D1.1 INSIGHT INTO BARRIERS FOR SHARING PERSONAL DATA RELATED TO FOOD

WP 1, T1.1

AUTHORS: Francesca Grossi (CSCP); Ahmad Hafiz (CSCP);
Michael Bloch von Blottnitz (CSCP)

ABSTRACT

The transition towards fairer, healthier and more sustainable food systems depends increasingly on the availability of high-quality, food-related personal data. Yet citizens' willingness to collect and share such data remains uneven and poorly understood. This report presents the results of a consumer research study within the SPOON project, which investigated the main barriers and enablers influencing the sharing of food-related personal data in the context of citizen science initiatives. This research applied a mixed-methods approach combining a scoping review of 41 academic publications with qualitative validation through focus groups conducted across six Citizen Science Labs in Europe.

Findings indicate that privacy concerns, lack of trust in data handlers, perceived loss of control over shared data, and the time and effort required for data collection are the most significant barriers. At the same time, strong enablers include altruistic motivations to contribute to research, transparent communication about data use, visible security safeguards, user empowerment through opt-in/opt-out mechanisms, and the provision of meaningful feedback or personal benefits.

Overall, the report concludes that responsible food-data sharing is a socio-technical challenge requiring integrated technical solutions, trust-building governance frameworks and inclusive, user-centred design. These insights directly inform the implementation of SPOON's Citizen Science Labs and support the project's objective to enable participatory, data-driven food system transformation.

DISCLAIMER

This project has received funding from the Horizon Europe Framework Programme (HORIZON) under Grant Agreement No. 101182299.

This document has been prepared by SPOON project partners as an account of work carried out within the framework of the EC-GA contract No. 101182299.

Neither the Project Coordinator, nor any signatory party of the SPOON Project Consortium Agreement, nor any person acting on behalf of any of them:

(a) Makes any warranty or representation whatsoever, express or implied:

(i) With respect to the use of any information, apparatus, method, process, or similar item disclosed in this document, including merchantability and fitness for a particular purpose.

(ii) That such use does not infringe on or interfere with privately owned rights, including any party's intellectual property.

(iii) That this document is suitable for any particular user's circumstance.

(b) Assumes responsibility for any damages or other liability whatsoever, including any consequential damages, even if the Project Coordinator or any representative of a signatory party of the SPOON Project Consortium Agreement has been advised of the possibility of such damages, resulting from your selection or use of this document or any information, apparatus, method, process, or similar item disclosed in this document.

TECHNICAL REFERENCES

Project Acronym	SPOON
Project Title	Food Systems in transition – ParticipatOry, Open citizen research for sustainable Nutrition
Project Coordinator	Arlind Xhelili Collaborating Centre on Sustainable Consumption and Production (CSCP) arlind.xhelili@cscp.org
Project Duration	December 2024 – November 2028 (48 months)

Deliverable No.	D1.1
Dissemination level*	PU
Work Package	WP 1 - Research on food system dynamics
Task	T1.1. Research on existing known barriers for sharing personal data, especially related to food
Lead beneficiary	EV ILVO
Contributing beneficiary/ies	AIT, SFC, CSL1: Braunschweig (Germany), CSL2: Thessaloniki (Greece), CSL3: Turin (Italy), CSL4: Bruges (Belgium), CSL5: Valencia (Spain), CSL6: Pomurje region (Slovenia)
Due date of deliverable	31.01.2026
Actual submission date	30.01.2026

- *PU = Public

Funded by the European Union

- SEN= sensitive

v/d	Date	Beneficiary and description	Author
D 1	07/01/2026	CSCP shared a first draft for quality review to SFC and AIT.	Francesca Grossi (CSCP), Ahmad Hafiz (CSCP), Michael Bloch von Blottnitz (CSCP)
D 1	16/01/2026	SFC & AIT provided feedback and completed the quality review process.	Surya Knöbel (AIT), Sergi Lopez (SFC), Arlind Xhelili (CSCP)
D2	30/01/2026	CSCP integrated feedback	Francesca Grossi (CSCP), Ahmad Hafiz (CSCP), Michael Bloch von Blottnitz (CSCP)
V1	31/01/2026	CSCP submitted first version of the deliverable to the granting authority.	Arlind Xhelili (CSCP)

Funded by the European Union

TABLE OF CONTENTS

Funded by the European Union

LIST OF TABLES

LIST OF FIGURES

LIST OF BOXES

1. Introduction

1.1. Background to the topic

Current food systems are estimated to contribute approximately 37% of global greenhouse gas emissions, and their impact on the climate are projected to increase by 50–90% in the coming decades due to population growth and urbanisation (Oakden et al., 2021). At the same time, more than 820 million people worldwide experience food insecurity, highlighting persistent inequalities in access to sufficient, healthy, and nutritious food (Grimaccia & Naccarato, 2020).

Addressing these interconnected challenges requires a transition towards food systems that are both environmentally sustainable and socially inclusive. Policy initiatives and practical approaches, such as the Thrifty Food Plan in the United States, demonstrate that it is possible to maintain nutritious diets even under constrained economic conditions (Donovan et al., 2025). However, implementing such transitions at scale remains complex and depends not only on technological or regulatory solutions, but also on behavioural change and active citizen engagement.

Food consumption practices are deeply embedded in cultural, social, and temporal routines. As a result, meaningful food system transitions can only succeed if these dimensions are adequately understood and addressed (Oakden et al., 2021). Citizens possess unique contextual knowledge of their everyday practices, making their involvement essential for identifying barriers, feasible interventions, and socially acceptable solutions. In this context, food-related personal data represent a valuable resource for understanding consumption patterns, behavioural dynamics, and decision-making processes, and for informing evidence-based policy and research.

Within the European Union, food-related personal data can play a key role in supporting research and policy development aimed at food system transformation. Such data can contribute, for example, to the implementation of the Farm to Fork Strategy, which seeks to promote fair, healthy, and environmentally sustainable food systems and forms a core pillar of the European Green Deal, which is the EU's framework for achieving climate neutrality by 2050 (European Commission, n.d.). The collection and analysis of personal data for these purposes is supported by the European Data Strategy, which aims to create a single market for data, enabling it to flow across sectors for the benefit of researchers, public authorities, and other stakeholders.

At the same time, these policy ambitions depend fundamentally on citizens' willingness to collect and share their personal data. While food-related personal data offer significant potential for research, innovation, and policymaking, data sharing also raises concerns related to privacy, trust, control, and perceived risks. Understanding the barriers, enablers, and contextual factors that shape citizens' willingness to share food-related personal data, particularly in participatory research contexts such as citizen science, is therefore essential. This report addresses this need by examining the factors influencing data-sharing decisions

and identifying strategies that can support responsible, transparent, and trustworthy data sharing.

1.2. The SPOON project

The SPOON project is a European Union–funded research and innovation initiative that addresses the challenges outlined above by placing citizens and their everyday food practices at the centre of food system transformation. By combining behavioural science, digital innovation, and participatory approaches, SPOON seeks to generate evidence that reflects real-world consumption patterns and supports the transition towards fairer, healthier, and more sustainable food systems.

Bringing together citizens, researchers, industry actors, civil society organisations, and policymakers, the project focuses on understanding food purchasing and consumption behaviours and on identifying leverage points for change. Through the collaboration of 16 partner organisations across Europe, SPOON aims to improve knowledge on how dietary behaviours are shaped, to support healthier and more sustainable choices, and to provide decision-makers with evidence grounded in citizens' lived experiences.

A central element of SPOON is the development and implementation of a Digital Toolset (see a short description of the toolset in **Box 2**) that enables citizens to actively collect and share food-related personal data within Citizen Science Labs (CSLs) (see an overview of the SPOON CSLs in **Box 1)**. These tools support the generation of high-quality, real-world data and facilitate joint reflection between citizens and research hers. By embedding the collection and use of food-related personal data within co-creation processes, SPOON integrates citizen-generated evidence with scientific analysis to support participatory, data-driven food system innovation. In doing so, the project directly addresses the behavioural, contextual, and governance challenges associated with food system transformation, as outlined in the previous section.

Box 1: SPOON CSLs

SPOON CSLs: A BLEND OF CITIZEN SCIENCE AND LIVING LABS

SPOON brings science into everyday life through CSLs: locally based, participatory labs where people from diverse backgrounds explore their food environments, collect and analyse data, and co-create practical solutions for healthier and more sustainable food habits. CSLs ensure research is not only about communities, but with communities-so the insights, tools, and interventions developed through SPOON reflect real needs and can be owned and used locally.

SPOON's CSLs combine two complementary approaches:

- **Citizen Science:** public participation in research: citizens help define questions, gather evidence, interpret findings, and share results.
- **Living Labs:** real-life co-design and testing: participants and local stakeholders collaboratively ideate solutions in everyday contexts (homes, neighbourhoods, shops, schools, community hubs), with an emphasis on usability, feasibility, and impact.

HOW CSLs WORK IN PRACTICE

Across the pilot sites, CSL participants:

- **Map and assess local food environments** (availability, affordability, accessibility, and exposure to healthy vs. unhealthy options).
- **Track food-related behaviours** across the food journey (planning, buying, storing, preparing, eating, and disposing).
- **Test and refine locally relevant actions**—from awareness initiatives to behavioural nudges and community or policy-oriented ideas.
- **Use SPOON's digital tools** to support participation and local ownership, enabling participants to collect, visualise, and reflect on their data and feed insights directly into co-design activities.

SIX EUROPEAN PILOT LOCATIONS

SPOON selected six CSLs across six European countries, **Germany, Greece, Italy, Belgium, Spain, and Slovenia**, to reflect diverse contexts, including differences in geography and climate, food production systems, and access to healthy and sustainable food. The selection also considers **food deserts/food swamps**, varying levels of food insecurity, and a wide range of thematic challenges. The CSLs span both **urban and rural** settings and include Mediterranean contexts linked to culinary heritage as well as northern/central European regions with different supply-chain realities.

Funded by the European Union

Box 2: SPOON Digital Toolset

SPOON DIGITAL TOOLSET

The **SPOON Digital Toolset** is a **suite of interconnected digital solutions** that helps **citizens, researchers, and policymakers** support food-systems transformation using **data-driven innovation, citizen science**, and **secure digital interactions**.

It is built around **GDPR compliance, transparency, and user control**, so individuals can take part in research and decision-making while maintaining **full sovereignty over their personal data**.

MAIN COMPONENTS AND PURPOSE

DataU and DashboardU
A GDPR-compliant consent and data-sharing management system. It enables transparent and secure user-controlled sharing through DashboardU.

Personal Data Wallet
An encrypted personal repository where citizens can store, manage, and selectively share their food-related data.

Questionnaire Generator Tool
A customizable survey platform to collect citizen food data, which is then stored in the SPOON Database.

SPOON Data Lake
A repository of anonymized datasets coming from the data collected in the project and third party applications, supporting broader analysis and reuse.

Software Development Kit
A developer toolkit that makes it easier for external apps to connect to DataU and align with GDPR-compliant consent/data-access workflows.

Funded by the European Union

1.3. Purpose, scope and research questions of this deliverable

This report presents the results of a SPOON consumer research study which examines the main barriers and enablers influencing the sharing of food-related personal data, with a particular focus on citizen participation in research contexts. The analysis is based on a comprehensive scoping literature review synthesising existing academic knowledge on data-sharing practices, privacy concerns, trust, and governance mechanisms related to personal food data. These initial findings were then complemented by empirical validation through focus group discussions conducted within each CSL.

By integrating insights from both literature and citizen perspectives, this report provides an evidence base to inform the design and implementation of SPOON's CSLs and to support the planning and execution of citizen science activities within the project.

Building on this evidence base, the analysis examines the factors shaping citizens' willingness to share food-related personal data and explores how trust, technology, incentives, and governance arrangements influence responsible data-sharing practices in the context of sustainable food systems. The analysis is guided by the following research questions:

1. What are the main barriers to food data sharing, and how do privacy concerns, trust, and past experiences influence consumer willingness?
2. How do emerging technologies (e.g., blockchain, AI, differential privacy) enhance consumer trust and willingness to share food-related personal data?
3. What strategies and regulatory frameworks can effectively address consumer concerns and encourage responsible food data sharing?
4. How do incentives and cultural/socio-demographic differences influence consumer willingness to share food-related personal data?

1.4. Structure of this report

Following the introductory sections, this report is structured as follows:

Section 2 describes the mixed-method design combining a scoping literature review and focus group validation to analyze barriers, facilitators, and contextual factors affecting the sharing of personal food-related data.

Section 3 reviews definitions, types, sources, sharing methods, and key actors involved.

Section 4 presents key evidence on barriers, enablers, and contextual factors influencing citizens' willingness to share food-related personal data, structured around the research questions.

Section 5 reports how citizens perceive, prioritize, and negotiate literature-based barriers, enablers, and governance issues, with additional insights from SPOON CSL discussions.

Section 6 proposes solutions to overcome barriers and promote responsible data sharing, covering technical tools, governance models, trust-building incentives, and policy actions for stakeholders.

Section 7 synthesizes cross-cutting insights, reflects on implications for SPOON CSL design and implementation, and outlines limitations and future directions for research and policy.

Funded by
the European Union

2. Methodology

2.1. Overview of the methodological approach

The methodological approach adopted in this consumer research study combines a structured scoping literature review with qualitative validation through focus group discussions. This mixed-methods design was selected to ensure a comprehensive understanding of the factors influencing citizens' willingness to share food-related personal data, drawing both on existing academic evidence and on empirical insights from citizen perspectives.

The scoping literature review provides a systematic overview of established knowledge on barriers, enablers, and contextual factors related to personal data sharing, with particular attention to food-related data and adjacent domains such as health and lifestyle data. Given that findings in this field are often context-dependent, the literature review was complemented by focus group discussions conducted within the six SPOON CSLs. This validation step serves to assess the relevance of literature-based findings in the specific context of participatory food system research and to identify additional barriers or enabling factors not sufficiently covered in existing studies.

Together, these methods allow for triangulation between academic evidence and citizen experiences, strengthening the robustness, relevance, and applicability of the findings for subsequent SPOON activities.

2.2. Literature review procedure

A scoping review of the academic literature was conducted to identify and synthesise existing evidence on barriers and enablers related to the sharing of food-related personal data. The literature review followed a Preferred Reporting Items for Systematic reviews and Meta-Analyses (PRISMA) inspired framework adapted for qualitative and thematic analysis. Systematic keyword searches across the following five academic databases were conducted during the identification phase, to ensure broad coverage across disciplines relevant to data sharing, privacy, health, and food systems research: 1) Google Scholar: 2) JSTOR: 3) Web of Science: 4) PubMed: 5) ResearchGate.

A set of keywords was used in various combinations to identify relevant publications, including: (i) Barriers, (ii) Food consumption data, (iii) Personal food data, (iv) Health data, (v) Lifestyle data, (vi) Personal data, (vii) Data sharing, (viii) Data sharing for research, (ix) Data donation, (x) Citizen science, (xi) Data privacy, (xii) Data security, (xiii) Privacy, (xiv) Perceived privacy, (xv) Privacy concerns, (xvi) Privacy calculus, (xvii) Consumer trust, (xviii) Willingness to share, (xix) Cryptography, (xx) Privacy-preserving systems, (xxi) Differential privacy, (xxii) Encryption, (xxiii) Internet of things, (xxiv) Blockchain, (xxv) GDPR, (xxvi) National culture, (xxvii) Monetary compensation, and (xxviii) Data monetization.

