

EU REGULATION BUILDS A FAIRER DATA ECONOMY

The opportunities of the Big Five proposals for businesses, individuals and the public sector

Tobias Bräutigam

Partner
Bird & Bird

Francine Cunningham

Regulatory & Public Affairs Director
Bird & Bird

Meeri Toivanen

Specialist
Sitra

Maria Aholainen

Associate
Bird & Bird

Marjolein Geus

Partner
Bird & Bird

Floora Kukorelli

Associate
Bird & Bird

The European Commission's legislative proposals for the data economy focus on establishing a European single market for data with a level playing field by harmonising rules on data sharing, regulating the dominant players and giving people more control over their data. The five new data law proposals published by the European Commission in recent years will reshape the data-driven business environment in Europe. Are European businesses and the public sector ready for the emerging opportunities and to act in order to realise the potential of the data?

The working paper complements the general understanding about the current operational environment by taking an overall view of the five data law proposals and exploring the opportunities that the proposals offer together from the perspectives of the public sector, SMEs and individuals.

© Sitra 2022

Sitra working paper

**EU regulation builds a fairer data economy
The opportunities of the Big Five proposals for
businesses, individuals and the public sector**

Bird & Bird team: Tobias Bräutigam, Maria Aholainen,
Francine Cunningham, Marjolein Geus, Floora
Kukorelli

Sitra team: Meeri Toivanen, Reijo Aarnio, Laura
Halenius, Taru Rastas, Johanna Kippo

Sitra Layout: PunaMusta Oy

ISBN 978-952-347-276-1 (PDF) www.sitra.fi
ISSN 2737-1042 (electronic publication)

PunaMusta Oy 2022

Sitra working papers provide multidisciplinary information about developments affecting societal change. Working papers are part of Sitra's future-oriented work conducted by means of forecasting, research, projects, experiments and education.

Contents

Foreword	5
Summary	6
Tiivistelmä	7
Sammanfattning	8
1 Overview of data legislation in the EU	9
1.1 Introduction	9
1.2 The scopes of the data legislation in the EU and their relationship to the Big Five proposals	10
1.3 Shortcomings of the current system	11
2 The European Data Strategy and the Big Five	13
2.1 Introduction	13
2.1.1 Summary of the European Data Strategy	13
2.1.2 Analysis of the strategy	14
2.1.3 Motivation behind the data strategy	14
2.1.4 What can be done about it?	15
2.1.5. Where are we now?	16
2.2 Summary of the Big Five proposals	17
2.2.1 Data Governance Act (DGA)	18
2.2.2 Digital Markets Act (DMA)	20
2.2.3 Digital Services Act (DSA)	22
2.2.4 Artificial Intelligence Act (AIA)	24
2.2.5 Data Act	26
2.3 Synopsis	27
2.3.1 The Big Five proposals pave the way for a fairer data economy	27
2.3.2 Questions to answer	28
3 The Big Five proposals in relation to the vision and objectives of the data strategy	29
3.1 What do the Big Five mean for individuals?	29
3.1.1 Access to data generated using connected devices	29
3.1.2 Control over ads shown online	30
3.1.3 Rules on AI to create trust	32

3.2	What do the proposed measures mean for the public sector?	33
3.2.1	Reuse of data in the public sector	33
3.2.2	Increased use of AI on the public sector	34
3.2.3	New powers and new authorities	35
3.2.4	What would this all mean for Finland?	37
3.3	What do the proposed measures mean for businesses and especially for SMEs?	40
3.3.1	Levelling the playing field may increase competition	40
3.3.2	Changes will not impact everyone in the same way	41
3.3.3	Business opportunities	43
3.4	How well do the Big Five meet the objectives of the European Data Strategy?	46
3.4.1	How do the Big Five support the data strategy?	46
3.4.2	Synopsis	46
4	Recommendations and next steps	48
4.1	General recommendations	48
4.2	Recommendations per stakeholder group	48
4.2.1	Recommendations for the public sector	48
4.2.2	Recommendations for the private sector, in particular SMEs	49
4.2.3	Recommendations for individuals	49
4.3	Further studies and research on the topic	50
4.3.1	Monitoring the implementation process across the EU	50
4.3.2	Assessment of impact and the interplay between the various instruments	50
4.3.3	Focus on specific use cases	50
5	Sitra's conclusions: Seizing the future opportunities today	52
	References	59
	Annex 1: Abbreviations	62
	Annex 2: Existing data legislation	63
	Annex 3: Cornerstones of the current framework	64
	Annex 4: Summary of the Big Five	66
	Annex 5: Interviewees and workshop participants	67
	About the authors	69

Foreword

The amount of data in the world is growing exponentially. It offers opportunities to reform the economy and society. Data and the information derived from it can do a lot of good, providing us all with better services and well-being. The ability to harness new types of information is also needed to address the sustainability crisis, the heightened security situation in Europe and the aftermath of the pandemic.

As growth slows down, finding sources of growth is becoming increasingly important and a lot of expectations have been placed on digitalisation and data. The European Union wants to emerge alongside China and the United States as a major data economy by creating an internal market for data, in which information can flow freely between countries and sectors, in line with its data strategy. At the same time, the aim is to strengthen the rights of the SME sector and the individual in particular, and to make the use of data fairer than at present.

Now that Europe and Finland in particular are facing complex challenges on different fronts, it is critical that the legislation and other policy measures now being taken are timely and proportionate in order to live up to the expectations placed on the data. The most important of these policy measures are the five new digital legislative proposals published by the European Commission in recent years, which will radically change the business environment for the data economy in Europe.

Sitra builds a human-driven and fair data economy based on European values. This study

is part of the Roadmap to the Data Economy project, which aims to encourage a common understanding, awareness about the current operational environment and the will to promote the data economy and to identify the most effective ways to achieve this goal.

