technical</td>
<td>TE9</td>
<td>Data quality issues due to the existence of data silos</td>
<td>3</td>
<td>2, 42, 50</td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>Data Quality</td>
<td>DQ7</td>
<td>Data quality issues due to language barriers such as jargon problems</td>
<td>3</td>
<td>3, 30, 42</td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>Usage</td>
<td>US2</td>
<td>Data quality issues due to the overload of information</td>
<td>3</td>
<td>2, 46, 49</td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>Organizational</td>
<td>OR4</td>
<td>Lack of available data</td>
<td>3</td>
<td>8, 18, 21</td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>Human resources</td>
<td>HR4</td>
<td>Lack of skilled employees to lead big data projects</td>
<td>3</td>
<td>1, 39, 42</td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>Political and</td>
<td>PL3</td>
<td>Legal issues due to the lack of stable regulatory frameworks</td>
<td>3</td>
<td>2, 18, 33</td>
<td></td>
</tr>
<tr>
<td>34</td>
<td>Legal</td>
<td>OE5</td>
<td>Asymmetry of information due to the lack of information sharing policies</td>
<td>2</td>
<td>2, 3</td>
<td></td>
</tr>
<tr>
<td>35</td>
<td>Technical</td>
<td>TE10</td>
<td>Lack of data accessibility</td>
<td>2</td>
<td>43, 45</td>
<td></td>
</tr>
<tr>
<td>36</td>
<td>Economical</td>
<td>EC5</td>
<td>Financial issues due to limited budgets</td>
<td>2</td>
<td>3, 4</td>
<td></td>
</tr>
<tr>
<td>37</td>
<td>Organizational</td>
<td>OR6</td>
<td>Lack of algorithmic openness</td>
<td>2</td>
<td>1, 5</td>
<td></td>
</tr>
<tr>
<td>38</td>
<td>Organizational</td>
<td>OR7</td>
<td>Organizational issues due to the lack of awareness about big data possibilities</td>
<td>2</td>
<td>5, 6</td>
<td></td>
</tr>
</tbody>
</table>
| 39 | Ethical           | ET1   | Instigator: 21, 23, 25, 30, 33, 34, 35, 37, 38, 39, 44, 46, 48  
|     |                   |       | Sources: 1, 2, 4, 5, 6, 10, 11, 14, 15, 20, 27, 28, 30, 33, 36, 37, 38, 39, 44, 46, 48 |            |         |

(continued on next page)
Appendix C. Design principles for digital transparency

Table C.1
Design principles for digital transparency.

<table>
<thead>
<tr>
<th>#</th>
<th>Category</th>
<th>Code</th>
<th>Barrier</th>
<th>Description</th>
<th>Cite Count</th>
<th>Sources</th>
</tr>
</thead>
<tbody>
<tr>
<td>40</td>
<td>Ethical</td>
<td>ET2</td>
<td>Privacy issues due to human resource habits, ethics and culture</td>
<td>Algorithms can have biases such as, e.g. discrimination of certain ethnic groups</td>
<td>2</td>
<td>42, 44</td>
</tr>
<tr>
<td>41</td>
<td>Technical</td>
<td>TE10</td>
<td>Security issues due to the lack of log collection and forensic analysis</td>
<td>Culture influences bad habits that can lead to privacy issues</td>
<td>2</td>
<td>1, 2</td>
</tr>
<tr>
<td>42</td>
<td>Technical</td>
<td>TE12</td>
<td>Technical issues due to the lack of user-friendly big data tools</td>
<td>Organizations have no log collection to allow forensic analysis</td>
<td>2</td>
<td>31, 33</td>
</tr>
</tbody>
</table>

P1 Name Separating privacy and non-privacy sensitive data at the source

| Short Name | Privacy |
| Statement | The essential requirement for transparency is determining the privacy level of data. Without knowing whether the data contains sensitive, personal information, it is risky to open it. |
| Rationale | Open data must be balanced with the need to restrict the privacy and sensitivity of data. Private and sensitive data must be protected to prevent improper use and misinterpretation. |
| Implications | There should be a process of determining whether the data can be opened without violating privacy. Government and developers should understand the impact of releasing data and find solutions if such data must be opened but is constrained due to its sensitive nature. |
| Practical Example | Organizations collect daily a lot of data from users. Part of this data can be collected, stored, and used internally. However, sharing part of this data must comply with the privacy laws such as the General Data Protection Regulation (GDPR). A practical example is given by Chanson et al. (2019) using blockchain cases, where the proper level of transparency is achieved to identify essential aspects of transactions without compromising privacy. |