Following the PRISMA framework (**Figure 5**), an initial screening of publications identified through the keyword search was conducted based on titles and abstracts. Three main inclusion criteria were applied. First, priority was given to studies addressing food-related personal data; however, due to the limited volume of literature specifically focused on food data, studies on health-related or general personal data were also included when they provided relevant insights. Second, studies were required to address data sharing, with a preference for research-related data sharing contexts, while allowing for the inclusion of more general data-sharing studies where appropriate. Third, the selected publications needed to adopt a user-centred perspective, focusing on user perceptions, concerns, motivations, or decision-making related to data sharing (See annex for coding scheme used for the qualitative research).

Based on these criteria, a total of 41 publications (see below the narrowing down process of research) were selected for full-text analysis as per the PRISMA framework's last step. Insights from these studies were systematically extracted and organised into six overarching thematic categories: (i) technological or systemic barriers, (ii) socio-demographic variability, (iii) ethical and psychological factors, (iv) perceived lack of personal benefits, (v) trust in data handlers, and (vi) privacy and data security concerns. These themes were further refined into barriers, enablers, and context-dependent factors, and operationalised through a structured codebook.

Table 1: PRISMA Workflow

Stage	Description	Number of Articles
Identification	Records identified across databases (PubMed, Google Scholar, Web of Science, ResearchGate, JSTOR)	**Not numerically logged**
Screening	Records screened (title and abstract review)	**50**
Eligibility	Full-text articles excluded after detailed review	**9**
Included	Full-text articles included in final analysis	**41**

All selected publications were imported into MAXQDA (version 24), where full-text coding was conducted. Studies were categorised as food-related, health-related, or general personal data studies. Relevant text segments were coded using the predefined codebook and linked to the research questions guiding the analysis, enabling both qualitative synthesis and quantitative comparison across themes and study types.

2.3. Focus groups design & implementation

Focus group discussions were conducted to validate and contextualise the findings of the literature review and to capture citizens' perspectives on sharing food-related personal data in participatory research settings. Rather than generating statistically representative data, the focus groups were designed as a qualitative validation mechanism to assess whether

literature-based barriers and enablers are perceived as relevant within the context of the SPOON CSLs and to identify additional factors emerging from lived experiences.

The focus groups were organised in person as part of the first iteration of the csls and followed a common discussion framework across all participating sites. Each session explored participants' familiarity with food-related data sharing, perceived risks and benefits, knowledge and perceptions of data protection, views on governance and potential solutions, and motivations or incentives for participation. This structure ensured consistency while allowing flexibility for participants to elaborate on locally relevant issues.

Group sizes typically ranged from six to twelve participants (a total of 75 participants took part in the first CSL iteration across the six CSLs), enabling interactive discussion while maintaining diversity of perspectives in terms of age, gender, educational background, and levels of digital literacy. All discussions were moderated by trained facilitators and documented using a standardised Focus Group Summary Template (see Annex) to further ensure comparability of discussion outcomes across sites. The resulting summaries formed the empirical basis for validating, refining, and contextualising the literature-based findings presented in this deliverable.

2.4. Analytical framework and approach

The analytical framework combined qualitative thematic analysis with descriptive quantitative analysis to synthesise evidence from the literature review and focus group validation. This dual approach was adopted to capture both the relative prominence of different barriers and enablers in the literature and the substantive meaning and interpretation of these factors across contexts.

2.4.2. Quantitative analysis

Quantitative analysis focused on the systematic examination of coded segments across the selected publications. This included analysing the frequency and distribution of coded barriers, enablers, and context-dependent factors across the predefined thematic categories and research questions. The analysis also compared the occurrence of themes across different types of studies (food-related, health-related, and general personal data studies), allowing for an assessment of how evidence varies by domain.

The quantitative component does not aim to establish causal relationships or statistical significance, but rather to identify patterns, gaps, and areas of concentration within the existing literature. These descriptive insights provide an overview of where academic attention has been concentrated and where evidence remains limited.

2.4.2. Qualitative analysis

Qualitative analysis was used to interpret and synthesise the content of the coded material in depth. Coded segments within each theme and sub-theme were reviewed holistically to identify recurring arguments, tensions, and contextual nuances related to food-related

personal data sharing. The research questions served as an organising framework to ensure that the analysis addressed all relevant dimensions of willingness to share data, including trust, privacy, technology, incentives, and governance.

In addition, a gap analysis was conducted by identifying themes and sub-themes with limited coverage in the literature, as well as areas where findings were inconsistent or context-dependent. Insights from the focus group discussions were then used to validate, nuance, or extend the literature-based findings, supporting a richer understanding of how barriers and enablers manifest in real-world citizen science contexts.

3. OVERVIEW OF PERSONAL DATA IN THE FOOD SECTOR

3.1. Defining “food-related personal data”

While no single, universally accepted definition exists, food-related personal data can be broadly understood as data that directly or indirectly reveal information about an individual’s food-related behaviours, preferences, purchases, health-related characteristics, or contextual factors such as location. Due to their potential to reveal sensitive aspects of daily life and lifestyle, such data are subject to privacy, ethical, and governance considerations (Reitano et al., 2024; Donovan et al., 2025).

In the context of this report, food-related personal data primarily encompass information related to individuals’ dietary behaviours and food consumption practices. For example, loyalty card records can provide detailed insights into purchasing patterns, dietary choices, and consumption frequency, while online food purchases and delivery data may reveal consumption histories and routines relevant for food safety, nutrition, and sustainability research (Donovan et al., 2025; Reitano et al., 2024). Similarly, data generated through nutrition and health applications, including food logs, activity levels, and diet-related health indicators, constitute personal data due to their link to identifiable individuals and their potential sensitivity (Donovan et al., 2025).

By capturing both objective behaviours (such as purchases or logged consumption) and subjective dimensions (such as preferences or perceptions), food-related personal data offer valuable insights into how individuals interact with food systems. At the same time, their personal and potentially sensitive nature makes citizens’ willingness to collect and share such data a critical issue for participatory research and policy development.

3.2. Typologies and sources of food-related personal data

Food-related personal data encompass a wide range of information reflecting not only what individuals eat or purchase, but also how they perceive, interpret, and evaluate food products, food systems, and associated risks. To structure this diversity and support the subsequent analysis, this report distinguishes between three main categories of food-related personal data: behavioural data (including sharing about the food they eat via social media apps and platforms), transactional data, and perceptual data. While these categories differ in terms of content, sources, and modes of collection, together they provide a comprehensive picture of food-related practices, decisions, and attitudes (Maringer et al., 2018).

Behavioural data: Behavioural data capture individuals’ food-related actions, habits, and preferences, including dietary choices, meal patterns, and consumption routines. This

category encompasses information on personal food preferences and eating behaviours that is typically generated through self-reporting, for example via food diaries, mobile applications, or digital platforms, as well as through semi-automated tools such as barcode scanning or image recognition (Maringer et al., 2018).

From an analytical perspective, behavioural data enable researchers to examine dietary patterns over time, assess adherence to nutritional guidelines, and explore how cultural, social, and personal factors shape food consumption practices. At the same time, the reliance on active user input highlights the importance of usability, user experience, and sustained engagement, particularly in participatory research contexts such as citizen science initiatives.

Transactional data: Transactional data refer to records of food-related purchases and expenditures, offering relatively objective insights into consumption behaviour. These data include point-of-sale records, online grocery transactions, and loyalty card histories, which document what products are purchased, in what quantities, and at what times (Donovan et al., 2025; Kosior & Młodawska, 2024). Due to their high temporal resolution and longitudinal nature, transactional data are particularly valuable for analysing purchasing trends, market dynamics, and the impacts of policy or behavioural interventions over time (Qian et al., 2023).

A more granular subset of transactional data is represented by loyalty card purchase histories, which capture food and non-food purchases made through retailer-issued loyalty schemes. Automatically generated at the point of sale and stored in integrated databases, these records provide detailed information on product types, quantities, brands, and purchase timing. As such, loyalty card data offer a robust empirical basis for analysing dietary patterns, health-related behaviours, market segmentation, and the effects of policy or technological interventions within food systems (Donovan et al., 2025).

Perceptual data: Perceptual data capture individuals' subjective judgments, beliefs, and concerns related to food products and food systems. One key dimension within this category is perceived food safety, which reflects how safe individuals believe food products to be. While behavioral data record what people do (e.g., purchases, consumption, waste patterns), perceptual data capture what people think and feel, reflecting subjective judgments, beliefs, and concerns about food products and systems. Unlike objective scientific assessments, perceptual food safety data represent personal attitudes, risk perceptions, and levels of trust, and are commonly collected through surveys, experiments, or digital feedback mechanisms (Qian et al., 2023).

Perceived risk of origin extends this perspective by focusing on individuals' beliefs regarding the authenticity, quality, and safety of food products based on their geographical or production origin. These data encompass perceptions of the accuracy and reliability of origin information, concerns about fraud or mislabelling, and apprehensions related to regional production standards. Typically collected through consumer surveys, choice experiments, interviews, or digital platforms, perceived risk-of-origin data provide valuable insights into consumer trust, purchasing behaviour, and barriers to the adoption of traceability and origin-verification technologies (Kosior & Młodawska, 2024).

Relevance for the SPOON project: Taken together, the behavioural, transactional, and perceptual data types outlined above provide an evidence base that directly supports the

objectives of the SPOON project. Behavioural data on personal food preferences enable the mapping of dietary habits and the identification of leverage points for promoting healthier and more sustainable consumption patterns (Maringer et al., 2018). Transactional data, including consumer purchasing records and loyalty card histories, offer objective and high-resolution insights into actual food purchases, allowing for the validation of self-reported behaviours and the monitoring of changes over time (Donovan et al., 2025; Kosior & Młodawska, 2024; Qian et al., 2023). Perceptual data, such as perceptions of food safety, risk of origin, and traceability authenticity, capture citizens' attitudes, trust levels, and concerns, which are essential for designing interventions that are both socially acceptable and effective (Kosior & Młodawska, 2024; Qian et al., 2023). By integrating these complementary data types, SPOON's participatory approach combines behavioural science and digital innovation to co-create evidence-based solutions that empower citizens, inform policymakers, and support the transformation towards fairer, healthier, and more sustainable food systems.

3.3. Current practices and actors involved in food data sharing

Food-related personal data are currently generated, collected, and shared through a diverse set of practices involving digital platforms, commercial services, research initiatives, and public institutions. These practices differ substantially in the types of data collected, the level of user involvement required, and the governance and consent arrangements under which data are processed. Understanding how food-related data are currently generated and circulated across various actors provides important context for assessing existing barriers, enablers, and risks associated with data sharing. The following subsections outline the some key channels / platforms and actors shaping contemporary food-related data ecosystems.

Food consumption applications: are mobile or web-based platforms that enable individuals to record, monitor, and manage their dietary behaviours, including calorie counting, diet tracking, nutrition planning, and food delivery. These applications collect data through three primary mechanisms: (i) direct user input, such as manual logging of meals, ingredients, portion sizes, and timing of consumption; (ii) semi-automated acquisition via barcode scanning, image recognition, and integration with wearable devices or online grocery accounts; and (iii) background tracking of contextual information, including location, activity levels, and purchase histories (Cordeiro et al., 2015; Maringer et al., 2018; Donovan et al., 2025).

The data captured through food consumption applications typically include personal food preferences; detailed consumption records (e.g. caloric and nutrient intake, meal timing, portion size); transactional information (e.g. grocery purchases or restaurant visits); biometric indicators when linked to health devices; and contextual data related to users' environments and routines (Cordeiro et al., 2015; Maringer et al., 2018; Donovan et al., 2025). These data are primarily stored within application-specific databases to support personalised feedback and self-monitoring functionalities. Depending on user consent and platform policies, they may

also be shared with third parties, such as researchers, analytics providers, or commercial partners, or exported to connected health platforms or research projects, contributing to a broader data ecosystem for analysing dietary patterns and health-related behaviours (Maringer et al., 2018; Donovan et al., 2025).

Nutrition applications: represent a closely related but distinct category of digital platforms designed to support individuals in improving diet quality, achieving health-related goals, and making informed food choices by integrating nutrition science, behavioural guidance, and data analytics (Maringer et al., 2018; Donovan et al., 2025). Beyond basic food logging, these applications analyse nutritional content, track micronutrients such as vitamins, minerals, and fibre, and provide personalised feedback aligned with users' health objectives.

Many nutrition apps generate tailored meal plans for specific needs, such as weight management, sodium reduction, or blood glucose control, and offer educational content to enhance users' understanding of the relationship between food and health (Maringer et al., 2018; Donovan et al., 2025). Data collection relies on a combination of manual input, barcode scanning, photo recognition, integration with wearable devices, and linkage to online grocery services (Cordeiro et al., 2015; Maringer et al., 2018; Donovan et al., 2025). The resulting datasets include detailed consumption and nutrient profiles, health-related indicators, and contextual information, which are stored within application systems to support personalised feedback. With user consent, these data may be shared with researchers or analytics providers or integrated into broader health data platforms, enabling longitudinal monitoring of dietary behaviour (Maringer et al., 2018; Donovan et al., 2025).

Other actors and data-sharing practices: Beyond food consumption and nutrition applications, a wide range of additional actors and practices contribute to the generation, collection, and sharing of food-related personal data. Retailers and loyalty-card systems automatically generate transactional records, such as product type, quantity, brand, and timing of purchases, which may be shared with advertisers, data brokers, or research partners (Donovan et al., 2025). Food delivery and restaurant platforms collect information on order choices, frequency, location, and expenditure, which can be used to optimise menus, logistics, and personalised marketing strategies (Donovan et al., 2025).

Smart kitchen devices and other Internet-of-Things (IoT) products monitor in-home consumption patterns and transmit data to manufacturers or cloud service providers to support functions such as replenishment prediction, recipe recommendations, or targeted advertising. Wearable devices and digital health platforms integrate biometric and dietary data, which may be shared with health professionals or researchers, subject to user consent (Donovan et al., 2025).

In addition, social media platforms host voluntarily shared food-related content, such as recipes, meal photographs, and reviews, that can be analysed to identify trends, preferences, or sentiments (Cordeiro et al., 2015). Blockchain-based traceability systems disclose information on product journeys while also recording consumer interactions, such as QR-code scans, thereby generating insights into demand patterns and trust in food supply chains (Kosior & Młodawska, 2024). Finally, government health surveys and food-frequency questionnaires remain important sources of population-level food consumption data (Donovan et al., 2025).

3.4. Key influencing factors

A range of contextual factors shape how individuals perceive and engage with the sharing of food-related personal data. Drawing on established literature on personal data sharing, privacy, and trust, this section introduces a set of key influencing factors that are commonly identified as relevant across domains. These factors do not represent findings of the present literature review, but rather provide an analytical framing that informs the synthesis of evidence presented in Section 4.

Specifically, this section introduces three key groups of influencing factors, namely, privacy and data protection awareness, trust and perceived control, and socio-demographic and cultural characteristics which are examined in greater analytical depth in the subsequent literature review and validated through focus group discussions.

Privacy concerns and data protection awareness: Individuals' perceptions of digital privacy, together with their awareness of data protection practices and regulatory frameworks, form an important context for food-related personal data sharing. Privacy is commonly understood as the condition of being free from unwanted intrusion; however, in digital environments it increasingly encompasses the appropriate collection, processing, and use of personal data (Sharma, 2019). Digital privacy therefore relates not only to the protection of individuals' digital identities, but also to safeguards ensuring that personal data cannot be misused or accessed by unauthorised actors (Sharma, 2019).