The aim of this working paper is to complement the general understanding about the current operational environment by taking an overall picture of the five digital legislative proposals and to explore the opportunities that the legislative proposals together offer from the perspective of society, SMEs and European citizens. The report is a continuation of “Finland's Strengths, Challenges and Opportunities in Building a Data Economy”, published in January 2022, in which the infrastructure, know-how, network co-operation, regulation and sustainability were identified as the areas where national co-operation and measures are needed.

I hope that this working paper will spark a debate and lay the groundwork for the actions and co-operation we need to realise the potential of the data identified in this study and in society at large. I would like to thank the authors of the working paper, the experts who gave their time for the interviews and workshops, and others who helped with the background work for their excellent contributions.

Laura Halenius

Project Director, A Roadmap for a Fair Data Economy

Summary

In February 2020, the European Commission published the European Data Strategy. The aim of this policy programme is to “create a society empowered by data” and to build “a strong legal framework in terms of data protection, fundamental rights, safety and cyber-security”. The aim is to “increase the use of, and demand for, data and data-enabled products and services throughout the Single Market”.

To set up this new model for a data economy, the commission launched several legislative proposals, which aim at improving and harmonising the currently fragmented legal framework in the European Union (EU). This will enable the EU data economy to develop and contribute to growth and innovation in Europe, while supporting the bloc’s digital and green transitions. The proposed legislation focuses on establishing a single market for data with a level playing field by providing rules for data sharing, regulating dominant players and giving people more control over their data.

This report consists of five parts.

- Chapter 1 provides an overview of the current legal landscape in the EU in relation to the data economy – the status quo.
- Chapter 2 provides an overview of the European Data Strategy and an initial analysis of the five related legislative proposals: the Data Governance Act, the Digital Markets Act, the Digital Services Act, the Artificial Intelligence Act and the Data Act (together known as the “Big Five”).
- Chapter 3 includes a deeper analysis of the Big Five and assesses what the proposed

governance model would mean for (a) an ordinary citizen; (b) a small or medium-sized company; and (c) the public administration in Finland. In addition, it assesses whether these proposals meet the vision and objectives set out by the European Commission in the data strategy, that is, would the proposed governance model work and what alternatives exist?

- Chapter 4 and 5 list recommendations for individuals, companies and the public sector and identifies next steps and areas for further studies on the topic.

Sources used for this report comprised a combination of a literature review, interviews with EU legislators and policy experts and two workshops with Finnish stakeholders representing the public administration, businesses and consumers.

This report focuses only on the five legislative proposals (Big Five) rather than all actions proposed or introduced in the European Data Strategy. The legislative proposals are referenced in their current form (as of 31 March 2022), as most of the proposed legal acts are currently still going through the European legislative process.

Given the limited space, this report uses examples to illustrate potential use cases for the three stakeholder groups: individuals, small and medium-sized companies, and the public administration. This report serves as inspiration for further and more analytical studies on the topic of data economy regulation.

Tiivistelmä

Euroopan komissio julkaisi helmikuussa 2020 Euroopan datastrategian. Tämän politiikka-ohjelman tavoitteena on edistää datapohjaisen yhteiskunnan rakentamista ja luoda vahva oikeudellinen kehys datalle tietosuojan, perusoikeuksien sekä (kyber)turvallisuuden näkökulmasta. Keskeinen tavoite on myös lisätä datan ja datapohjaisten tuotteiden sekä palveluiden käyttöä ja kysyntää koko Euroopan unionin sisämarkkina-alueella.

Tämän uuden datatalousmallin luomiseksi komissio on antanut useita lainsäädäntöehdotuksia, joilla pyritään parantamaan ja yhdenmukaistamaan EU:n tällä hetkellä hajaista lainsäädäntökehystä. Uudistukset luovat EU:n datataloudelle paremmat mahdollisuudet kehittyä ja ne edistävät talouskasvua ja innovointia Euroopassa. Samalla tarkoituksena on tukea unionin digitaalista ja vihreää siirtymää. Ehdotetussa lainsäädännössä keskitytään datan sisämarkkinoiden luomiseen sääntelemällä datan jakamista, markkinoita hallitsevia toimijoita ja antamalla ihmisille enemmän mahdollisuuksia hallita omia tietoaan.

Tämä raportti koostuu viidestä osasta:

- Luku 1 antaa yleiskatsauksen EU:n tämänhetkiseen datatalouteen liittyvään lainsäädäntöön.
- Luku 2 sisältää yleiskatsauksen Euroopan datastrategiasta ja alustavan analyysin viidestä siihen liittyvästä lainsäädäntöehdotuksesta: datahallintosäädöksestä (Data Governance Act), digimarkkinasäädöksestä (Digital Markets Act), digipalvelusäädöksestä (Digital Services Act), tekoälysäädöksestä (Artificial Intelligence Act) ja datasäädöksestä (Data Act). Yhdessä näitä kutsutaan tässä raportissa nimellä viisi keskeistä lainsäädäntöehdotusta sekä termillä Big Five ehdotukset.
- Luku 3 sisältää syvällisemmän analyysin näistä viidestä keskeisestä

lainsäädäntöehdotuksesta ja arvioi, mitä ehdotettu hallintomalli merkitsisi (a) tavalliselle kansalaiselle, (b) pienelle tai keskisuurelle yritykselle ja (c) julkishallinnolle Suomessa. Lisäksi tarkastellaan, vastaavatko nämä ehdotukset Euroopan komission datastrategiassa esittämää visiota ja tavoitteita, eli ehdotetun hallintomallin toimivuutta ja mahdollisia vaihtoehtoisia malleja.

- Luvut 4 ja 5 sisältävät keskeiset johtopäätökset, suositukset puutteiden korjaamiselle yksityishenkilöiden, yritysten ja julkisen sektorin näkökulmasta sekä ehdotukset jatkotutkimuksille.