P2 Name The openness of processes and actors

| Short Name | Openness |
| Statement | This principle enables the public to gain information about the operation, structures and decision-making processes of an organization. |
| Rationale | If people are aware of how decisions are made, by whom and using which tools, they will be more trustful towards the outcomes of such decisions. |
| Implications | In order to be transparent, a public organization must be opened in terms of the process, e.g. the procurement or audit flow, who is responsible for which activities, and which tools were used to make decisions. Any change in those aspects should be documented, and the change process itself must be opened. |
| Practical Example | Some processes are unclear, and actors are unwilling to provide details about their actions. A practical example about the openness of processes and actors is the constitution of the United States which aims at reducing corruption and increasing the level of transparency to the public (John C. Bercot et al. (2010), “...” |

P3 Name Feedback Mechanisms for improving digital transparency

| Short Name | Feedback Mechanisms |
| Statement | Feedback mechanisms are critical in understanding the data, which leads to achieving transparency. |
| Rationale | Creation of transparency is an ongoing process, a cycle, which requires feedback, especially to improve the data, system and service quality. |
| Implications | A transparency platform should provide an interface to allow communication between data users, data providers and policymakers regarding the quality and use of the released data. Furthermore, data providers and policymakers should spare some resources (time, dedicated employees, etc.) to interact with data users. |
| Practical Example | Communication is based on a two-way process comprising listening and speaking. Giving voice to users is an important factor identified by Rawlins (2008) who recommended to ask for feedback from people to improve information quality, and consequently, transparency. |

P4 Name Various levels of abstraction for data access

| Short Name | Data Abstraction |
| Statement | Data is accessible for users based on their needs. |
| Rationale | Broader audience leads to different types of user needs and requires various levels of data access. |
| Implications | A transparency platform should define different privileges for user access by understanding different uses of data for each group of users against levels of data sensitivity. |
| Practical Example | Taking into consideration the needs and levels of users, not everyone should have a similar type of access to data. Due to this, Farnams and Siewiorek (1975) recommend reducing transparency to provide the best user experience. Avoiding exposing the algorithms, e.g. creating queries with search boxes using simple words like in Google Search, will help less knowledgeable users work with systems and data. We can also include practical examples following Privacy (P1) principle because depending on the user level in the hierarchy (managerial, tactical, operational, etc.), users should not have access to all data, avoiding GDPR issues. |

P5 Name Avoiding any types of jargon or terms that the public does not understand

| Short Name | Comprehension |
| Statement | Data are presented as simply as possible. |
| Rationale | This principle allows a broader audience to understand and interpret data correctly. |
| Implications | Data should be checked if regular people can understand and interpret it so that they can use it. |
| Practical Example | Jargon and lack of simple language can create barriers to users. As an example, O’Connor and Kelly (2017) recommend using “bureaucratic language and lack of clarity on specifications, as well as a lack of staff professionalism” because this can reduce transparency when small and medium-size enterprises try to access government funds and services. |

P6 Name Checking and rating data quality

| Short Name | Data Quality Rating |
| Statement | Enable ways to provide user features to double-check data quality. |
| Rationale | Data quality plays a vital role in the creation of transparency. The use of data depends on its quality. |
| Implications | Information regarding data quality must be provided in the metadata. The expected effect of transparency, e.g. accountability, requires enriching data with photos or links to external data sources, e.g. Google maps and crowdsources. |

(continued on next page)
Table C.1 (continued)