Public awareness of digital privacy risks has been heightened by high-profile data breaches and misuse scandals. Incidents such as the unauthorised use users' data by Cambridge Analytica in 2018, as well as subsequent large-scale data leaks, have drawn attention to vulnerabilities within digital data ecosystems and to the potential consequences of inadequate data protection (Schumacher et al., 2022). In parallel, the introduction of the General Data Protection Regulation (GDPR) in the European Union has increased awareness of individual rights related to consent, transparency, and data access, while also establishing a regulatory framework that shapes expectations around lawful and ethical data use (Yadav et al., 2024).

Trust and control perceptions: Trust represents a further key contextual factor influencing data-sharing behaviour and refers to confidence in the integrity, competence, and intentions of actors involved in data collection and use. In personal data-sharing contexts, trust is closely linked to perceptions of whether data handlers will respect privacy, act responsibly, and comply with stated rules and safeguards (van Panhuis et al., 2014).

Closely related to trust is the perception of control over personal data. In digital contexts, control refers to individuals' ability to decide when and how their data are shared, to understand the purposes for which data are used, and to withdraw consent or request data deletion where applicable (Ackermann et al., 2021). Perceived control shapes how data-sharing arrangements are interpreted by users and influences their confidence in engaging with data-driven systems, even when formal safeguards are in place.

Socio-demographic and cultural aspects: Socio-demographic and cultural characteristics add an additional layer of context to data-related attitudes and practices. Factors such as age, education level, and digital literacy influence individuals' familiarity with digital technologies, awareness of data-related risks, and understanding of data protection mechanisms. Cultural frameworks, including values associated with individualism or collectivism, norms of reciprocity, and historical experiences with institutions and authority. further shape how concepts such as privacy, data ownership, and trust are understood and negotiated (Schumacher et al., 2022).

Recognising these socio-demographic and cultural dimensions is essential for understanding diversity in perspectives on data sharing and for developing data-sharing approaches that are inclusive and responsive to differing levels of awareness, expectations, and concerns across population groups.

4. KEY FINDINGS FROM THE LITERATURE REVIEW

This section synthesises the analytical findings of the literature review, focusing on the barriers, enablers, and contextual conditions influencing the sharing of food-related personal data. Building on the conceptual overview provided in Section 3, this section examines how these factors are evidenced and discussed across the literature in relation to the research questions. The findings are structured into an initial overview (Section 4.1), barriers (Section 4.2), enablers (Section 4.3) and context-dependent factors that may function as either depending on circumstances (Section 4.4), followed by a cross-cutting synthesis (Section 4.5).

4.1. Overview of the analytical synthesis

This subsection provides a quantitative overview of the literature synthesis based on the coding and analytical procedures described in Section 2.

Figure 5 and **Figures 1, 2, and 3** summarise the number of coded segments, disaggregated by research question, thematic category, type of publication, and classification as barrier or enabler. **Figure 4** presents the frequency of individual codes across all reviewed articles.

Table 2: Matrix of coded-segment counts by theme for each research question

Theme	RQ1	RQ2	RQ3	RQ4	Total
Technological or systemic barriers	42	27	27	0	96
Socio-demographic variability	6	0	0	16	22
Ethical and psychological factors	92	11	20	2	125
Perceived lack of personal benefits	28	1	0	17	46
Trust in data handlers	40	11	13	1	65
Privacy concerns & data security	68	49	12	2	131

As illustrated in **Table 2**, the distribution of coded segments varies across thematic categories and research questions:

Research Question 1 accounts for the highest number of coded segments overall, with ethical and psychological factors representing the most frequently coded theme, although all

thematic categories are represented. This reflects the broad scope of Research Question 1, which encompasses multiple dimensions of food-related personal data sharing.

Research Question 2 is associated with a smaller number of coded segments, with a higher concentration in the themes of technological or systemic barriers and privacy concerns and data security. This pattern reflects the focus of Research Question 2 on technological approaches and mechanisms related to privacy-preserving data sharing.

For Research Question 3, coded segments are predominantly associated with technological or systemic barriers and ethical and psychological factors. Legal and regulatory aspects, which are particularly relevant to this research question, were coded under the category of systemic barriers, contributing to the prominence of this theme.

Research Question 4 shows a different distribution, with most coded segments falling under socio-demographic variability and perceived lack of personal benefits, including insights related to incentives and participation conditions. These themes appear less frequently in relation to the other research questions, highlighting their more specific relevance to factors influencing willingness to share data across different population groups.

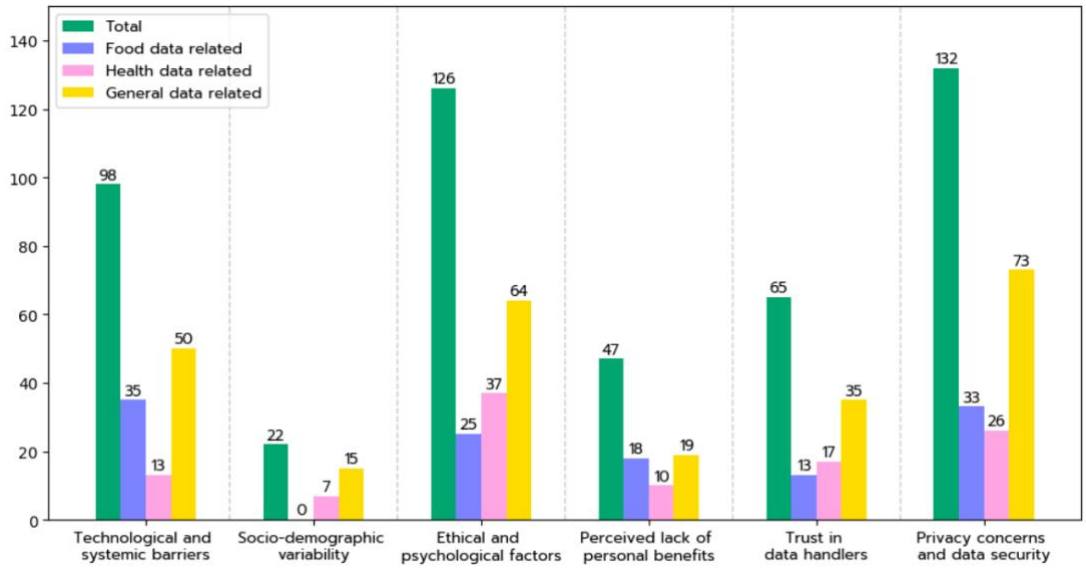

Figure 1: Overview of coded segments identified per theme and article type

As shown in **Figure 1**, a higher number of coded segments is associated with the themes privacy concerns and data security, ethical and psychological factors, and technological or systemic barriers, compared to the other thematic categories. In contrast, fewer coded segments were identified for socio-demographic variability, perceived lack of personal benefits, and trust in data handlers, with socio-demographic variability representing the least frequently coded theme.

Across all thematic categories, the largest share of coded segments originates from studies addressing general personal data. The relative contribution of food-related and health-related studies varies by theme, but general data–related literature consistently accounts for the highest number of coded segments. For technological or systemic barriers, perceived lack of

personal benefits, and privacy concerns and data security, food-related studies contribute more coded segments than health-related studies, while for the remaining themes both food- and health-related studies contribute smaller shares relative to general data–focused research. Socio-demographic variability shows no coded segments originating from food-related studies.

While socio-demographic factors such as income and education are strongly linked to food insecurity and dietary outcomes, the reviewed literature provides limited direct evidence linking these factors to individuals' willingness to share food-related personal data. This underscores their role as contextual rather than causal influences in data-sharing behaviour.

The distribution of coded segments classified as barriers, enablers, or context-dependent factors also varies across themes. Technological or systemic barriers and perceived lack of personal benefits are predominantly associated with barriers, reflecting the way these themes are conceptualised in the literature. In contrast, ethical and psychological factors are more frequently associated with enablers. The themes trust in data handlers and privacy concerns and data security display a more balanced distribution of barriers and enablers, alongside several context-dependent elements that may function as either, depending on the data-sharing context. Socio-demographic variability is represented exclusively by context-dependent factors, as it captures differences across population groups rather than factors that inherently promote or hinder data sharing.

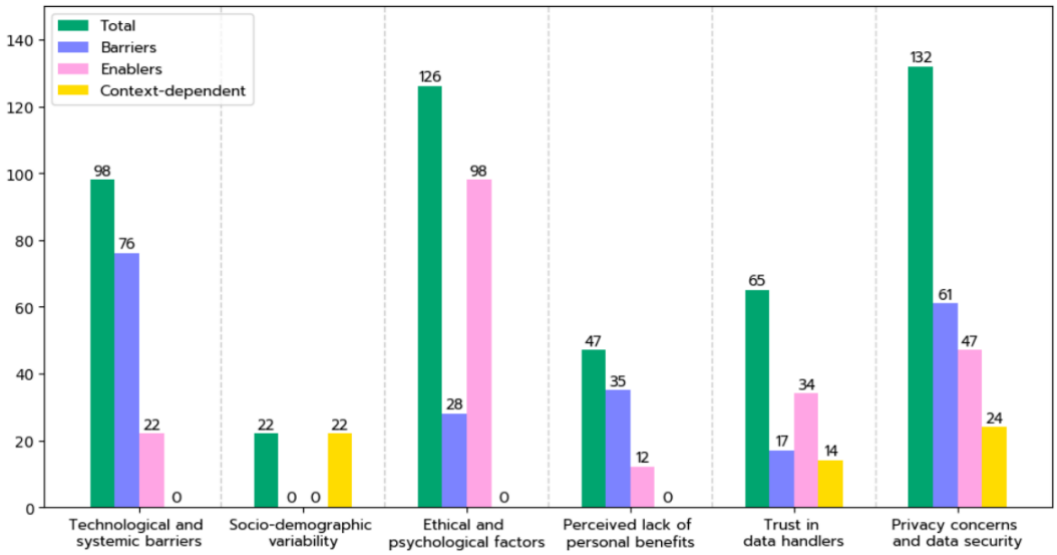

Figure 2: Distribution of barrier and enabler codes per theme

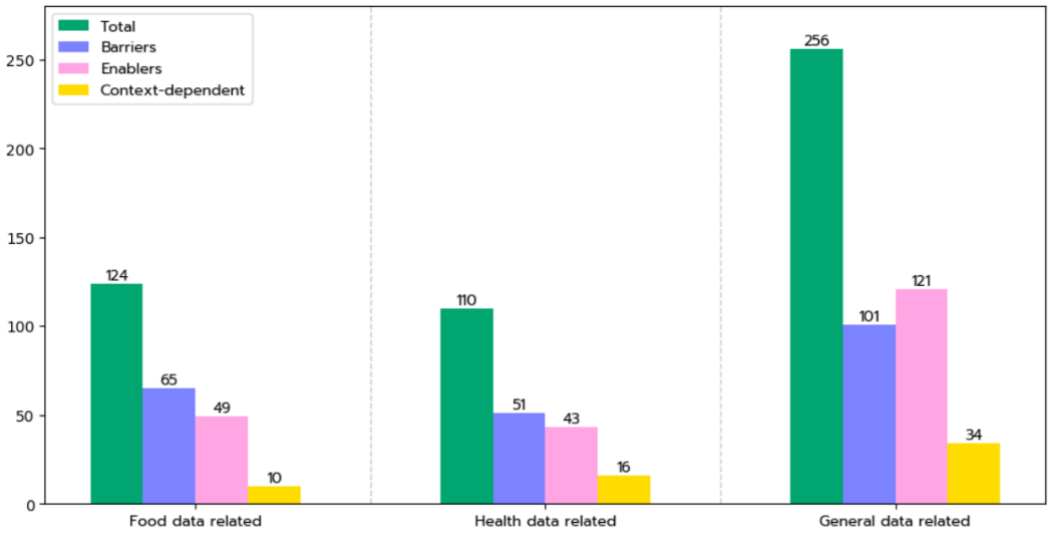

Figure 3: Distribution of barrier and enabler codes per type of article

As illustrated in **Figure 2** and **Figure 3**, the distribution of coded segments classified as barriers and enablers varies across thematic categories and types of literature. While barriers constitute the majority of coded segments for themes such as technological or systemic barriers and perceived lack of personal benefits, ethical and psychological factors are predominantly associated with enablers across all types of articles.

Differences are also evident across article types. General personal data studies show a higher overall number of enablers and context-dependent factors compared to food-related and health-related studies, whereas food- and health-focused literature places relatively greater emphasis on barriers. Themes such as trust in data handlers and privacy concerns and data security display a more balanced distribution of barriers and enablers, with notable variation across article types.

Overall, the figures indicate that while similar thematic issues are discussed across food-related, health-related, and general personal data literature, the way these issues are framed, as barriers, enablers, or context-dependent factors, differs by both theme and empirical focus. This highlights the importance of considering both thematic and domain-specific perspectives when interpreting evidence on data-sharing barriers and enablers.

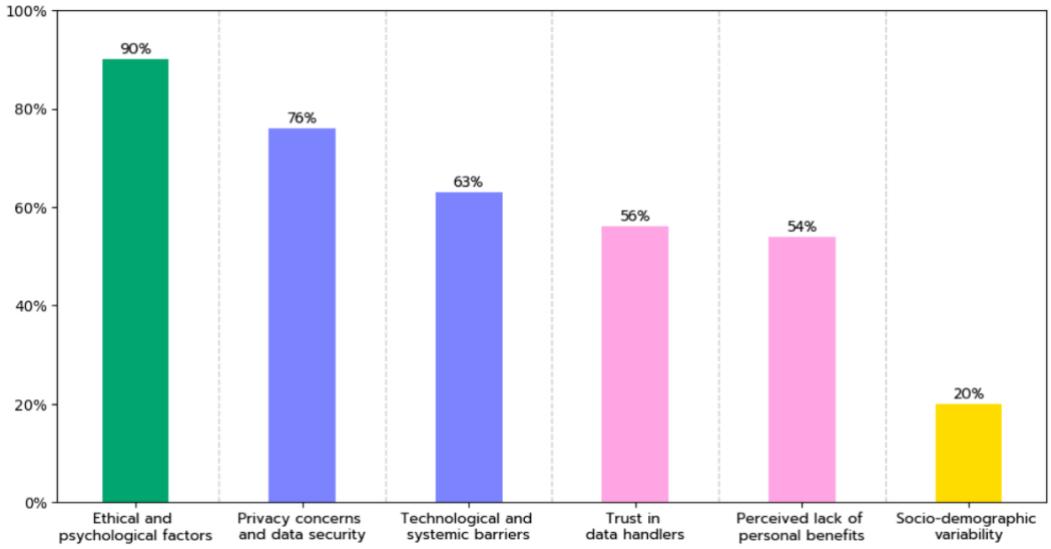

Figure 4: Frequency of different codes across all articles[1]

As shown in **Figure 4**, ethical and psychological factors represent the most frequently occurring coded theme across the reviewed literature, followed by privacy concerns and data security and technological or systemic barriers. These themes account for the largest share of coded segments, indicating that issues related to individual perceptions, motivations, privacy, and technical or structural conditions are most prominently discussed in existing studies on personal data sharing.

Trust in data handlers and the perceived lack of personal benefits are also relatively well represented, with similar frequencies, suggesting that these aspects are regularly considered in the literature, albeit less prominently than ethical, psychological, and privacy-related factors. In contrast, socio-demographic variability is the least frequently coded theme, pointing to comparatively limited attention to how characteristics such as age, education, or cultural background are addressed in relation to data-sharing attitudes.