Lähteinä tässä raportissa on käytetty oikeuskirjallisuutta, virallisia EU-materiaaleja, EU-virkahenkilöiden ja sidosryhmien edustajien haastatteluita sekä näkemyksiä, jotka on koottu kahdesta sidosryhmätyöpajasta. Työpajat oli suunnattu suomalaisille julkishallintoa, yrityksiä sekä kuluttajia edustaville sidosryhmille.

Raportti keskittyy ainoastaan mainittuihin viiteen keskeiseen lainsäädäntöehdotukseen eikä syvenny kaikkiin Euroopan datastrategiassa ehdotettuihin tai käyttöön otettuihin toimenpiteisiin. Tässä raportissa lainsäädäntöehdotuksiin viitataan niiden nykyisessä muodossa (31. maaliskuuta 2022). Suurin osa ehdotetuista säädöksistä on edelleen EU:n lainsäädäntöprosessissa.

Rajallisen tilan vuoksi tässä raportissa havainnollistetaan esimerkkien avulla mahdollisia käyttötapauksia kolmelle toimijaryhmälle: kansalaisille, pk-yrityksille sekä julkishallinnolle. Tämän raportin tarkoituksena on toimia inspiraationa tuleville ja mahdollisesti analyttisemmille tutkimuksille datatalouden sääntelystä.

Sammanfattning

Europeiska kommissionen offentliggjorde Europas datastrategi i februari 2020. Syftet med detta politiska program är att främja uppbyggnaden av ett databaserat samhälle och skapa en stark rättslig ram ur dataskyddets, de grundläggande rättigheternas och (cyber)säkerhetens perspektiv. Ett centralt mål är också att öka användningen av och efterfrågan på data och databaserade produkter och tjänster inom hela Europeiska unionens inre marknadsområde.

För att skapa denna nya dataekonomi-modell har kommissionen lagt fram ett flertal lagstiftningsförslag, med vilka man strävar efter att förbättra och harmonisera EU:s nuvarande splittrade lagstiftningsram. Förnyelserna skapar bättre möjligheter för EU:s dataekonomi att utvecklas och de främjar ekonomisk tillväxt och innovationer i Europa. Samtidig är syftet att stödja unionens digitala och gröna övergång. I den föreslagna lagstiftningen fokuserar man på att skapa en inre marknad för data genom att reglera delning av data, aktörer som dominerar marknaden och ge människorna fler möjligheter att hantera sina egna uppgifter.

Den här rapporten består av fem delar:

- Del 1 ger en överblick av EU:s nuvarande lagstiftning i anslutning till dataekonomi.
- Del 2 innehåller en överblick av Europas datastrategi och en preliminär analys av fem lagstiftningsförslag i anslutning till detta: dataförvaltningsakten (Data Governance Act), rättsakten om digitala marknader (Digital Markets Act), rättsakten om digitala tjänster (Digital Services Act), rättsakten om artificiell intelligens (Artificial Intelligence Act) och dataförordningen (Data Act). I den här rapporten går dessa tillsammans under namnet de fem centrala lagstiftningsförslagen och termen Big Five-förslag.
- Del 3 innehåller en mer djupgående analys av dessa fem centrala lagstiftningsförslag och en bedömning av vad den föreslagna

förvaltningsmodellen skulle betyda för (a) den vanliga medborgaren, (b) ett litet eller medelstort företag och (c) den offentliga förvaltningen i Finland. Dessutom kontrolleras om dessa förslag motsvarar den vision och de mål som har angetts i Europeiska kommissionens datastrategi, det vill säga den föreslagna förvaltningens funktionalitet och eventuella alternativa modeller.

- Del 4 och del 5 innehåller centrala slutsatser, rekommendationer för korrigerande av brister ur privatpersoners, företags och den offentliga sektorns perspektiv samt förslag till fortsatta undersökningar.

Källor i denna rapport utgörs av juridisk litteratur, officiellt EU-material, intervjuer med EU-tjänstemän och representanter för intressenter samt åsikter som har sammanställts från två intressentworkshoppar. Workshopparna var riktade till den finska offentliga förvaltningen, företag samt intressenter som representerar konsumenterna.

Rapporten fokuserar endast på de fem centrala lagstiftningsförslag som har nämnts och fördjupar sig inte i alla föreslagna eller vidtagna åtgärder i Europas datastrategi. I den här rapporten hänvisas till lagstiftningsförslagen i deras nuvarande form (den 31 mars 2022). De flesta av de föreslagna förordningarna ingår fortfarande i EU:s lagstiftningsprocess.

På grund av det begränsade utrymmet i den här rapporten klargörs eventuella användningsfall för tre aktörsgrupper med hjälp av exempel: för medborgare, små och medelstora företag och den offentliga förvaltningen. Syftet med den här rapporten är att fungera som inspiration för kommande och eventuellt mer analytisk forskning om reglering av dataekonomin.

1 Overview of data legislation in the EU

The value of the data economy is constantly rising and is the subject of close legislative scrutiny. However, the legal framework relating to the data economy in the European Union is fragmented. It is hard for enterprises to understand and apply the regulations appropriately. The European Commission wants to change the fragmented legal framework with the explicit aim of creating a comprehensive and clear framework with proposals for new legislation.

1.1 Introduction

The data economy is defined by the European Commission as a part of the economy in which business is based wholly or largely on the utilisation and use of data in different ways by ensuring that data is accessible and usable (European Commission 2017). The value of the data economy is constantly rising and is thus the subject of close legislative scrutiny.

Over the last decade, the commission has introduced further legislation on data. However, the legal framework relating to the data economy in the European Union (EU) is fragmented. It consists of various legal instruments that are both sector-specific and more generally applicable without an overarching vision for an EU data economy or a data-driven society.