<table>
<thead>
<tr>
<th>P1</th>
<th>Name</th>
<th>Separating privacy and non-privacy sensitive data at the source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Short Name</td>
<td>Privacy</td>
<td></td>
</tr>
<tr>
<td>Statement</td>
<td>The essential requirement for transparency is determining the privacy level of data. Without knowing whether the data contains sensitive, personal information, it is risky to open it.</td>
<td></td>
</tr>
<tr>
<td>Rationale</td>
<td>Open data must be balanced with the need to restrict the privacy and sensitivity of data. Private and sensitive data must be protected to prevent improper use and misinterpretation.</td>
<td></td>
</tr>
<tr>
<td>Implications</td>
<td>There should be a process of determining whether the data can be opened without violating privacy. Government and developers should understand the impact of releasing data and find solutions if such data must be opened but is constrained due to its sensitive nature.</td>
<td></td>
</tr>
<tr>
<td>Practical Example</td>
<td>Organizations collect daily a lot of data from users. Part of this data can be collected, stored, and used internally. However, sharing part of this data must comply with the privacy laws such as the General Data Protection Regulation (GDPR). A practical example is given by Chanson et al. (2019) using blockchain cases, where the proper level of transparency is achieved to identify essential aspects of transactions without compromising privacy.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>P7</th>
<th>Name</th>
<th>Visualization of different views</th>
</tr>
</thead>
<tbody>
<tr>
<td>Short Name</td>
<td>Visualization</td>
<td></td>
</tr>
<tr>
<td>Statement</td>
<td>Different types of data require different types of visualization.</td>
<td></td>
</tr>
<tr>
<td>Rationale</td>
<td>Providing different types of visualizations such as tables, graphs or maps, as well as the options expected by users, enables more usage and insights.</td>
<td></td>
</tr>
<tr>
<td>Implications</td>
<td>Providing different views on the same data is relevant when working in an interconnected operation. A practical example is given by Matheus et al. (2018) using the IBM Center of Operations as an empirical initiative to demonstrate how different departments might use the same data in different ways. A car accident data would be relevant for various departments in a diversity of forms. Traffic managers would be interested in seeing how much traffic jam it is creating and how to reduce its impact. Police would be interested in contacting the closest car and managing the accident locality as a crime scene requiring a forensic officer. Ambulances would like to know what the fastest route to any hospital with the available surgical operating room is.</td>
<td></td>
</tr>
<tr>
<td>Practical Example</td>
<td>Disclosed data should have a certain level of accountability to avoid practical issues such as a fear of publishing inaccurate or wrong data leading to misuse or mistakes, e.g. the Australian government example in Hardy and Mauroshat (2017), reducing the level of public benefits including transparency.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>P9</th>
<th>Name</th>
<th>Use of standardized formats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Short Name</td>
<td>Standardized Formats</td>
<td></td>
</tr>
<tr>
<td>Statement</td>
<td>Data is available in different but standardized formats to allow comparison.</td>
<td></td>
</tr>
<tr>
<td>Rationale</td>
<td>Different user needs and preferences require different data format types, ranging from human- to machine-readable.</td>
<td></td>
</tr>
<tr>
<td>Implications</td>
<td>The use of data depends on available formats. Data should be available in many formats.</td>
<td></td>
</tr>
<tr>
<td>Practical Example</td>
<td>A practical example of the relevance of accessing data using different protocols was made in Finland to monitor the growth of companies (Salonen et al., 2013). Facebook, Twitter and Google are public web portals. To collect data, data scientists can scrape the portals using bots that copy-paste data from the web pages, or access such pages using Application Programming Interfaces (APIs). Depending on the amount of data, the difference between scraping and APIs can be in the magnitude of hours or days. While some people can be satisfied to access Facebook, Twitter and Google web pages, developers would prefer the automated versions using APIs.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>P10</th>
<th>Name</th>
<th>Persistence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Short Name</td>
<td>Data Persistence</td>
<td></td>
</tr>
<tr>
<td>Statement</td>
<td>Keeping the data with the same original characteristics, i.e. content, name, place etc.</td>
<td></td>
</tr>
<tr>
<td>Rationale</td>
<td>The original data characteristics should be maintained to facilitate data comparisons.</td>
<td></td>
</tr>
<tr>
<td>Implications</td>
<td>The implications include applying a consistent place of access, using the same data content and updating metadata.</td>
<td></td>
</tr>
<tr>
<td>Practical Example</td>
<td>General Transit Feed Specification (GTFS) when dealing with traffic data, e.g. Google maps-related features and data. Other examples can be given of data related to Geographical Information Systems (GIS) such as shapefiles, open data standards such as Comma-Separated Value (CSV) or linked data using the Resource Description Framework (RDF). While CSV and RDF are machine-readable and can be easily used by developers, they also enable human reading.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>P11</th>
<th>Name</th>
<th>Data and system interoperability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Short Name</td>
<td>Interoperability</td>
<td></td>
</tr>
<tr>
<td>Statement</td>
<td>Promoting data, application and technology interoperability.</td>
<td></td>
</tr>
<tr>
<td>Rationale</td>
<td>In order to ensure the integration between building blocks and data, interoperability is required.</td>
<td></td>
</tr>
<tr>
<td>Implications</td>
<td>In order to implement system and data standards for interoperability, a process to implement standards, updates and exceptions should also be provided.</td>
<td></td>
</tr>
<tr>
<td>Practical Example</td>
<td>Transparency is a crucial element of Smart Cities, which have different sources of data and various departments using the same data. A functional Smart City architecture has a high level of interoperability. A practical example is given by Pamp, Nam, and Burke (2012) through the interoperability architecture created to share and integrate all systems and data within internal and external organizational boundaries.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>P12</th>
<th>Name</th>
<th>Include metadata for understandability of data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Short Name</td>
<td>Metadata</td>
<td></td>
</tr>
<tr>
<td>Statement</td>
<td>High-quality metadata supports the understandability of data.</td>
<td></td>
</tr>
<tr>
<td>Rationale</td>
<td>Provide insights, allow combining and check methodology. High-quality metadata is needed to assess data quality and understand the nature of data for the usage intention.</td>
<td></td>
</tr>
<tr>
<td>Implications</td>
<td>Quality Metadata must be provided, including information about context, supporting multilingualism, and identifying data properties and quality.</td>
<td></td>
</tr>
<tr>
<td>Practical Example</td>
<td>Metadata is a crucial element to understand and describe what the data contains. Practical examples are given by Pradipta, Jansen, and Salastri (2017) and (Pradipta, Salastri, Bhasara, &amp; Jansen, 2016). They describe the importance of including metadata in the Extensible Business Reporting Language (XBRL) for transparent financial reporting.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>P13</th>
<th>Name</th>
<th>Transparency-by-design (automatically opening data)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Short Name</td>
<td>Transparency-by-design</td>
<td></td>
</tr>
<tr>
<td>Statement</td>
<td>Transparency requirements are satisfied by the very nature of the design, that the outcomes of the design process should meet these requirements.</td>
<td></td>
</tr>
<tr>
<td>Rationale</td>
<td>The software and business processes should be designed to be open and to open up the public sector.</td>
<td></td>
</tr>
<tr>
<td>Implications</td>
<td>Transparency requirements are considered when designing new systems, administrative processes and procedures. The systems should enable the collection of data and metadata from the source and ensure that such data and metadata can be opened for transparency. Also, the systems should facilitate the understanding and interpretation of data.</td>
<td></td>
</tr>
</tbody>
</table>