Overall, the distribution of coded segments reveals an uneven emphasis across thematic areas, with stronger representation of individual-level and system-level considerations and more limited coverage of socio-demographic dimensions. Building on this descriptive overview, the following section moves beyond frequency patterns to examine how the main barriers to sharing food-related personal data are discussed, framed, and evidenced across the literature.

Taken together, the thematic coding indicates that these barriers do not operate in isolation, but cluster around recurring patterns related to individual perceptions and capabilities, technological design and usability, and governance and regulatory conditions. These clusters provide the analytical basis for the higher-level grouping of barriers presented in the next section.

[1] *Colours in above figure do not represent categories indicated for columns*

4.2. Barriers to sharing food-related personal data

Building on the thematic coding of the literature, barriers to sharing food-related personal data can be grouped into three analytically distinct but interrelated domains:

- Human/individual-level barriers
- technological barriers, and
- governance, legal, and structural barriers

An overview of these barriers is presented in **Figure 5**.

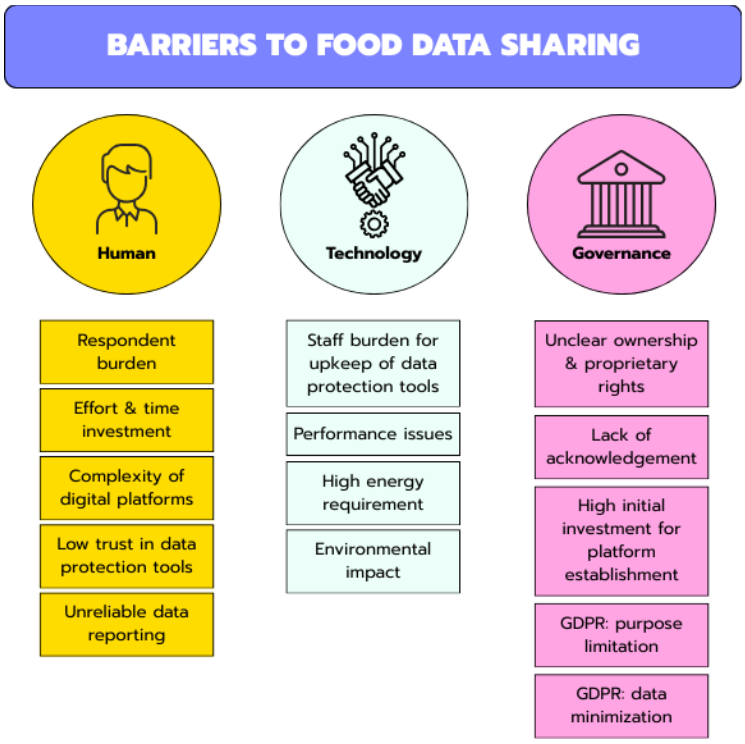

Figure 5: Overview of barriers to sharing food-related personal data

These categories reflect the aggregation of recurring themes identified across studies and are used as an analytical lens to structure the discussion. While conceptually separable, the barriers frequently interact in practice and jointly shape the conditions under which food-related personal data are collected, shared, and reused. The following subsections examine each category in turn. Importantly, the applied categorisation is intended as an analytical device to structure the discussion of barriers identified in the literature, rather than as mutually exclusive or exhaustive categories.

4.2.1. HUMAN/INDIVIDUAL-LEVEL BARRIERS

A substantial body of literature identifies barriers related to the effort, burden, and lived experiences of individuals asked to collect and share food-related personal data. Food journaling and dietary self-reporting are widely recognised as time-consuming activities, with only a small proportion of users sustaining consistent data entry beyond the short term (Cordeiro et al., 2015; Fewings et al., 2022). Complex digital interfaces further exacerbate respondent burden, particularly for users with limited digital skills or when logging home-made meals that require detailed ingredient-level input (Boeschoten et al., 2022; Cordeiro et al., 2015).

High respondent burden is consistently associated with incomplete participation, early drop-out, and reduced continuity in data provision, which in turn limits the feasibility of longitudinal data collection in both research and applied contexts (Maringer et al., 2018). In addition, individuals may experience discomfort, stigma, or fear of judgement when collecting or sharing food-related data, particularly in social or public settings, which can further discourage sustained engagement (Cordeiro et al., 2015).

Beyond effort and emotional burden, the literature also highlights limitations related to users' capacity to provide accurate data. Self-reported food data are susceptible to memory bias, social desirability bias, and inaccuracies in portion-size estimation or ingredient reporting (Donovan et al., 2015; Cordeiro et al., 2015). While food databases and digital aids can support data entry, their coverage is often incomplete, with culturally specific or atypical foods frequently missing (Cordeiro et al., 2015; Maringer et al., 2018). These constraints do not represent barriers to *willingness* per se, but they affect individuals' ability to contribute reliable data and may reduce motivation to engage when data entry is perceived as inaccurate or frustrating.

4.2.2. TECHNOLOGICAL BARRIERS

Technological barriers relate to the design, implementation, and operation of digital systems used to collect, store, process, and protect food-related personal data. From an organisational and system-level perspective, the deployment of privacy-preserving technologies and advanced data protection tools often requires substantial time, specialised technical expertise, and ongoing maintenance. These requirements can place a significant burden on project teams and data controllers, particularly in research projects, pilot initiatives, or smaller organisations with limited technical capacity and financial resources (Durrant et al., 2021; Shaji George & Hovan George, 2022). Regular system updates, monitoring, documentation, and compliance checks further increase operational complexity.

Beyond implementation challenges, technological solutions intended to enhance privacy and security may introduce functional constraints that affect system performance and scalability. Measures such as encryption, anonymisation, or distributed ledger technologies can reduce processing speed, limit real-time data analysis, and complicate interoperability across platforms and datasets (Durrant et al., 2021). These constraints can hinder the integration of food-related personal data into broader research infrastructures or decision-support systems, reducing the practical value of data sharing.

In addition, some privacy-enhancing technologies raise concerns regarding sustainability and feasibility. Blockchain-based solutions, for example, are associated with high energy consumption and infrastructure demands, which may conflict with environmental sustainability objectives and limit their suitability for large-scale or long-term deployment (Durrant et al., 2021).

While these barriers are primarily technological in nature, the literature also notes that technological safeguards do not automatically translate into increased trust or participation. Users often struggle to assess the effectiveness of complex protection mechanisms and may overestimate the capabilities of malicious actors while underestimating the robustness of cryptographic systems (Dechand et al., 2019). As a result, increased technical complexity may fail to yield proportional gains in willingness to share data, reinforcing the need to consider technological barriers in relation to system usability and communication rather than as purely technical challenges.

4.2.3. GOVERNANCE, LEGAL AND STRUCTURAL BARRIERS

Governance-related barriers concern the legal, institutional, and organisational frameworks that shape food-related data sharing practices. Within the European Union, the GDPR establishes strict conditions for the collection, processing, and sharing of personal data. While these provisions are designed to protect individuals' rights, certain principles, most notably purpose limitation and data minimisation, can constrain data reuse and secondary data sharing. Data collected for a specific purpose may not be reused for incompatible purposes, and only data deemed adequate and necessary for a given objective may be processed (Graef et al., 2019).

Beyond regulatory constraints, structural challenges further hinder data sharing across projects and platforms. User-generated food data are often produced in heterogeneous formats, with inconsistent naming conventions and varying levels of granularity, which complicates aggregation and comparison across datasets (Donovan et al., 2025; Maringer et al., 2018). Missing values, multilingual datasets, and divergent documentation practices introduce additional barriers to interoperability and large-scale analysis (van Panhuis et al., 2014).

Unclear arrangements regarding data ownership, access rights, and attribution represent another persistent governance barrier. Intellectual property frameworks may conflict with open data-sharing objectives, and the literature highlights ongoing uncertainty around how ownership and credit for data contributions should be allocated (Donovan et al., 2025). While some individuals express limited concern about ownership, many prefer to retain ownership or shared control over the data they generate (Bietz et al., 2016; Chen et al., 2016). In research contexts, participants may be willing to entrust project teams with data stewardship, but expectations regarding use, reuse, and recognition vary widely (Wiggins & Wilbanks, 2019). Notably, no single, widely accepted governance model for citizen-generated data has emerged in the literature.

Alternative governance approaches, such as data cooperatives, have been proposed to address some of these challenges by enabling collective ownership and negotiated data access (Donovan et al., 2025). However, establishing such models entails substantial barriers,

including high initial investment, technical complexity, and the need to develop robust legal and institutional frameworks before meaningful data sharing can occur (Hafen, 2019).

4.3. Enablers to sharing food-related personal data

Figure 6 provides an overview of the main enablers to sharing food-related personal data identified in the literature. Mirroring the structure adopted for barriers in Section 4.2, these enablers can be grouped into human/individual (user-related), technological, and governance-related enablers. While analytically distinct, these categories often reinforce one another in practice and jointly shape individuals' willingness to engage in food-related data sharing. The following subsections examine each category in more detail.

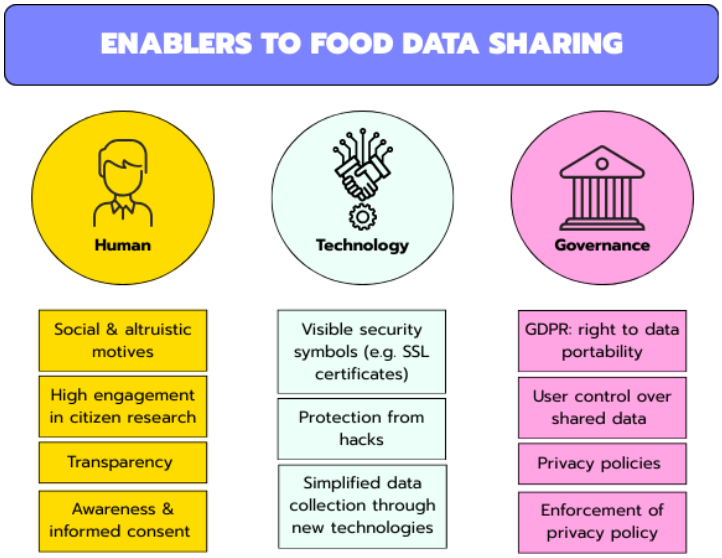

Figure 6: Overview of enablers to sharing food-related personal data

4.3.1. HUMAN/INDIVIDUAL (BEHAVIOURAL AND MOTIVATIONAL) ENABLERS

A substantial body of literature indicates that many individuals are willing to contribute personal data to scientific research, particularly when they perceive clear social or public value. Citizen science initiatives demonstrate high levels of participation, with millions of individuals donating their time, expertise, and data to research projects (Chen et al., 2016; Fewings et al., 2022; Hafen, 2019). In health research contexts, for example, a large proportion of participants express general consent for the use of their personal and even genomic data for research purposes (Hafen, 2019).

Social and altruistic motivations play a central role in this willingness to share data. Individuals are more inclined to contribute their personal data when they believe it will be used for socially

beneficial purposes, such as advancing public health or improving food systems (Clarke et al., 2021; Fewings et al., 2022; Skatova & Goulding, 2019). Engagement is further strengthened when participants find the research topic meaningful or interesting, as opposed to abstract or personally irrelevant studies (Bietz et al., 2016).

Transparency and informed participation are additional human-level enablers. Clearly communicating who will have access to the data, how it will be protected, and for what purposes it will be used can increase participants' confidence in data-sharing arrangements (Clarke et al., 2021). Equally important is ensuring that participants understand the potential implications and risks of data sharing, including possible misuse, which supports informed decision-making and enhances trust (Fewings et al., 2022; Skatova & Goulding, 2019).

4.3.2. TECHNOLOGICAL ENABLERS

Technological enablers relate to the design and functionality of digital systems that facilitate the efficient, secure, and scalable collection and sharing of food-related personal data. Advances in data capture and processing technologies can significantly lower the operational complexity of data collection processes and improve their feasibility in research and participatory contexts. Tools such as barcode scanners, image recognition, voice input, structured food databases, and wireless data transfer interfaces reduce manual data entry requirements and enable more standardised and consistent data capture (Maringer et al., 2018; Fewings et al., 2022). Developments in machine learning and artificial intelligence further enhance the ability to process, integrate, and analyse large and heterogeneous datasets, supporting more timely and robust use of food-related personal data (Donovan et al., 2025).

From a system design perspective, usability and interaction design also function as critical technological enablers. The literature highlights that user experience is not merely a surface feature, but an integral component of data collection systems that can either support or undermine data-sharing processes (Cordeiro et al., 2015). Well-designed interfaces, intuitive workflows, and automation of repetitive tasks contribute to higher data completeness and sustained engagement, whereas poorly designed systems can negate the potential benefits of advanced technical functionalities.

Technologies aimed at enhancing data security and privacy can further enable data sharing by strengthening the overall robustness and credibility of data infrastructures. Privacy-preserving measures, when effectively implemented, reduce the objective risk of data breaches and misuse, thereby addressing a key structural concern in data-sharing systems (Cummings et al., 2021). However, the enabling effect of such technologies depends not only on their technical performance but also on their integration into system architectures in a way that is transparent and verifiable. Research shows that visible and recognisable security features, such as SSL certificates and other trust signals, can increase confidence in digital platforms and support participation in data-sharing initiatives (Dechand et al., 2019; Yadav et al., 2024).

Overall, technological enablers support food-related data sharing by reducing system-level complexity, improving usability and interoperability, and strengthening data protection infrastructures. When these elements are coherently integrated, they create conditions that

make data-sharing systems more reliable, efficient, and acceptable for both project teams and participants.

4.3.3. GOVERNANCE, LEGAL AND STRUCTURAL ENABLERS

Governance, legal, and institutional frameworks can function as important enablers of food-related personal data sharing by establishing clear rules, rights, and accountability mechanisms for data use. Within the European Union, the GDPR provides a structured legal basis for lawful, transparent, and rights-based data sharing. While the regulation introduces constraints under certain conditions, it also creates enabling mechanisms that support responsible data flows and citizen participation.

One key enabling provision is the right to data portability (Article 20 GDPR), which grants individuals the right to obtain machine-readable copies of their personal data and to transfer them across services. This legal instrument facilitates the reuse of data already collected by third parties and enables individuals to contribute aggregated datasets to research or citizen science initiatives without duplicating data collection efforts (Hafen, 2019; Fewings et al., 2022). In practice, many digital platforms, smartphone systems, search engines, and financial institutions operationalise this right through data download packages (DDPs), which can serve as a valuable structural resource for research-oriented data sharing (Boeschoten et al., 2022).

Beyond formal legal rights, governance arrangements that embed transparency, accountability, and controllability into data-sharing processes further enable participation. Organisational practices that clearly define data access conditions, usage purposes, and retention periods help reduce uncertainty and establish predictable data-sharing environments. Mechanisms such as opt-in and opt-out options, data deletion rights, and traceability of data access support compliance with governance requirements while strengthening the overall integrity of data infrastructures (Ackermann et al., 2022; Frey et al., 2017; Weydert et al., 2019; Yadav et al., 2024).

Clear and accessible privacy policies constitute an additional governance-level enabler. When policies are written in understandable language and include enforcement provisions specifying sanctions for misuse, they operationalise legal safeguards and enhance the credibility of data-sharing arrangements (Chang et al., 2018). Collectively, these governance and legal enablers contribute to more stable, transparent, and trustworthy data-sharing ecosystems, creating conditions under which food-related personal data can be shared in a responsible and sustainable manner.