The European Commission published the European Data Strategy in 2020 to change this fragmented landscape with the explicit aim of creating a comprehensive and clear data regulation framework with proposals for new legislation (European Commission 2020a). The Big Five proposals flowing from the data strategy – the Data Governance Act (DGA), the Digital

Markets Act (DMA), the Digital Services Act (DSA), the Artificial Intelligence Act (AIA) and the Data Act (DA) – will be described in more detail in chapter 2.

Beyond the data strategy and the Big Five, the key legal instruments relating to the data economy comprise:

- General Data Protection Regulation (2016/679, GDPR)
- ePrivacy Directive (2002/58)
- Regulation on Non-Personal Data (2018/1807)
- Open Data Directive (2019/1024)
- Payment Services Directive 2 (2015/2366, PSD2)

The next section will present an overview of the key instruments above and their relationships to the Big Five. Further, there are several other instruments (such as the Cybersecurity Act, the Network and Information Security Directive, the Reach Regulation, the Clinical Trial Regulation and the Electricity Directive) that are listed in Annex 1 as they could not be covered within the scope of this paper.

1.2 The scopes of the data legislation in the EU and their relationship to the Big Five proposals

Table 1: An overview of the scopes of the data legislation in the EU and their relationship to the Big Five proposals

Law	Type of data	Overlap	Aim	Status
General Data Protection Regulation (EU) 2016/679 (GDPR)	Personal data	All acts that regulate personal or mixed data sets overlap to some degree with the GDPR	Protect personal data, create a solid framework for digital trust	Applicable since 25 May 2018
Directive on open data and the re-use of public-sector information (EU) 2019/1024 (Open Data Directive)	Non-personal data	The GDPR prevails Overlap with the DGA in so far as reuse of non-personal data is concerned	Enable reuse of data held by public-sector bodies	Applicable since 17 July 2021
Regulation on a framework for the free flow of non-personal data in the European Union (EU) 2018/1807 (Free Flow Regulation)	Non-personal data	The GDPR prevails Overlap with the DGA in so far as reuse of non-personal data is concerned Slight overlap regarding data portability with the DA	Free movement of data Encourage porting of data for professional users Restriction of data localisation rules in the EU	Applicable since 28 May 2019
Proposal for a Regulation on Privacy and Electronic Communications (E-Privacy Regulation)	Personal data, non-personal data	The GDPR prevails; can be applied simultaneously with the GDPR Includes more specific provisions on protecting privacy in the context of electronic communications	Privacy in electronic communications	Proposal published on 10 January 2017; Trilogue since spring 2021 Possibly applicable in the second half of 2024, 24 months after entry into force.
Proposal for a Regulation on European data governance (Data Governance Act or DGA)	Personal data, non-personal data, confidential data	The GDPR and the Free Flow Regulation prevail	Make more data available and create governance models for sharing Increase trust in data intermediaries	Proposal on 25 November 2020 Political agreement on 10 December 2021 Possibly applicable in summer 2023, 15 months after entry into force
Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act or AIA)	Mixed data, personal data, non-personal data	The GDPR prevails; exceptions for sensitive personal data Transparency obligations on top of Articles 13 and 14 of the GDPR	Improve predictability, optimise operations and resource allocation, and personalise service delivery of the use of AI Categorisation of AI according to risk	Proposal on 21 April 2021 Possibly applicable in 2024, 24 months after entry into force

Law	Type of data	Overlap	Aim	Status
Proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act or DMA)	Personal data and non-personal data	Access to search data in compliance with the GDPR only Transparency obligations on top of Articles 13 and 14 of the GDPR Restricting combination of personal data Sharing obligations	Remove barriers to access of data Regulate gatekeepers Preserve incentives to invest in data generation	Proposal Political agreement was reached on 25 March 2022; needs approval still by the European Parliament and Council Possibly applicable in the first half of 2023
Proposal for a regulation on a Single Market for Digital Services (Digital Services Act or DSA)	Caching data, reporting data in aggregated form, personal data	Revising the e-commerce framework, GDPR-compliant data sharing	Proper functioning of the internal market for intermediary services Set out uniform rules for a safe, predictable and trusted online environment	Proposal published on 15 December 2020; Political agreement was reached on 23 April 2022; needs approval still by European Parliament and Council Possibly applicable in 2023
Proposal for a regulation on harmonised rules on fair access to and use of data (Data Act or DA)	Mixed data, mainly IoT data	The GDPR prevails, exception of data sharing to gatekeepers in the DMA Rules for transfer of non-personal data	Proper use and access of data	Proposal published on 23 February 2022 Possibly applicable in the second half of 2023, 12 months from entry into force

1.3 Shortcomings of the current system

Looking at the landscape of EU regulation on the data economy, three key observations stand out.

First, the landscape is fragmented and there is no overarching narrative that ties the different legislative acts together. This is supported by the different definitions, focus areas and scopes of application of the legislation presented in the above table and listed in Annex 2. This makes it hard, especially for small and medium-sized enterprises (SMEs), to understand and apply the regulation correctly and without excessive compliance costs. This has also been shown in a study conducted by Sitra in 2021, which concluded that SMEs find regulation the biggest obstacle to joining the data economy (Sitra 2021, p. 37).

Second, while it is generally recognised that the potential for economic growth is huge when

data is used more efficiently, EU legislation has so far not led to fundamental changes. Where data sharing is promoted (with the Open Data Directive or the Free Flow Regulation, for instance), the provisions are not sufficiently ambitious and devoid of concrete frameworks to enable data sharing.

It is hard, especially for small and medium-sized enterprises, to understand and apply the regulation correctly and without excessive compliance costs.