(continued on next page)
that we would like to cover. If time begins to run short, it may be necessary to interrupt you to push ahead and complete this line of questioning. (www.opengovintelligence.eu). This research aims to synthesize the principles behind the design of transparency portals. We argue that in order to achieve a level of transparency, principles should be considered in the creation of open data portals.

### Appendix D. Interview Protocol Form

**Introduction**

You are selected as the respondent of this interview to contribute to the creation of transparency portals of the OpenGovIntelligence (OGI) project (www.opengovintelligence.eu). This research aims to synthesize the principles behind the design of transparency portals. We argue that in order to achieve a level of transparency, principles should be considered in the creation of open data portals.

Essentially, this document states that:

(1) all information will be held confidential;
(2) your participation is voluntary, and you may stop at any time if you feel uncomfortable; and, (3) we do not intend to inflict any harm.

**Thank you for agreeing to participate!**

We have planned this interview to last about one hour due to the wide range of the needed information. During this time, we have several questions that we would like to cover. If time begins to run short, it may be necessary to interrupt you to push ahead and complete this line of questioning.

**Section A – General information**
1. What was your pilot?
   ( ) Belgium     ( ) England     ( ) Ireland     ( ) Other: __________________________

Section B – Following Enterprise Architecture and Principles

2. I followed the Enterprise Architecture when creating applications ( ) Strongly disagree
   ( ) Strongly Disagree ( ) Disagree ( ) Neutral ( ) Agree ( ) Strongly Agree

3. I followed (one or more) Design Principles when creating applications ( ) Strongly disagree
   ( ) Strongly Disagree ( ) Disagree ( ) Neutral ( ) Agree ( ) Strongly Agree

Section C – Principle Questions.
This section contains questions about the 16 principles identified in Scientific Literature Review. You will be asked to evaluate each of the principles in the context of the OGI project. You are most welcome to recommend changes in the name and description of each principle. Below you have a figure with the list of Principles.