4.4. Context-dependent factors

In addition to clearly identifiable barriers and enablers, the literature highlights a set of factors whose influence on willingness to share food-related personal data is highly context-dependent. These factors do not consistently function as barriers or enablers in isolation; rather, their effects vary depending on individual characteristics, institutional arrangements,

data types, and usage contexts. The following subsections examine key context-dependent factors identified in the literature.

4.4.1. PRIVACY CONCERN LEVELS

Privacy concerns play a central role in shaping data-sharing decisions, but their influence varies considerably across individuals and contexts. Wenz et al. (2019) found that respondents exhibit a 31.4% lower predicted probability of completing data-sharing tasks perceived as threatening to privacy. Data sharing can be experienced as intrusive and is sometimes framed as a "big brother" scenario, particularly when monitoring or surveillance is implied (Clarke et al., 2021). As a result, privacy assurance is a prerequisite for data sharing for many participants, especially when contributing to public scientific databases (Chen et al., 2016).

However, privacy concerns are not uniform. Only a minority of individuals hold fixed positions, either consistently refusing to share data or sharing data unconditionally. The majority adopt more flexible, context-dependent positions (Grande et al., 2022). Jai and King (2016) identify approximately 55% of individuals as "privacy pragmatists", who weigh perceived risks, fairness of information exchange, and trust in the specific organisation or sector involved before deciding whether to share data. In contrast, around 25% are "privacy fundamentalists", who place a very high value on privacy and rarely share data, while approximately 20% are "privacy unconcerned" and exhibit few reservations about data sharing (Jai & King, 2016). These distinctions underline the importance of situational factors in shaping privacy-related decisions.

4.4.2. TRUST IN DATA HANDLERS

Trust in the entity collecting and managing data represents another critical context-dependent factor. Low trust can amplify concerns about misinterpretation, misuse, or intentional abuse of personal data (van Panhuis et al., 2014). Individuals tend to be particularly sceptical of service providers perceived to benefit commercially from data misuse, such as through targeted advertising or secondary data sales (Berezowska et al., 2014; Yadav et al., 2024).

Trust levels vary systematically across sectors. For example, health-related organisations and professionals, as well as academic institutions, are generally perceived as more trustworthy data handlers (Bietz et al., 2016; Donovan et al., 2025). In contrast, commercial actors are often viewed with greater suspicion, even when data collection is framed as contributing to research or innovation (Bietz et al., 2016; Donovan et al., 2025; Hirst et al., 2023). These sectoral differences highlight that trust is relational and institution-specific, rather than a fixed individual trait.

4.4.3. EFFECTS OF PAST EXPERIENCES

Past experiences with data sharing and privacy breaches influence future behaviour, but not always in intuitive ways. Individuals who have previously experienced data misuse or privacy violations are not necessarily less willing to share data in subsequent contexts (Hirst et al., 2023). In some studies, such individuals were even more willing to share data for health research, potentially reflecting greater awareness of risks rather than heightened aversion (Hirst et al., 2023).

At the same time, organisational track records appear to play a decisive role in shaping data-sharing decisions. Empirical evidence shows that 69% of individuals report avoiding brands or services that have experienced recent data breaches (Yadav et al., 2024). This finding suggests that negative experiences related to data misuse are more likely to undermine trust in data-handling institutions than to reduce individuals' general willingness to engage in data sharing per se. In this sense, the perceived reliability and accountability of the data-collecting actor's past behaviour appears more influential than the prior experiences of the individual sharing their data.

4.4.4. WHAT, HOW, AND WHY DATA ARE COLLECTED

As described above, willingness to share personal data is strongly shaped by perceptions of what data are collected, how collection occurs, and for what purpose. Studies show that certain data types, such as financial, medical, or location (GPS) data, are widely regarded as more sensitive than demographic information, activity data, or purchase histories (Ackermann et al., 2022; Bietz et al., 2016; Cummings et al., 2021; De Schaepdrijver et al., 2022). As perceived intrusiveness increases, perceived privacy risks rise and willingness to share tends to decline (Donovan et al., 2025).

Data collection modality also matters. Individuals generally exhibit higher willingness to share data when collection is active (i.e. consciously submitted by users) rather than passive (i.e. automatically captured) (Roeber et al., 2015; Wenz et al., 2019). Tasks requiring the installation of dedicated applications are associated with lower participation rates than those that do not impose additional technical requirements (Wenz et al., 2019).

Purpose further shapes acceptance. Across studies, participants consistently report greater willingness to share data for research or public-interest purposes than for commercial use, toward which many express scepticism or aversion (Bietz et al., 2016; Chen et al., 2016). Data sharing is also more readily accepted when it aligns with "appropriate information flows", meaning that data are used in ways participants consider legitimate and expected. Concerns intensify when data collection appears excessive or irrelevant to the stated purpose (Ackermann et al., 2022; Cummings et al., 2021; Li et al., 2010).

4.4.5. SOCIO-DEMOGRAPHIC VARIABILITY

Socio-demographic characteristics influence data-sharing attitudes in complex and context-dependent ways. Cultural factors play a role: Schumacher et al. (2022) found higher willingness to share personal data in countries characterised by high power distance, potentially reflecting greater acceptance of institutional authority. Conversely, individuals in cultures with strong long-term orientation tend to share less personal information (Schumacher et al., 2022).

Gender and age differences are also observed. Men are generally more willing to share data for research purposes than women (Ackermann et al., 2022; Hirst et al., 2023; Jai & King, 2016), while increasing age is associated with lower willingness to share personal data (Ackermann et al., 2022; Hirst et al., 2023). These patterns may be partially mediated by differences in digital literacy and technology use, as more intensive device users tend to exhibit greater openness to data sharing (Wenz et al., 2019).

Socio-economic and demographic differences further add complexity to patterns of data-sharing behaviour. Studies indicate that individuals from historically marginalised racial or ethnic backgrounds and those from lower-income households often report heightened concerns about digital privacy, particularly in relation to risks such as identity theft or government surveillance (Grande et al., 2022). However, these concerns do not consistently translate into lower willingness to share personal data. In certain research and commercial contexts, these groups have been found to exhibit equal or higher willingness to share personal data, while individuals from more socio-economically advantaged backgrounds may express stronger general privacy concerns (Grande et al., 2022; Hirst et al., 2023). This highlights the importance of interpreting socio-demographic differences as context-dependent influences rather than as deterministic predictors of data-sharing behaviour.

4.5. Synthesis of literature findings and implications for empirical validation

Across the reviewed literature, a recurring pattern emerges: while stated willingness to share personal data for research purposes, particularly when associated with social or scientific benefits, is often high, actual participation levels tend to be lower. This discrepancy reflects the cumulative influence of human, technological, governance-related, and context-dependent factors identified in Sections 4.2 to 4.4.

User-level barriers such as time constraints, perceived effort, limited digital skills, and concerns related to privacy and data security frequently constrain sustained engagement, even among individuals who express positive attitudes toward data sharing. At the same time, the literature highlights the potential of technological solutions, such as automated data capture, barcode scanning, and image recognition, to reduce respondent burden, provided that these tools are accessible, transparent, and aligned with users' capabilities.

Trust consistently emerges as a central cross-cutting factor shaping data-sharing behaviour. Transparent communication about data collection, storage, use, and protection, along with the provision of meaningful user control mechanisms, is associated with higher willingness to share data. Conversely, unclear data-use purposes, limited transparency, or a history of data breaches can undermine participation, even among individuals who are otherwise open to data sharing.

Taken together, these findings suggest that high stated willingness to participate in research does not automatically translate into sustained engagement. Empirical validation is therefore required to examine how these literature-identified factors are experienced, prioritised, and negotiated by citizens in specific local and project contexts. Section 5 addresses this need by validating the literature-based insights through focus group discussions conducted within each SPOON CSLs.

5. VALIDATION THROUGH FOCUS GROUPS

5.1. Objective and rationale for validation

The focus groups conducted within the SPOON CSLs served to empirically validate the findings of the scoping literature review by examining how identified barriers, enablers, and context-dependent factors are experienced and interpreted by citizens. While the literature synthesis provides a conceptual understanding of factors influencing the sharing of food-related personal data, the focus groups enable an assessment of how these factors are perceived, prioritised, and negotiated in practice.

Through moderated group discussions, participants reflected on issues related to data sharing, privacy, trust, and governance from their own perspectives, allowing literature-based insights to be examined in light of locally situated experiences. This approach strengthens the empirical relevance of the research by complementing theoretical findings with qualitative evidence and by providing a more nuanced understanding of how general patterns identified in the literature manifest across diverse social and practical contexts.

5.2. Design and implementation in the CSLs

The focus group discussions were designed to elicit participant perspectives relevant to the research questions and to validate key findings from the literature review. Each session addressed four thematic areas aligned with the analytical framework developed in Section 4: (i) barriers and concerns related to sharing food-related personal data, (ii) knowledge and perceptions of data protection and privacy, (iii) governance arrangements and potential solutions, and (iv) motivations and incentives for data sharing.

Each CSL convened between six and twelve participants, a group size selected to facilitate interactive discussion while ensuring diversity in gender, age, occupational background, and levels of digital literacy. Focus groups were conducted using a standardised discussion guide to ensure consistency across CSL locations, while retaining flexibility for participants to raise context-specific issues.

Data collection took place through structured, moderated discussions. Each session was facilitated by one or more moderators, supported by a designated note taker who documented key contributions and discussion dynamics using a standardised Focus Group Summary Template. Following each session, facilitators synthesised the inputs into a structured summary report, including anonymised illustrative quotes and a concise overview of main findings. Where relevant, supporting materials were archived. This process enabled systematic comparison across CSLs and provided a consistent qualitative evidence base for subsequent analysis and reporting.

5.3. Key results and validation of literature insights

5.3.1. EXPLORING FAMILIARITY AND EVERYDAY CONTEXTS

Across all CSLs, participants reported routinely providing a wide range of personal information when using food-, health-, or shopping-related applications and websites. Most commonly shared data included basic personal details such as name, age, address, email address, and phone number. Attitudes toward data sharing varied considerably: some participants reported a preference for sharing only the minimum information required, while others indicated that they typically share all requested data, perceiving this as a normal and unavoidable aspect of digital service use.

Information perceived as relevant and beneficial, such as dietary preferences, allergies, intolerances, or purchase history, was generally shared more readily, particularly when it enabled convenience, discounts, or personalised services. In contrast, GPS location data and financial information were consistently perceived as more sensitive. In the Valencia focus group in particular, concerns about card fraud heightened reluctance to share payment-related data.

Overall, these findings closely align with the literature regarding perceived sensitivity of different data types (Ackermann et al., 2022; Bietz et al., 2016; Cummings et al., 2021; De Schaepdrijver et al., 2022) and the variability of privacy attitudes across individuals (Grande et al., 2022; Jai & King, 2016). Most participants displayed characteristics of “privacy pragmatists”, weighing perceived benefits against potential risks, while smaller groups reflected “privacy fundamentalist” or “privacy unconcerned” orientations.

Across all CSLs, participants reported that they rarely read privacy policies, cookie notices, or detailed information about data use, primarily because such information was perceived as overly long, complex, and difficult to understand. Only a few isolated cases reported reading these materials, mainly out of curiosity or to better understand how data might be used.

Decisions to accept or decline data sharing permissions varied widely. Some participants reported routinely declining permissions, others allowing only what they considered necessary, and others approving permissions they deemed important.

These patterns align with existing literature on trust and distrust in data sharing, particularly regarding aversion to commercial data use (Berezowska et al., 2014; Yadav et al., 2024) and resistance to the collection of irrelevant personal data (Ackermann et al., 2022; Cummings et al., 2021; Li et al., 2010). The motivating role of contributing to research or a meaningful purpose also strongly reflects findings in the literature (Clarke et al., 2021; Fewings et al., 2022; Skatova & Goulding, 2019).

When asked whether they felt able to remain in control of what happens to their data once shared, the majority of participants across all CSLs responded negatively. Many described data sharing as effectively irreversible *(“once it’s out, it’s out”)* and reported difficulty maintaining an overview of how their data are used. While some participants occasionally made use of unsubscribing mechanisms, many were unsure of their effectiveness. Others

were aware of legal rights to delete or withdraw data but did not know how to exercise them. Overall, participants expressed a sense of "digital resignation", describing data collection as pervasive and difficult to avoid in everyday life.

5.3.2. EXPLORING BARRIERS AND CONCERNS

Perceptions of the sensitivity of food-related data varied across CSLs. Participants in Thessaloniki and Turin generally viewed food data as not sensitive, while participants from Braunschweig and Bruges considered it "not too sensitive". In contrast, participants from the Pomurje region and Valencia were the only groups to describe food data as potentially "too personal".

Context emerged as a key moderating factor. Participants across CSLs reported a generally positive attitude toward sharing food-related data for research purposes. However, some concerns were highly situational. A participant from Bruges emphasised discomfort with sharing information about their child, while participants in Braunschweig highlighted that calorie intake data could be problematic for individuals with eating disorders. Participants from Valencia expressed concerns about being judged based on their food consumption habits.

Practical barriers related to data collection were also raised. In Braunschweig and Valencia, participants expressed concern about the burden of collecting and sharing data on a daily basis. In the Braunschweig CSL, participants suggested that a data collection period of approximately two weeks might be manageable, whereas longer durations would become tedious. Community-building was mentioned as a potential mitigating factor. Participants from Braunschweig also noted that collecting data while eating - particularly in social settings - could feel inappropriate. Participants from Valencia emphasised the importance of convenience, favouring automated solutions such as receipt scanning and AI-based analysis over manual form completion. They also stressed the value of objectivity in data collection, particularly to reduce bias and reliance on self-perception. These concerns strongly align with barriers identified in the literature, particularly regarding effort and time investment leading to high drop-out rates (Cordeiro et al., 2015) and issues of data reliability related to participant bias (Cordeiro et al., 2015). However, barriers related to eating disorders or sharing data about children were not prominently discussed in the reviewed literature.

Participants in Braunschweig, Bruges, Turin and Thessaloniki also reported greater openness to data sharing when clear added value was provided, including feedback, benefits, or recommendations. Examples included advice on reducing food waste, optimising fridge inventories, improving personalised health guidance, in-store services, vouchers, and discounts. These forms of added value were not strongly emphasised in the literature, indicating a potential gap.

Concerns about sharing data with unknown individuals were also raised, particularly in the Braunschweig and Pomurje CSLs. Braunschweig participants suggested that personal relationships with evaluators could alleviate such concerns. Across all CSLs, participants expressed higher willingness to share data when the data type was directly related to the stated purpose, and lower willingness when data collection appeared irrelevant. This aligns with

literature on appropriate information flows (Ackermann et al., 2022; Cummings et al., 2021; Li et al., 2010).

The most prominent concerns reported across CSLs related to data misuse, loss of control, and profiling. Data misuse referred to fears that data would be sold to third parties or used for unintended purposes. Loss of control reflected perceptions that data become irreversible once shared, with limited transparency about subsequent use. Profiling concerns centred on the use of eating habits to influence purchasing behaviour, particularly toward unhealthy consumption. Participants in the Turin and Bruges CSLs additionally mentioned risks of hacking or data breaches.

Trust emerged as a key contextual factor shaping willingness to share. Familiarity with, and prior knowledge of, the data-collecting entity increased perceived trustworthiness. Research institutions were consistently identified as the most trusted actors, viewed as objective, ethically bound, and not profit-driven. Trust in public authorities and governments was mixed: while they were seen as relatively objective, concerns were raised about security breaches and inconsistent accountability. Commercial entities were viewed as least trustworthy due to fears of data misuse, although some participants in Bruges acknowledged benefits of targeted services, and participants in Turin noted that smaller companies might be perceived as less attractive targets for data breaches. These findings closely align with literature on sector-based trust differentiation (Bietz et al., 2016; Donovan et al., 2025).