There are exceptions to this rule, and the idea to regulate central market participants is not new in EU legislation. Traditional telecom operators and banks in the finance sector, both covered by sectoral legislation, have long been subject to more stringent rules. For example,

PSD2 obliged traditional banks to open up their platforms and services to third-party providers, which exposed banking-related data to wider use and thereby created several new business models. The European Electronic Communications Code (EECC) extends rules to providers that were not regulated based on the previous framework, such as over-the-top (OTT) providers offering interpersonal communications, content and cloud services.

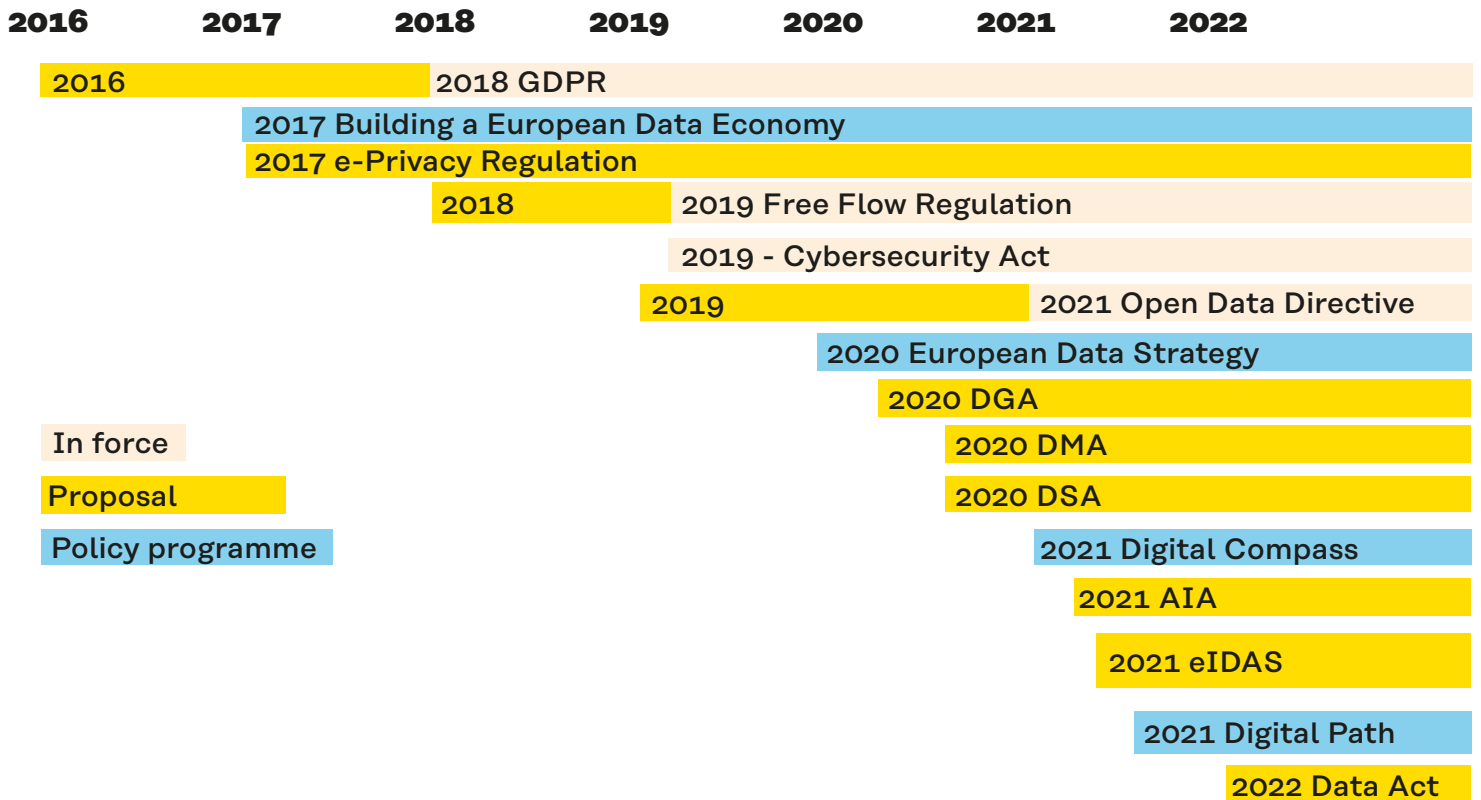
However, these exceptions to data access are sector specific and they apply only to a small part of the data economy. Thus, they alone are not sufficient to address and fix the identified market failures prevalent currently.

Third, and in some way connecting the first and second observations, it becomes apparent

that the legal instruments in question leave a lot of room for manoeuvre. Even regulations include several opening clauses for member states. This leads to further legal fragmentation in the EU and demonstrates how hard it is to reach compromises at the EU level in matters relating to the data economy. This is because this area is new and different member states have developed conflicting ideas on how to regulate the data economy. This phenomenon was also visible when negotiating the GDPR and remains so in the ongoing negotiations over the ePrivacy regulation.

In the next chapter, we will analyse what the commission set out to do with the European Data Strategy and will briefly cover the Big Five proposals.

Figure 1: An overview of data legislation in the EU



2 The European Data Strategy and the Big Five

The five new legislative proposals launched by the European Commission as part of the data strategy aim to level the playing field by providing fair rules for data sharing and use, regulating the dominant players and strengthening people's control over their data. A new kind of internal market for data based on EU values, within which data can move freely and be accessible to European businesses, researchers and public administrations, should help to capture the benefits of the available data. However, the proposed European model can only work if, on the one hand, the Big Five proposals succeed in creating a new regulatory framework that facilitates growth and innovation and, on the other hand, this framework is supported by investment, research and upskilling.