<table>
<thead>
<tr>
<th>Code</th>
<th>Name</th>
<th>Short Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1</td>
<td>Separating privacy-sensitive and -insensitive data at the source</td>
<td>Privacy</td>
</tr>
<tr>
<td>P2</td>
<td>The openness of processes and actors</td>
<td>Openness</td>
</tr>
<tr>
<td>P3</td>
<td>Feedback mechanisms for improving transparency</td>
<td>Feedback Mechanisms</td>
</tr>
<tr>
<td>P4</td>
<td>Various levels of abstraction for data access</td>
<td>Data Abstraction</td>
</tr>
<tr>
<td>P5</td>
<td>Avoid any jargon or terms that the public does not understand</td>
<td>Comprehension</td>
</tr>
<tr>
<td>P6</td>
<td>Checking and rating data quality</td>
<td>Data Quality Rating</td>
</tr>
<tr>
<td>P7</td>
<td>Visualization of different views</td>
<td>Visualization</td>
</tr>
<tr>
<td>P8</td>
<td>Data access in different protocols</td>
<td>Data Access</td>
</tr>
<tr>
<td>P9</td>
<td>Use of standardized formats</td>
<td>Standardized Formats</td>
</tr>
<tr>
<td>P10</td>
<td>Ensuring that data is unaltered and its history can be traced</td>
<td>Data Persistency</td>
</tr>
<tr>
<td>P11</td>
<td>Data and system interoperability</td>
<td>Interoperability</td>
</tr>
<tr>
<td>P12</td>
<td>Include metadata for data comprehension</td>
<td>Metadata</td>
</tr>
<tr>
<td>P13</td>
<td>Transparency-by-design (automatically opening data)</td>
<td>Transparency-by-Design</td>
</tr>
<tr>
<td>P14</td>
<td>Opening of raw data</td>
<td>Opening of Raw Data</td>
</tr>
<tr>
<td>P15</td>
<td>Assigning stewards responsible for digital transparency</td>
<td>Stewardship</td>
</tr>
<tr>
<td>P16</td>
<td>Supporting views with different level of details</td>
<td>Gradation of Detail</td>
</tr>
</tbody>
</table>

Section D – Principles Evaluation only Example Principle 1 Structure.
Principle 1 - Separating privacy and non-privacy sensitive data at the source

Name: Separating privacy and non-privacy sensitive data at the source

Statement: The essential requirement for transparency is determining the privacy level of the data. Without knowing whether the data contains privacy (including non-privacy but sensitive) data or not, it is risky to opening data.

Rationale: Open data must be balanced with the need to restrict privacy and sensitive data. Privacy and sensitive data must be protected to prevent improper use and misinterpretation.

Implications: There should be a process to determine if the data can be opened without violating privacy issues. The organizations should understand the impact of releasing data and find solutions for opening data that is sensitive or constrained.

[1] Do you agree with this Principle Name? If not, please write below your modified Name (not mandatory)

[2] Do you agree with this Principle Statement? If not, please write below your modified Statement (not mandatory)

[3] Do you agree with this Principle Rationale? If not, please write below your modified Rationale (not mandatory)

[4] Do you agree with this Principle Implications? If not, please write below your modified Implication (not mandatory)

[5] Did you take into account Principle 1 during the development of your OGI application?
   ( ) Yes   ( ) No

[6] What is your rating for Principle 1 in terms of importance?
   ( ) Low Importance ( ) Slightly Important ( ) Neutral ( ) Moderately Important ( ) Extremely Important

[7] Do you want to explain your argument about importance? If yes, please explain below (not mandatory)

[8] In practice, it is easy to implement Principle 1
   ( ) Strongly Disagree ( ) Disagree ( ) Neutral ( ) Agree ( ) Strongly Agree

[9] Do you want to explain your argument about the easiness to implement this principle? If yes, please explain below (not mandatory)

[10] What is your rating for Principle 1 in terms of priority?
    ( ) Low Priority ( ) Somewhat Priority ( ) Neutral ( ) High Priority ( ) Essential Priority

[11] Do you want to explain your argument about your rating in terms of priority? If yes, please explain below (not mandatory)

[12] What is the impact of Principle 1 on the Organization?
    ( ) No Impact ( ) Minor Impact ( ) Neutral ( ) Moderate Impact ( ) Major Impact

[13] Do you want to explain your argument about the impact of this principle on the organization? If yes, please explain below (not mandatory)