Experiences with data breaches varied across CSLs. Participants in the Pomurje region, Valencia, and Turin reported fewer experiences than those in Braunschweig, Bruges, and Thessaloniki. Reported incidents included targeted advertising, spam communications, account hacking, fraudulent banking activity, and phishing attempts. These experiences increased caution and adoption of additional security measures but did not lead to complete refusal of data sharing, which was widely perceived as unavoidable for everyday convenience. This aligns with literature indicating that past breaches increase caution rather than eliminate data sharing behaviour (Hirst et al., 2023), alongside avoidance of brands with a history of breaches (Yadav et al., 2024).

5.3.3. EXPLORING MOTIVATIONS AND INCENTIVES

Participants across all CSLs reported that willingness to share food-related personal data increased when clear benefits were perceived. Financial incentives, such as personalised benefits such as discounts or rewards, or personalised vouchers, were frequently mentioned as strong motivators, though some participants noted that such incentives could attract primarily money-driven participation, potentially affecting data quality. At the same time, financial incentives were seen as useful for engaging vulnerable or hard-to-reach groups.

Non-monetary benefits were viewed as equally important. Participants in all CSLs highlighted benefits such as gaining insight into personal eating habits, improving health, reducing food waste, saving money, discovering new recipes, and social interaction through project participation.

Beyond personal benefits, social and altruistic motivations played a significant role. Participants from Braunschweig, Bruges, the Pomurje region and Thessaloniki expressed

motivation to contribute to research, assing in a soceital cause, support the greater good, and engage in projects perceived as meaningful or interesting. Trust and control were identified as critical preconditions: participants wanted transparency about data use, assurance against misuse, and the ability to choose which data to provide. A simple, low-effort data collection process was also highlighted as a key enabler of participation.

Comparison with the literature revealed partial divergence regarding financial incentives. Participants did not express concerns that monetary rewards might signal commercial exploitation, as suggested by Weydert et al. (2019), though this may reflect the framing of the discussion. The focus groups also identified additional enablers not strongly emphasised in the literature, particularly the importance of clear added value and personal relationships with data collectors. At the same time, strong alignment was observed with literature on altruistic motivations (Clarke et al., 2021; Fewings et al., 2022; Skatova & Goulding, 2019) and the role of trust, transparency, and control (Ackermann et al., 2022; Clarke et al., 2021; Frey et al., 2017; Weydert et al., 2019; Yadav et al., 2024).

When asked whether different social groups might hold different views on data sharing, participants in the Pomurje region expressed discomfort with making assumptions. In contrast, participants in other CSLs commonly perceived generational differences. Younger people and students were seen as more willing to share data, often perceiving data sharing as an unavoidable aspect of digital life. Older adults were viewed as more sceptical, though potentially more vulnerable to fraud due to lower familiarity with digital risks. Education level and digital literacy were frequently cited as key factors shaping these attitudes. These findings align well with existing literature on age, education, and digital literacy (Ackermann et al., 2022; Hirst et al., 2023; Wenz et al., 2019). An additional factor emerging from the focus groups was the reluctance of individuals with eating disorders or specific medical conditions to share food-related data, reflecting heightened sensitivity around personal health information that is less explicitly discussed in prior research.

5.3.4. EXPLORING KNOWLEDGE AND PERCEPTIONS OF DATA PROTECTION

Participants across all CSLs demonstrated highly uneven familiarity with data-protection technologies. Anonymisation was the most widely recognised concept; however, even where participants reported having heard the term, understanding was often superficial. In the Pomurje region, several participants stated explicitly that they were unable to explain what anonymisation entails despite recognising the term. Encryption was generally understood only in broad terms and was most often associated with securing messages in applications such as WhatsApp or Signal, commonly described as “scrambling” content. Blockchain was by far the least understood technology: most participants had either never heard of it or were unable to explain its meaning, with only a small number expressing confidence in their understanding.

Overall, participants from all CSLs frequently reported recognising technical terminology without having a clear understanding of how the technologies function or how effective they are in practice. Familiarity varied considerably both within and across CSLs, a pattern that closely aligns with the literature (Bietz et al., 2016; Cummings et al., 2021; Dechand et al., 2019; Frey et al., 2017).

Awareness that data would be anonymised or encrypted generally increased participants' comfort with data sharing, as these measures were perceived to reduce risks such as identity theft, personalised misuse, spam, or unwanted contact. Participants in Braunschweig, Bruges, and Valencia reported particularly strong increases in comfort when anonymisation and encryption were mentioned. In contrast, participants in Pomurje and Turin expressed noticeably greater hesitation, while responses in Thessaloniki were mixed.

Several reasons for this hesitation were articulated. Participants reported doubts about their own understanding of the technologies, uncertainty about who ultimately has access to the data, concerns that supposedly anonymised data could still be re-identified, and fears that data might be sold or linked with other datasets. As a result, technical safeguards alone were not considered sufficient. Instead, the perceived purpose of data collection and the trustworthiness of the data-handling entity remained more influential determinants of comfort than the presence of technical protection measures. This pattern is consistent with the literature, which shows that data-protection technologies can improve comfort only partially, with lack of understanding and uncertainty remaining key limiting factors (Cummings et al., 2021; Dechand et al., 2019).

To feel confident that their data are genuinely protected, participants emphasised the importance of transparency and control. They expressed a strong preference for short, clear, and non-legalistic explanations of what data are collected, who processes them, and for what purpose, as well as feedback on how their data are used. Control mechanisms, such as the ability to view, delete, and periodically reauthorise data use, were described as essential and should be easy to access and understand. These expectations align closely with the literature (Ackermann et al., 2022; Clarke et al., 2021; Frey et al., 2017; Weydert et al., 2019; Yadav et al., 2024). However, the emphasis on clarity, simplicity, and understandable language emerged more strongly from the focus groups than from the reviewed literature.

Visible security cues, such as shields, logos, or CAPTCHAs, were perceived as offering an immediate sense of protection, although some participants expressed scepticism and viewed these cues as potentially superficial. Ethical guarantees were therefore considered equally important. Participants highlighted the need for explicit commitments to recognised standards (e.g. GDPR or ISO norms), clear prohibitions on selling or sharing data with third parties, and full accountability in the event of misuse. These views are consistent with the literature on visible security symbols (Yadav et al., 2024) and the importance of enforcement clauses in privacy policies (Chang et al., 2018).

Notably, in the Pomurje region, a small number of participants stated that no explanation or technical safeguard would convince them that their data are safe, reflecting a fundamentally distrustful stance. In all other CSLs, however, the proposed transparency, control, and accountability measures were generally viewed as sufficient to increase comfort with data sharing.

5.3.5. EXPLORING GOVERNANCE AND SOLUTIONS

Participants articulated governance-related expectations largely in response to the concerns and needs identified in the preceding sections.

A sense of control over personal data was consistently associated with transparent and accessible governance structures. Participants from all CSLs except Valencia emphasised the need for clear oversight of data flows, including visibility over which organisations hold their data, for what purposes, and for how long. Several participants from Bruges and Thessaloniki suggested the idea of a "digital wallet" or central overview mechanism that would consolidate this information. Regular reporting by data-collecting organisations and explicit statements of purpose were also viewed as important governance tools. These expectations align with the literature, which identifies transparency as a key enabler of trust and willingness to share data (Ackermann et al., 2022; Clarke et al., 2021; Frey et al., 2017; Weydert et al., 2019; Yadav et al., 2024).

Participants from Braunschweig further expressed a preference for centralised and user-friendly data management systems, as opposed to fragmented arrangements across multiple providers. Simple and intuitive interfaces were considered essential by participants from Bruges, the Pomurje region and Thessaloniki to make governance mechanisms workable in everyday life. While this aspect is less prominently discussed in the literature, it is not contradicted by existing findings and reflects practical usability concerns raised by focus groups' participants. Additionally, control-related governance mechanisms were discussed in concrete terms. Participants highlighted the importance of being able to select which data are shared, approve who can access them, define access duration, and withdraw or delete data at any time. Periodic re-approval of data use was suggested as a safeguard against forgotten or passive consent. These expectations closely mirror findings in the literature on the importance of user control in data-sharing governance (Ackermann et al., 2022; Clarke et al., 2021; Frey et al., 2017; Weydert et al., 2019; Yadav et al., 2024).

Accountability emerged as a further governance requirement. Participants from all CSLs emphasised that organisations collecting data should provide explicit guarantees that data will only be used for the stated purposes. Clear sanctions for misuse or breaches were seen as necessary to ensure credibility and trust. This aligns with literature highlighting the role of enforcement clauses and accountability mechanisms in privacy governance (Chang et al., 2018).

When discussing collective or cooperative data governance models, responses were cautiously positive. Many participants appreciated the idea that citizens could collectively influence how data are used, particularly to ensure societal or communal benefits rather than purely commercial exploitation. At the same time, scepticism was expressed regarding the feasibility of such models, often due to limited familiarity, perceived complexity, or doubts about decision-making in large groups. Familiarity with data cooperatives was generally low, especially in the Turin and Valencia CSLs.

Finally, participants from all CSLs reiterated the importance of clear rules and safeguards within governance frameworks. They called for explicit use limitations without hidden or overly complex terms, simple mechanisms for withdrawing consent, default data deletion unless consent is renewed, and demonstrable data security. These expectations reinforce earlier findings and align with the literature on transparency, enforcement, and data protection as foundations of trustworthy data governance (Ackermann et al., 2022; Bietz et al., 2016; Cummings et al., 2021; Dechand et al., 2019; Frey et al., 2017).

6. STRATEGIES TO ADDRESS BARRIES AND STRENGHTEN ENABLING CONDITIONS

While the literature review and focus group validation identified a wide range of barriers to food-related personal data sharing, they also highlight actionable strategies that can help reduce these barriers and strengthen enabling conditions. Building on the barriers, enablers, and contextual factors identified in the scoping literature review (Section 4) and empirically validated through focus group discussions in the CSLs (Section 5), this section outlines actionable strategies to enhance willingness to share food-related personal data. The proposed solutions reflect both established academic evidence and citizens' lived experiences, expectations, and concerns, and are structured across technical, governance, incentive-based, and policy-oriented dimensions.

6.1. Technical & digital solutions

Technical and digital solutions can play a key role in reducing barriers to food-related personal data sharing by lowering participant burden, strengthening data protection, and increasing perceived safety. Evidence from both the literature and focus group discussions indicates, however, that such solutions are most effective when their practical benefits are clearly communicated and directly aligned with participants' concrete concerns, such as misuse, loss of control, or unauthorised access.

Focus group discussions revealed that participants' willingness to share food-related personal data is only partly driven by the presence of technical privacy safeguards alone. Many participants reported limited understanding of data protection technologies and expressed scepticism toward complex or opaque solutions. As a result, technical measures were perceived as meaningful primarily when their effects were tangible and easy to grasp. Consistent with the literature, guaranteeing anonymity has been shown to increase willingness to share data (Ackermann et al., 2022; Chen et al., 2016; Roeber et al., 2015). At the same time, participants echoed concerns that anonymisation alone does not fully prevent re-identification, particularly when datasets are linked across sources or over time (Bietz et al., 2016). These findings suggest that effective privacy protection requires combining anonymisation with additional safeguards, while also attending to user perceptions and perceived safety.

Blockchain (BC): BC-based systems can enhance data integrity by recording information across multiple devices, thereby reducing the risk of retroactive tampering (Frey et al., 2017; Lei et al., 2022). When combined with secure multiparty computation (SMC), BC can enable data processing without granting direct data access to involved parties (Frey et al., 2017; Lei et al., 2022). For users who understand these mechanisms, BC protection has been associated with substantially higher comfort in sharing personal data. However, less than 20% of

individuals report familiarity with BC as a privacy method (Frey et al., 2017). This lack of familiarity was strongly reflected in the focus groups, where most participants were unable to explain BC or distinguish it from other digital technologies, and several indicated that unfamiliar terminology reduced trust rather than increased it. While BC combined with monetary rewards has been shown to outperform standard privacy policies (Frey et al., 2017), these findings underline that BC's enabling potential depends heavily on communication, framing, and user comprehension.

Differential privacy (DP): DP protects individuals by introducing carefully calibrated noise into datasets, preserving aggregate insights while obscuring individual data points (Cummings et al., 2021; Lei et al., 2022). In principle, DP offers strong statistical privacy guarantees, but its mathematical formulation and parameter-based logic limit accessibility for non-technical users (Cummings et al., 2021). Empirical studies show that merely informing users that DP is applied has little effect on willingness to share data, likely due to low understanding (Cummings et al., 2021). Focus group participants similarly emphasised that abstract or highly technical explanations did not increase confidence and that uncertainty about how protections operate often outweighed their potential reassurance. Where DP is used, its enabling effect therefore depends on either building participant understanding (e.g. through training) or reframing explanations to emphasise concrete outcomes rather than technical detail.

Encryption: Encryption converts readable plaintext into ciphertext that can only be decoded with an appropriate key, and advanced forms such as homomorphic encryption allow certain operations to be performed on encrypted data (Lei et al., 2022; Shaji George & Hovan George, 2022). Compared to other privacy-preserving approaches, encryption is relatively easier to explain, yet distrust remains widespread. Focus group discussions revealed persistent scepticism, often rooted in perceptions that encryption can be easily bypassed. This aligns with evidence that individuals tend to overestimate hackers' capabilities while underestimating the robustness of encryption (Dechand et al., 2019). Uncertainty about who holds the encryption key, and thus access to the data, may further undermine trust (Dechand et al., 2019), indicating that governance arrangements around encryption are as important as the technology itself.

Federated learning (FL) and zero-knowledge proofs (ZKP): FL enables joint data processing or machine learning without raw data leaving local environments, while ZKPs allow verification of information without revealing the information itself (Lei et al., 2022; Qian et al., 2023). These approaches offer promising privacy-preserving capabilities, but are technically complex and remain largely unfamiliar to lay users. The literature provides limited evidence on how users perceive these methods or whether they directly increase willingness to share data. This gap mirrors focus group findings, where participants generally expressed discomfort with unfamiliar or opaque technical solutions, suggesting that such methods may only function as enablers when embedded within clear governance and communication frameworks.

Implications for implementation and communication: Taken together, the literature and focus group findings indicate that technical privacy protection measures are a necessary but insufficient condition for increasing willingness to share food-related personal data. Users frequently misjudge digital risks (Dechand et al., 2019), which implies that communication

strategies can be as important as technical choices. Explaining the effects of safeguards, such as reduced risks of hacking or misuse, has been shown to be more persuasive than explaining technical mechanisms (Cummings et al., 2021), a finding strongly confirmed in the focus groups. Visible security cues, such as SSL certificates or recognisable trust symbols, can further strengthen perceived trustworthiness (Yadav et al., 2024).

Operational considerations: Implementing and maintaining privacy-protection tools requires substantial time, resources, and ongoing effort (Durrant et al., 2021; Shaji George & Hovan George, 2022). In some cases, privacy-preserving systems may also reduce processing speed or limit real-time data analysis (Durrant et al., 2021). BC and similar approaches can entail environmental trade-offs due to high energy and water requirements (Durrant et al., 2021). While focus group participants did not explicitly raise environmental concerns, they repeatedly emphasised proportionality, suggesting that technical solutions are most acceptable when their perceived benefits clearly outweigh their complexity and costs.