2.1 Introduction

2.1.1 Summary of the European Data Strategy

The European Data Strategy is a policy programme of the European Commission published on 19 February 2020. Its vision is to “create an attractive policy environment” that by 2030 will boost the EU's share and role in the global data economy. The data economy is defined by the European Commission as that part of the economy in which business is based wholly or largely on the utilisation and use of data in different ways by ensuring that data is accessible and usable (European Commission 2017).

The value of the data economy is constantly rising and is thus also the subject of close legislative scrutiny. The European Commission envisages a single European data space – a genuine single market for data “where EU law can be enforced effectively, and where all

data-driven products and services comply with the relevant norms of the EU's single market”. According to one interviewee, there is a clear shift away from data protection to other policy areas such as enhancing the effective use of data on the inner market.

This new kind of internal market for data based on EU values, within which data can move freely and be accessible to European businesses, researchers and public administrations, should help to capture the benefits of the available data and lead to more data being stored and processed in the EU. This could lead to gains in productivity, higher competitiveness, improvements for individuals and a better functioning public service.

To meet the strategy's vision, the commission has identified the following tools: fit-for-purpose legislation and governance to ensure the availability of data; investments in standards, tools and infrastructures; and competence for handling data.

Aims of the data strategy

- Europe as a global leader in a data-driven society
- Free flow of data within the EU and across sectors
- Availability of high-quality data with which to create and innovate
- European rules and values are respected

Pillars of the data strategy

- A cross-sectoral governance framework for data access and use
- Enablers: investments in data and strengthening Europe's capabilities and infrastructures for hosting, processing and using data, interoperability
- Competences: empowering individuals, investing in skills and small and medium-sized enterprises (SMEs)
- Common European data spaces in strategic sectors and domains of public interest

2.1.2 Analysis of the strategy

First, with the data strategy, the EU is proposing an alternative to the current business model that is more human-centric and benefits all. Currently, the European market is dominated by “gatekeepers”, the largest companies offering one or more core platform services with a very significant impact on the European market.

In short, gatekeepers could be described as companies an ordinary EU citizen cannot avoid when operating in the digital environment. Core platform services are the services offered by these gatekeepers and encountered by consumers and businesses daily. To set up this new business model, the commission launched as part of the data strategy several legislative proposals (the Big Five), which aim to level the playing field by providing fair rules for data sharing and use, regulating the dominant players and strengthening people’s control over their data.

Second, the data strategy wrestles with a dilemma. On the one hand, the commission wants to create a thriving data-driven society and, indeed, acquire a world-leading role in the data economy. On the other hand, the commission does not want to erode core European values and fundamental rights. At times, it

seems that the commission is proposing many rules that conflict with creating a thriving data-driven society and reducing legal barriers.

At times, it seems that the commission is proposing many rules that conflict with creating a thriving data-driven society and reducing legal barriers.

Third, the commission is clearly more ambitious than in its previous attempts to foster data sharing in the EU as it aims to create a European model for data sharing and use. In other words, the goal is to build a strong regulatory framework for the data economy and the entirety of the data value chain in the internal market.

2.1.3 Motivation behind the data strategy

The European Commission sees access to data as essential for the competitiveness of the EU. This is true from at least three perspectives.

First, there are very few European companies in the top 100 technology companies. The leading technology companies have typically faced little regulation in their home countries outside the EU. This has made it hard for European companies to enter their market (lack of competition regulation has enabled the paying up of smaller players and controlling the market entry) while still upholding European values of data protection, consumer protection and freedom of speech, to name a few. This puts the EU at a strategic disadvantage as technology markets currently are often winner-takes-all markets.

Second, without data to develop new ideas and improve current ones, the gap between Europe on one side and the United States and China on the other will only widen. The commission is aiming to influence the markets in a way that reflect European values and give more room for European companies to succeed in the fierce competition between leading technology companies. If this does not happen soon, it might be too late.

The current business model aims primarily to maximise profit. This model is referred to by some observers as a “surveillance-based” business model, where the power is concentrated in the hands of a few private companies (Zuboff 2018, Amnesty International 2019). Another form of surveillance is the state-controlled model in China. China has a largely separate ecosystem as the Chinese government maintains internet censorship and determines what websites and data Chinese users can access. The commission made it very clear in the design of the data strategy that the European model needs to be different from both the current model and the Chinese model.

Without access to data, data-intensive applications for the public good, such as developing innovations in medicine or using data for public policies, will not work.

Third, without access to data, data-intensive applications for the public good, such as developing innovations in medicine or using data for public policies, will not work. Access to data is currently lacking not only because there is no general (regulatory) framework for sharing data safely but also because citizens and companies are not sufficiently motivated to share their data with others. Lack of motivation also means that different systems are not usually designed and developed with interoperability in mind.

Access to data is currently lacking because there is no general regulatory framework for sharing data safely but also because citizens and companies are not sufficiently motivated to share their data with others.

2.1.4 What can be done about it?

Without stating this aim directly, the EU is proposing a more regulated model of data use with the hope that this will work for the benefit of the European society as a whole, while keeping the businesses and individuals who generate the data in control. To this end, the European Commission introduced five proposals for regulation in the aftermath of the data strategy (known as the Big Five).