6.2. Governance and ownership models

Governance arrangements and data ownership models constitute a central lever for enabling food-related personal data sharing, particularly by shaping trust, perceived legitimacy, and accountability. Focus group discussions repeatedly highlighted that willingness to share personal data depends not only on technical safeguards, but also on clear and understandable rules regarding who controls the data, for what purposes it may be used, and how misuse is prevented and sanctioned. These empirical insights provide important context for interpreting governance mechanisms discussed in the literature.

In the European Union, the GDPR is one of the most important frameworks governing data privacy and protection. The GDPR comprises a set of complex and interplaying mechanisms that can both incentivise and limit data sharing (Graef et al., 2019). Key elements that may constrain data sharing include purpose limitation and data minimisation. Purpose limitation requires that data collected for a specific purpose cannot be reused in ways that are incompatible with that original purpose, while data minimisation stipulates that only data that are adequate, relevant, and necessary for a defined purpose may be processed (Graef et al., 2019). From a governance perspective, these principles require careful ex ante consideration of data collection objectives and data needs, a point that aligns with focus group participants' emphasis on relevance and proportionality in data requests.

At the same time, GDPR can strongly incentivise data sharing through several mechanisms. First, GDPR compliance itself can enhance trust and increase willingness to share personal data (Yadav et al., 2024), a finding echoed across focus groups, where participants associated formal regulatory frameworks with greater accountability. Second, Article 20 of the GDPR ("right to data portability") entitles citizens to obtain machine-readable copies of their personal data, enabling them to actively contribute to research by making aggregated datasets accessible (Hafen, 2019; Fewings et al., 2022). Most private data-processing entities, such as media platforms, smartphone systems, search engines, photo storage services, email providers, and banks, comply with this right by offering data download packages (DDPs) to data

subjects, which could represent a valuable resource for research purposes (Boeschoten et al., 2022). Focus group discussions, however, revealed limited awareness of this right and uncertainty about how such data could be meaningfully reused, highlighting the need for clearer guidance and facilitation.

Providing a privacy policy has been shown to significantly increase willingness to share data, particularly when policies are simple and understandable (Yadav et al., 2024). Users are least willing to share data when no privacy policy is provided (Frey et al., 2017). Privacy policies are perceived as most effective when they include an enforcement clause, which specifies how data may be used and outlines sanctions in case of misuse (Chang et al., 2018). Additionally, users value organisations' efforts to clearly communicate information practices and allow individuals to access, modify, or withdraw their data, further enhancing trust (Chang et al., 2018). Focus group discussions strongly reinforced these findings, with participants repeatedly calling for clear, non-legalistic explanations and explicit guarantees against secondary or commercial data use.

Regarding data ownership models, emerging research has explored the concept of a "data cooperative" (Donovan et al., 2025; Hafen, 2019). In this model, participants' data are collectively owned and governed by citizens. Data may be made available for public research or commercial use, but governance arrangements are designed to safeguard individual privacy and ensure fair use (Donovan et al., 2025). Operationally, data cooperatives rely on secure IT platforms that allow individuals to store, manage, and control access to their data copies (Hafen, 2019). Unlike many existing systems, where administrators retain broad access rights, each data record in a personal data platform would be accessible only to its proprietor (Hafen, 2019). When participants choose to share data for research, the cooperative's management negotiates access conditions with researchers or other entities, aiming to ensure fairness and transparency (Hafen, 2019).

Focus group responses reflected cautious interest in such collective governance models. While many participants appreciated the idea of citizens jointly deciding how their data are used - particularly to support societal or research goals - others expressed scepticism or disengagement, often due to perceived complexity, time requirements, and uncertainty about feasibility. These concerns align with literature-identified barriers, including the high upfront investment required to establish secure platforms, develop initial user-facing services, and create robust legal and governance frameworks (Hafen, 2019).

6.3. Incentives and trust-building mechanisms

Incentives and trust-building mechanisms can actively support willingness to share food-related personal data when they are designed in ways that reinforce transparency, fairness, and perceived societal value. Focus group discussions underscored that incentives are most effective not as standalone motivators, but when embedded within trusted data-sharing relationships, an insight that closely aligns with, and further nuances, existing literature.

Monetary incentives can be an effective motivator for data sharing. For instance, Bietz et al. (2016) found that 56% of participants reported being "more" or "much more" likely to share health data for research if compensated. Similarly, willingness to disclose private information has been shown to increase with higher levels of compensation (Roeber et al., 2015; De Schaepdrijver et al., 2022). Focus group participants generally confirmed that financial or material rewards, such as vouchers, discounts, or direct compensation, can increase engagement, particularly when participation requires sustained effort or targets hard-to-reach groups.

Evidence from both the literature and the focus group discussions indicates that incentives are most effective when they are carefully designed to avoid perceptions of commercial exploitation and unfair exchange. Monetary rewards can increase willingness to share data when they are transparent, proportional, and clearly linked to the purpose of data collection; however, when incentives are perceived as opaque or disconnected from societal value, they may undermine trust (Weydert et al., 2019; Li et al., 2010). Focus group participants consistently emphasised the importance of reciprocity, fairness, and public benefit, suggesting that incentives should complement, rather than substitute, trust-building measures and meaningful justification for data collection.

Willingness to share data can be further increased by providing users with greater control over their information. Mechanisms such as opt-in and opt-out choices for different data uses, the ability to delete data, and transparent overviews of how data are accessed and used have all been shown to increase trust and participation (Ackermann et al., 2022; Frey et al., 2017; Weydert et al., 2019; Yadav et al., 2024). Focus group participants consistently prioritised such control mechanisms, often describing them as prerequisites rather than optional features. At the same time, evidence from both the literature and the focus groups suggests that control mechanisms are most effective when combined with credible and well-communicated data protection technologies, particularly in contexts where users actively assess technical safeguards (Frey et al., 2017).

6.4. Policy recommendations and actions

Building on the combined insights from the literature review and the focus group discussions, this section outlines actionable strategies to enhance willingness to share food-related personal data. Sections 6.1 to 6.3 synthesise evidence-informed solution pathways across technical, governance, and incentive-related dimensions, explicitly reflecting both enabling mechanisms and their practical limitations. Section 6.4 then translates these insights into targeted, actor-specific recommendations for policymakers, regulators, and practitioners.

6.4.1. RECOMMENDATIONS FOR POLICYMAKERS AND REGULATORS

Develop clear, sector-specific guidance for food-related data sharing: Policymakers should establish clear and practical guidelines for sharing food-related personal data, comparable to those available in the health sector. The absence of dedicated guidance for food-related data creates uncertainty for both citizens and organisations and limits

responsible data reuse. Clear rules on permissible data uses, safeguards, and responsibilities would support trust and enable lawful and ethical data sharing (van Panhuis et al., 2014; Reitano et al., 2024).

Strengthen governance, accountability, and enforcement mechanisms: Privacy protection should be supported by transparent governance frameworks that clearly define purpose limitation, data minimisation, access rights, and sanctions in case of misuse. Both the literature and focus groups highlight that trust depends not only on legal compliance but also on visible accountability and enforceable guarantees regarding how data are used and protected (van Panhuis et al., 2014; Yadav et al., 2024).

Invest in data infrastructure and standardisation: Effective data sharing is hindered by fragmented infrastructures, inconsistent data formats, and lack of standardisation. Policymakers should promote investment in interoperable data infrastructures, harmonised standards, and robust metadata practices to support comparability, reuse, and long-term data stewardship across the food system (van Panhuis et al., 2014; Berezowska et al., 2014).

Provide incentives and sustainable resources for data sharing: Sharing personal data requires time, effort, and organisational capacity. Policy frameworks should therefore recognise and support these investments by establishing sustainable funding mechanisms and incentives for both individuals and institutions. Such support can help address motivational and economic barriers while improving data quality and fairness in data-sharing arrangements.

Promote public awareness and digital literacy: A recurring finding across focus groups was limited understanding of data protection, governance mechanisms, and digital risks. Policymakers should support education and awareness initiatives that improve citizens' understanding of how their data are used and protected, thereby strengthening trust and informed participation in data-sharing initiatives.

6.4.2. RECOMMENDATIONS FOR INDUSTRY AND PRACTITIONERS

Design data-sharing systems around user needs and everyday practices: Industry actors should prioritise simplicity, usability, and low effort in data collection and management. User-friendly interfaces, minimal data requests, and clear consent settings were consistently identified in focus groups as prerequisites for participation and trust.

Strengthen transparency and user control: Clear, non-technical explanations of what data are collected, for what purpose, and for how long are essential. Users should be able to easily access, manage, withdraw, or delete their data at any time. Such control mechanisms directly address concerns about irreversibility and loss of oversight highlighted by participants and are strongly supported by the literature.

Use technology selectively and communicate its effects clearly: While advanced technologies (e.g. BC or other privacy-preserving tools) may enhance transparency or security, their effectiveness depends on user understanding and perceived relevance. Industry actors should avoid technology-driven solutions that add complexity without clear user benefits and

instead focus on explaining the practical effects of safeguards, such as reduced misuse or lower risk of breaches.

Demonstrate clear personal and societal value: Both literature and focus group findings show that people are more willing to share data when they perceive tangible benefits. Industry should clearly communicate how data sharing leads to personal value (e.g. feedback, services, savings) and broader societal benefits (e.g. improved food systems, reduced waste, public health insights).

Recognise and reciprocate participation: Providing meaningful incentives (financial or non-financial) and acknowledging contributions can strengthen motivation and trust. Feedback loops, impact summaries, or community-level results help reinforce reciprocity and demonstrate that shared data are used responsibly and for agreed purposes.

Reinforce with Tangible Assurance: Combine technical and social proofs—pair encryption or BC with user testimonials, clear policies, and visible compliance certifications. Provide simple opt-in/opt-out controls so users feel in charge.

7. DISCUSSION, IMPLICATIONS & OUTLOOK

7.1. INTEGRATED DISCUSSION AND CROSS-CUTTING INSIGHTS

Rather than reiterating individual barriers and enablers identified in previous sections, this discussion integrates findings from the literature review and focus group validation to illuminate the broader patterns and systemic dynamics shaping citizens' willingness to share food-related personal data. The emphasis is therefore on how multiple factors interact in practice, reinforcing or counterbalancing one another, and on what these interactions imply for participatory data-sharing initiatives such as SPOON.

Across both evidence sources, trust emerges not as an isolated factor, but as an outcome produced through the combined effects of governance arrangements, perceived data protection, transparency, and institutional credibility. Participants are more willing to share food-related personal data when they understand who is responsible for the data, how it will be used, and what safeguards are in place. Trust is therefore closely tied to clarity and accountability, rather than to technical measures alone.

Privacy and data security concerns intersect strongly with trust dynamics. Both the literature and focus group discussions indicate that individuals frequently overestimate the likelihood and consequences of data misuse while underestimating the effectiveness of existing safeguards. Even when advanced technical protections are implemented, limited understanding of these mechanisms often diminishes their reassuring effect. This suggests that privacy concerns are shaped as much by perception and communication as by actual technical risk, reinforcing the socio-technical nature of data-sharing decisions.

At the same time, perceived personal and societal value plays a critical moderating role in how risks and efforts are evaluated. Willingness to share data increases when individuals clearly understand the purpose of data collection and can relate it to meaningful outcomes, such as improved public health, reduced food waste, or more sustainable food systems. When data sharing is framed as contributing to collective goals or tangible benefits, participants tend to reassess privacy concerns and accept higher levels of engagement.

Practical considerations further condition participation. Across studies and focus groups, effort, time burden, and digital literacy consistently shape willingness to engage. Food-related data collection is often experienced as intrusive or disruptive to everyday routines, particularly when tools are complex or poorly aligned with users' practices. Simplifying data collection processes and reducing cognitive and practical effort therefore emerge as prerequisites for sustained participation, rather than secondary design considerations.

Finally, contextual factors influence how these dynamics unfold across different settings and populations. Age, cultural background, perceived data sensitivity, and the voluntariness of participation all shape how trust, privacy concerns, effort, and perceived benefits are

balanced. Willingness to share tends to be higher when data are perceived as less sensitive, when participation is active and voluntary, and when data use aligns with personal values or collective priorities.

These findings underscore that sharing food-related personal data is not primarily a technical challenge, but a socio-technical one. Willingness to participate is shaped by the interaction between technological design, governance and accountability structures, communication practices, and citizens' everyday experiences. Addressing these dimensions in an integrated manner is therefore essential for fostering trusted and meaningful data-sharing practices within SPOON.

7.2. IMPLICATIONS FOR SPOON AND THE DIGITAL TOOLSET

The integrated findings provide clear and actionable guidance for the design and implementation of SPOON's CSLs and associated digital toolsets. Most importantly, trust must be treated as a foundational design principle rather than an outcome expected to emerge automatically from technical compliance. Transparent communication about data use, clear articulation of research purposes, and visible commitments to ethical standards and data protection are essential to establishing and sustaining participant engagement.

Closely linked to trust is the need for meaningful participant control and clarity. Focus group discussions consistently highlighted the importance of understandable explanations, intuitive consent processes, and the ability for participants to access, manage, or withdraw their data. These insights suggest that governance mechanisms within SPOON should be designed not only to meet legal requirements, but also to be experientially convincing and easy to navigate from a citizen perspective.

The findings further underscore the central role of effort and usability in shaping participation over time. Data collection tools and processes within the CSLs should minimise time burden, integrate smoothly into everyday routines, and avoid unnecessary complexity. Where automation or supportive technologies are employed, they should remain transparent and adaptable to users' preferences, ensuring that convenience does not come at the expense of understanding or perceived control.

Finally, the results highlight the importance of making value creation visible throughout the data-sharing process. Participants are more willing to contribute when they can clearly see how their data lead to tangible outcomes, whether through personal feedback, community-level insights, or broader societal benefits. Explicitly communicating these links can strengthen motivation, reinforce legitimacy, and support longer-term engagement within SPOON.

Taken together, these implications indicate that successful data sharing within SPOON depends on the alignment of technical solutions, governance frameworks, and

communication strategies with citizens' needs, expectations, and values, rather than on any single design element in isolation.

7.3. RESEARCH AND POLICY OUTLOOK

Despite the combined use of a scoping literature review and focus group validation, important knowledge gaps remain. One key limitation concerns how sensitive food-related personal data are perceived to be across different contexts and population groups. Limited empirical evidence in this area makes it difficult to anticipate how such perceptions may influence willingness to share data within SPOON and similar initiatives.

Further research is also needed on strategies to reduce the burden associated with collecting food-related data and to improve the reliability and quality of user-generated information. While effort and data quality emerged as recurring concerns, there is still limited evidence on which design approaches, technologies, or support mechanisms are most effective in addressing these challenges across diverse user groups.

In addition, several factors influencing data-sharing behaviour remain under-researched, including the long-term effects of prior privacy incidents, the contextual conditions under which incentives support or undermine trust, and how different privacy-protection technologies are perceived across socio-demographic groups.

Finally, the rapid expansion of digital food-consumption applications highlights a growing misalignment between data generation practices, governance frameworks, and user protection mechanisms. Future research and policy efforts should therefore focus on improving coordination between technological development, regulatory approaches, and citizen-centred data governance. Strengthening this alignment will be critical to ensuring the responsible, trustworthy, and socially legitimate use of food-related personal data in research and policy contexts.

7.4. CONCLUDING REMARKS

This deliverable provides an integrated evidence base on the factors shaping citizens' willingness to share food-related personal data, combining insights from a structured literature review with empirical validation through focus group discussions conducted in SPOON's CSLs. By jointly examining barriers, enablers, and contextual influences, the analysis demonstrates that data sharing in food-system contexts is fundamentally a socio-technical challenge, requiring alignment between technological design, governance arrangements, and citizens' everyday practices and expectations.

The findings offer concrete guidance for the design and implementation of SPOON's digital tools and participatory processes, highlighting the importance of trust, transparency, proportionality, and meaningful value creation. More broadly, the results contribute to ongoing

policy and research debates on responsible data sharing by emphasising the need for citizen-centred approaches that go beyond compliance and address lived experience.

As SPOON progresses towards tool development and large-scale experimentation, the insights presented here provide a foundation for translating evidence into practice and for supporting trustworthy, inclusive, and impactful data-sharing ecosystems within sustainable food systems.

REFERENCES

Ackermann, K.A., Burkhalter, L., Mildenberger, T., Frey, M. and Bearth, A. (2021). Willingness to share data: Contextual determinants of consumers' decisions to share private data with companies. *Journal of Consumer Behaviour*, 21(2), pp.375–386. doi: https://doi.org/10.1002/cb.2012.

Berezowska, A., Fischer, A.R.H., Ronteltap, A., Kuznesof, S., Macready, A., Fallaize, R. and Trijp, H.C.M. van (2014). Understanding Consumer Evaluations of Personalised Nutrition Services in Terms of the Privacy Calculus: A Qualitative Study. *Public Health Genomics*, [online] 17(3), pp.127–140. doi: https://doi.org/10.1159/000358851.

Bietz, M.J., Bloss, C.S., Calvert, S., Godino, J.G., Gregory, J., Claffey, M.P., Sheehan, J. and Patrick, K. (2016). Opportunities and challenges in the use of personal health data for health research. *Journal of the American Medical Informatics Association*, 23(e1), pp. e42–e48. doi: https://doi.org/10.1093/jamia/ocv118.

Boeschoten, L., Ausloos, J., Möller, J.E., Araujo, T. and Oberski, D.L. (2022). A framework for privacy preserving digital trace data collection through data donation. *Computational Communication Research*, 4(2), pp.388–423. doi: https://doi.org/10.5117/ccr2022.2.002.boes.

Chang, Y., Wong, S.F., Libaque-Saenz, C.F. and Lee, H. (2018). The role of privacy policy on consumers' perceived privacy. *Government Information Quarterly*, 35(3), pp.445–459. doi: https://doi.org/10.1016/j.giq.2018.04.002.

Chen, J., Bauman, A. and Allman-Farinelli, M. (2016). A Study to Determine the Most Popular Lifestyle Smartphone Applications and Willingness of the Public to Share Their Personal Data for Health Research. *Telemedicine and e-Health*, 22(8), pp.655–665. doi: https://doi.org/10.1089/tmj.2015.0159.

Clarke, H., Clark, S., Birkin, M., Iles-Smith, H., Glaser, A. and Morris, M.A. (2021). Understanding Barriers to Novel Data Linkages: Topic Modeling of the Results of the LifeInfo Survey. *Journal of Medical Internet Research*, [online] 23(5), p.e24236. doi: https://doi.org/10.2196/24236.

Cordeiro, F., Epstein, D.A., Thomaz, E., Bales, E., Jagannathan, A.K., Abowd, G.D. and Fogarty, J. (2015). Barriers and negative nudges: Exploring challenges in food journaling. In: *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. [online] Seoul, Republic of Korea: Association for Computing Machinery, pp.1159–1162. doi: https://doi.org/10.1145/2702123.2702155.

Cummings, R., Kaptchuk, G. and Redmiles, E.M. (2021). 'I need a better description': An Investigation Into User Expectations For Differential Privacy. In: *CCS '21: Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*. New York, NY, United States: Association for Computing Machinery, pp.3037–3052. doi: https://doi.org/10.1145/3460120.3485252.

De Schaepdrijver, L., Baecke, P. and Tackx, K. (2022). What Makes Consumers Willing to Share Their Data in Addressable TV Advertising? *Journal of Advertising Research*, 62(2), pp.131–147. doi: https://doi.org/10.2501/jar-2022-012.

Dechand, S., Naiakshina, A., Danilova, A. and Smith, M. (2019). In Encryption We Don't Trust: The Effect of End-to-End Encryption to the Masses on User Perception. In: *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*. Stockholm, Sweden: IEEE, pp.401–415. doi: https://doi.org/10.1109/eurosp.2019.00037.

Donovan SM, Abrahams M, Anthony JC, Bao Y, Barragan M, Bermingham KM, Blander G, Keck AS, Lee BY, Nieman KM, Ordovas JM, Penev V, Reinders MJ, Sollid K, Thosar S, Winters BL. Personalized nutrition: perspectives on challenges, opportunities, and guiding principles for data use and fusion. Crit Rev Food Sci Nutr. 2025;65(30):7151-7169. doi: 10.1080/10408398.2025.2461237. Epub 2025 Feb 5. PMID: 39907017.

Durrant, A., Markovic, M., Matthews, D., May, D., Leontidis, G. and Enright, J. (2021). How might technology rise to the challenge of data sharing in agri-food? *Global Food Security*, 28, p.100493. doi: https://doi.org/10.1016/j.gfs.2021.100493.

European Commission (no date) *Farm to fork strategy*. https://food.ec.europa.eu/horizontal-topics/farm-fork-strategy_en.

Fewings, A., Vandelanotte, C., Irwin, C., Ting, C., Williams, E. and Khalesi, S. (2022). The use and acceptability of diet-related apps and websites in Australia: Cross-sectional study. *DIGITAL HEALTH*, 8. doi: https://doi.org/10.1177/20552076221139091.

Frey, R.M., Bühler, P., Gerdes, A., Hardjono, T., Fuchs, K. and Ilic, A. (2017). The effect of a blockchain-supported, privacy-preserving system on disclosure of personal data. In: *2017 IEEE 16th International Symposium on Network Computing and Applications (NCA)*. Cambridge, MA, USA: Repository for Publications and Research Data (ETH Zurich), pp.1–5. doi: https://doi.org/10.1109/nca.2017.8171385.

Graef, I., Tombal, T. and de Streel, A. (2019). Limits and Enablers of Data Sharing. An Analytical Framework for EU Competition, Data Protection and Consumer Law. *SSRN Electronic Journa*l, TILEC Discussion Paper No. DP 2019-024. doi: https://doi.org/10.2139/ssrn.3494212.

Grande, D., Mitra, N., Iyengar, R., Merchant, R.M., Asch, D.A., Sharma, M. and Cannuscio, C.C. (2022). Consumer Willingness to Share Personal Digital Information for Health-Related Uses. *JAMA Network Open*, 5(1), p.e2144787. doi: https://doi.org/10.1001/jamanetworkopen.2021.44787.

Grimaccia, E. and Naccarato, A. (2020) 'Food insecurity in Europe: a gender perspective,' *Social Indicators Research*, 161(2–3), pp. 649–667. https://doi.org/10.1007/s11205-020-02387-8.

Hafen, E. (2019). Personal Data Cooperatives – A New Data Governance Framework for Data Donations and Precision Health. In: J. Krutzinna and L. Floridi, eds., *The Ethics of Medical Data Donation*. [online] SpringerOpen, pp.141–149. Available at: https://doi.org/10.1007/978-3-030-04363-6.

Hirst, Y., Stoffel, S.T., Brewer, H.R., Timotijevic, L., Raats, M.M. and Flanagan, J.M. (2023). Understanding Public Attitudes and Willingness to Share Commercial Data for Health Research: A Survey Study in the United Kingdom (Preprint). *JMIR Public Health and Surveillance*, 9, p.e40814. doi: https://doi.org/10.2196/40814.

Jai, T.-M. and King, N.J. (2016). Privacy versus reward: Do loyalty programs increase consumers' willingness to share personal information with third-party advertisers and data brokers? *Journal of Retailing and Consumer Services*, 28, pp.296–303. doi: https://doi.org/10.1016/j.jretconser.2015.01.005.

Kosior, K. and Młodawska, P. (2024) 'Understanding Market Actors' Perspectives on Agri-Food Data Sharing: Insights from the Digital Food Passports Pilot in Poland,' *Agriculture*, 14(12), p. 2340. https://doi.org/10.3390/agriculture14122340.

Lei, M., Xu, L., Liu, T., Liu, S. and Sun, C. (2022). Integration of Privacy Protection and Blockchain-Based Food Safety Traceability: Potential and Challenges. *Foods*, 11(15), p.2262. doi: https://doi.org/10.3390/foods11152262.

Li, H., Sarathy, R. and Xu, H. (2010). Understanding Situational Online Information Disclosure as a Privacy Calculus. *Journal of Computer Information Systems*, 51(1), pp.62–71. doi: https://doi.org/10.1080/08874417.2010.11645450.

Maringer, M., van't Veer, P., Klepacz, N., Verain, M.C.D., Normann, A., Ekman, S., Timotijevic, L., Raats, M.M. and Geelen, A. (2018). User-documented food consumption data from publicly available apps: an analysis of opportunities and challenges for nutrition research. *Nutrition Journal*, 17(1). doi: https://doi.org/10.1186/s12937-018-0366-6.

Oakden, L. et al. (2021) 'The importance of citizen scientists in the move towards sustainable diets and a sustainable food system,' *Frontiers in Sustainable Food Systems*, 5. https://doi.org/10.3389/fsufs.2021.596594.

Qian, C., Liu, Y., Barnett-Neefs, C., Salgia, S., Serbetci, O., Adalja, A., Acharya, J., Zhao, Q., Ivanek, R. and Wiedmann, M. (2022). A perspective on data sharing in digital food safety systems. *Critical Reviews in Food Science and Nutrition*, 63(33), pp.12513–12529. doi: https://doi.org/10.1080/10408398.2022.2103086.

Reitano, M. et al. (2024) 'Athletes preferences and willingness to pay for innovative high-protein functional foods,' *Appetite*, 203, p. 107687. https://doi.org/10.1016/j.appet.2024.107687.

Roeber, B., Rehse, O., Knorrek, R. and Thomsen, B. (2015). Personal data: how context shapes consumers' data sharing with organizations from various sectors. *Electronic Markets*, 25(2), pp.95–108. doi: https://doi.org/10.1007/s12525-015-0183-0.

Schumacher, C., Eggers, F., Verhoef, P.C. and Maas, P. (2022). The Effects of Cultural Differences on Consumers' Willingness to Share Personal Information. *Journal of Interactive Marketing*, 58(1), pp.72–89. doi: https://doi.org/10.1177/10949968221136555.

Shaji George, A. and Hovan George, A.S. (2022). Data Sharing Made Easy by Technology Trends: New Data Sharing and Privacy Preserving Technologies that Bring in a New Era of Data

Monetization. *Partners Universal International Research Journal*, 01(03). doi: https://doi.org/10.5281/zenodo.7111123

Sharma, S. (2019) 'A brief history of data privacy,' in *Data privacy and GDPR handbook*. 1st edn. Wiley Data and Cybersecurity, pp. 23–44. https://doi.org/10.1002/9781119594307.ch2

Skatova, A. and Goulding, J. (2019). Psychology of personal data donation. *PLOS ONE*, 14(11), p.e0224240. doi: https://doi.org/10.1371/journal.pone.0224240.

Van Panhuis, W.G., Paul, P., Emerson, C., Grefenstette, J., Wilder, R., Herbst, A.J., Heymann, D. and Burke, D.S. (2014). A systematic review of barriers to data sharing in public health. *BMC Public Health*, [online] 14(1). doi: https://doi.org/10.1186/1471-2458-14-1144.

VERBI Software (2021). MAXQDA 2022, computer software, VERBI Software, Berlin. Available at: www.maxqda.com

Wenz, A., Jäckle, A. and Couper, M.P. (2019). Willingness to use mobile technologies for data collection in a probability household panel. *Survey Research Methods*, 13(1), pp.1–22. doi: https://doi.org/10.18148/srm/2019.v1i1.7298.

Weydert, V., Desmet, P. and Lancelot-Miltgen, C. (2019). Convincing consumers to share personal data: double-edged effect of offering money. *Journal of Consumer Marketing*, 37(1), pp.1–9. doi: https://doi.org/10.1108/jcm-06-2018-2724.

Wiggins, A. and Wilbanks, J. (2019). The Rise of Citizen Science in Health and Biomedical Research. *The American Journal of Bioethics*, 19(8), pp.3–14. doi: https://doi.org/10.1080/15265161.2019.1619859.

Yadav, T.C., Kala, K., Kolachina, R., Kanneganti, M.C. and Pasupuleti, S.S. (2024). Data privacy concerns and their impact on consumer trust in digital marketing. *International Journal of Scientific Research in Engineering and Management*, 08(11), pp.1–7. doi: https://doi.org/10.55041/IJSREM38555.

ANNEXES

CODING TREE

The following codes and sub-codes were used in the analysis of the literature:

FOCUS GROUP GUIDELINES (HYPERLINK)

Welcome and Introduction (5 min)

- Explain that the discussion explores perceptions, motivations, and barriers to sharing personal data via/on digital tools related to food and sustainability, based on what earlier research (Task 1.1) has already shown.
- Reassure participants that the conversation is confidential, and data will be anonymised, and all opinions are welcome.

Exploring Familiarity and Everyday Contexts (15 min)

- When you use apps or websites related to food, health, or shopping, what kind of information do you usually share — and how aware do you feel about how this data is used?
- How do you decide whether to share or limit your data — and do you feel in control of what happens with it afterwards?

Exploring Barriers and Concerns (30 min)

- When you think of sharing your personal food data via digital tools (e.g. what you eat, buy, or throw away), what comes to mind first — would you feel comfortable doing so? Why or why not?
- What kinds of concerns would you have (e.g., privacy, data misuse, loss of control, being profiled)?
- How does trust influence your decision to share data? Who would you trust more — a research institution, a public authority, a company?
- Have you or someone you know ever experienced a data breach or privacy issue? How did it affect your attitude toward sharing information?

Exploring Motivations and Incentives (15 min)

- What could motivate you to share your personal food data — for example, contributing to research, receiving insights about your diet, or financial rewards? What kind of incentive would feel meaningful or trustworthy to you?

Exploring Knowledge and Perceptions of Data Protection (30 min)

- Have you heard about technologies such as encryption, blockchain, or anonymisation that protect data?
- Would knowing that your data are anonymised or encrypted make you feel more comfortable sharing them? Why or why not?
- What kind of explanation or guarantee would make you feel more confident that your data are safe?
- Do you think some groups of people (e.g. older adults, families, students) might have different levels of trust or comfort when it comes to sharing food-related data? Why do you think that is?

Exploring Governance and Solutions (30 min)

- What would make you feel in control of your data (e.g. ability to decide who can see it, delete it anytime, or approve uses)?
- How do you feel about collective or cooperative models, where citizens jointly decide how their data are used?
- What kind of rules or guarantees would you like to see to make data sharing more trustworthy (e.g. sanctions for misuse, transparency)?

Wrap-Up (10 min)

- Summarise key points: i.e., *What are the main barriers? What would increase trust?*
- Thank participants for their contribution.
- Explain that their views will be integrated with research results to help design fair and transparent data-sharing approaches.

CONSORTIUM

Funded by the European Union

SPOON

KEEP IN TOUCH:

@SPOON-PROJECT

INFO@
SPOONPROJECT.EU

@SPOON_EU