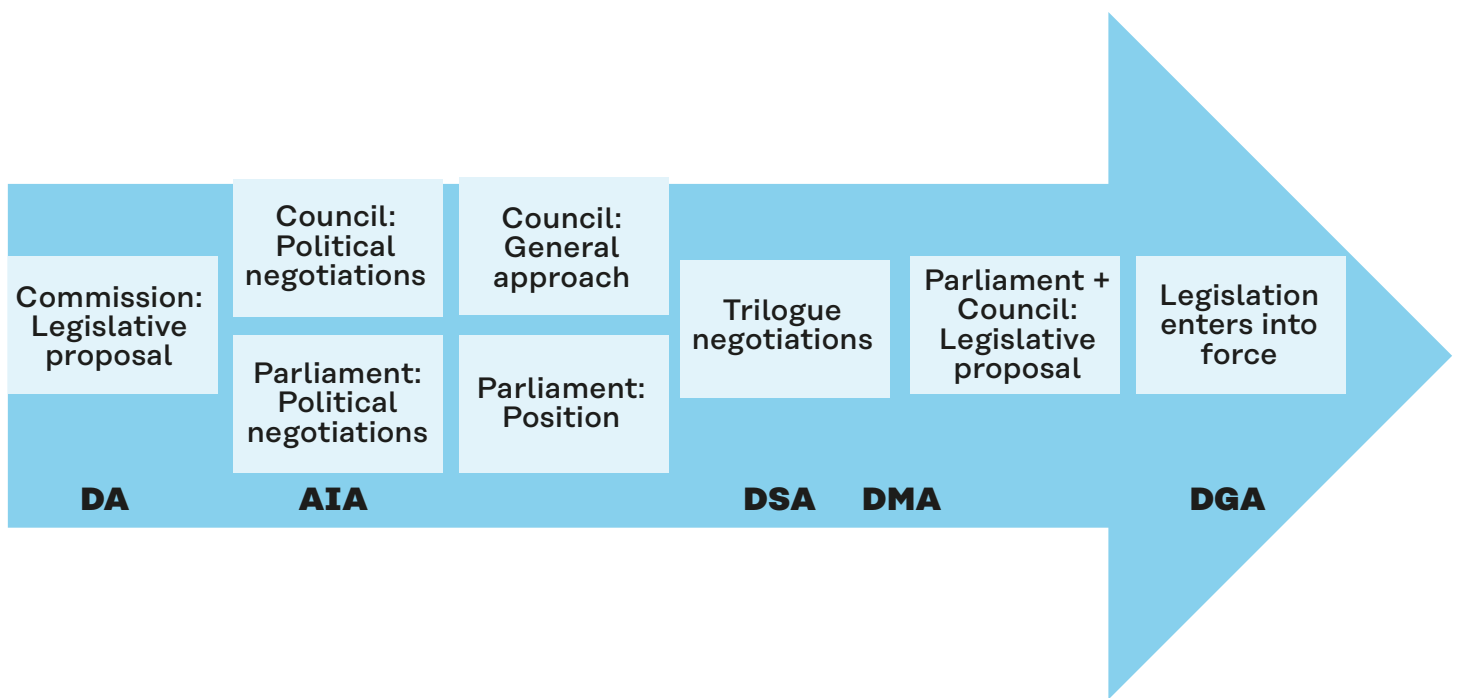
Unlike directives, regulations are directly applicable in all 27 EU member states, without the need to implement legislation at the national level. The commission chose to propose regulations to ensure uniform legislation in the field of the single market for data, which in principle does not depend on transpositions in national law in the member states, although application may still vary across them. The choice of the legal instrument demonstrates the commission’s level of ambition and a paradigm shift from “reactive” sector-specific

regulation to more ex ante regulation (i.e., based on forecasts rather than the actual results) in line with the European values in the single market for data.

2.1.5. Where are we now?

The proposals are at different stages in the legislative process in the EU. Thus, there is still some uncertainty about when the Big Five will finally be adopted at the EU level and what their final content will be.

Figure 2: The Big Five proposals are at different stages of the legislative process



As regards the Digital Services Act (DSA) and the Digital Markets Act (DMA), the European Commission and the current French Presidency of the EU have declared that they want to reach consensus by summer 2022, with an additional six months (timing to be confirmed) for the new legislation to enter into force. For the DMA, political consensus was reached in March 2022 and for DSA in April 2022.

The Data Governance Act (DGA) has advanced the furthest in the decision-making process. The EU institutions reached agreement on a final text in December 2021, and the DGA was officially adopted by the European Parliament and European Council in May 2022.

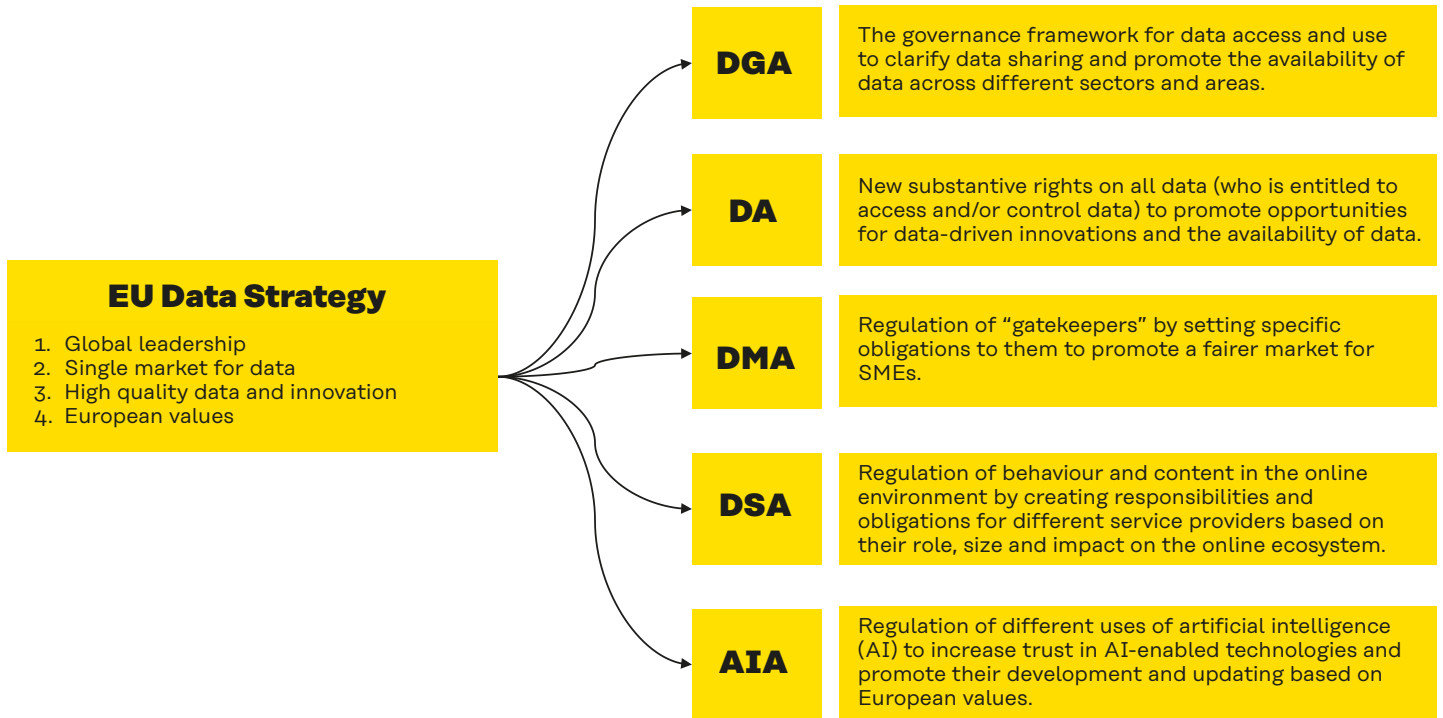
The DGA was published in the Official Journal of the European Union in June 2022 and the new rules will become applicable in September 2023.

The Artificial Intelligence Act (AIA) is currently under discussion in the Council, while the European Parliament’s work on the proposal was only set to begin in January 2022, following nine months of delays over deciding the competences between different committees.

The Data Act (DA) was the final proposal to be published on 23 February 2022, so discussions in the European Council and European Parliament only began in spring 2022.

2.2 Summary of the Big Five proposals

Figure 3: An overview of the data strategy and the Big Five proposals



2.2.1 Data Governance Act (DGA)

On 25 November 2020, the European Commission introduced its proposal for the DGA as a first step towards implementing the data strategy. The purpose of the proposal is to establish an enabling governance framework for European data spaces as well as strengthen confidence and trust between those in the data market. During the interviews, it was mentioned that the aim of the proposal is to enhance data sharing, which is only possible if there are enough rules and safeguards to protect data. The new assumption must be that the data subject is an active participant, not a passive agent.

The DGA would apply to protected data, which means data that is already subject to someone else's right (such as personal data, trade secrets, intellectual property rights). However, the proposal is not intended to grant, modify or remove existing rights, but to create a framework within which the use of such protected data could be allowed.

The DGA introduces reliable data intermediary services, which would help individuals exercise their rights under the GDPR. Data intermediary services refer to data-sharing services provided by organisations called data intermediaries. According to the DGA, these intermediaries are supposed to have a facilitating role and be independent from both data holders and data users (European Commission 2020b, p. 16). Furthermore, the DGA is also intended to facilitate data altruism, which refers to procedures in which companies or individuals voluntarily make data publicly available. In the future, it will be possible for an organisation to register as an altruistic organisation.

Overall, the interplay with the existing legislation, such as with the GDPR, is not clear-cut. For example, the DGA introduces a broad definition of “data” that also includes personal data. Therefore, the GDPR and the DGA would apply simultaneously, DGA being without prejudice to the GDPR. Despite its connection to the GDPR, the competence to monitor compliance with the DGA is not afforded to data-protection authorities but is up to the member states to decide, which may potentially lead to separate competent bodies with overlapping competences. The DGA covers both personal data and non-personal data.

Potentially, the DGA could mean, for example, the reuse of GPS or health data collected by the public sector for either commercial or non-commercial purposes. This idea is not new in Finland. There is already legislation in place to enable reuse of health data in Finland (Act on Secondary Use of Health and Social Data (552/2019)). One commission official mentioned that the biggest threat to the success of this legislative package is inaction, meaning that not enough people or businesses would be interested in the new opportunities provided by the DGA.

Connection to the other four proposals. The DGA proposal is most closely related to the proposed Data Act. While the DGA proposal deals with the governance framework, the Data Act should introduce new substantive rights on data, to solve the question of who is entitled to access and/or control which data.

DGA in a nutshell

Objective and relevance

- Make public-sector data available for reuse
- Facilitate the exchange of data in the EU and with third countries through data-sharing services
- Enable data sharing for the common good/data use on altruistic grounds
- Very relevant for the public sector, as it needs to deal with new types of requests for data

Who comes within its scope?

- Public sector
- Data-sharing “trust” services
- Individuals

Key obligations

- Confidentiality
- One-stop-shop mechanism for data requests

Key definitions

- Data
- Data altruism
- Data-sharing services

Regulator

- National supervisory authority
- Data Innovation Board
- Penalties decided at national level

2.2.2 Digital Markets Act (DMA)

On 15 December 2020, the European Commission published its Digital Services Package, which proposes two pieces of legislation: the DSA and the DMA. The latter represents the commission's ground-breaking set of proposals to challenge the power of the largest companies in the digital markets, which currently originate mainly from the US and China, while complementing EU competition law. According to an interviewed commission official, the proposal's aim is to bring back real competition to the European markets and enhance the effectiveness of the inner markets: in other words, the aim is to avoid becoming a data colony for other regions.

The DMA would apply to “gatekeepers” – online platforms offering core platform services – fulfilling a bottleneck function between companies and consumers for important digital services. Gatekeepers are deemed to have an entrenched market position, benefit from strong “network effects” and exercise market access control, with the result that other users (both consumers and businesses) are heavily reliant on these players. Lawmakers are concerned that this situation could result in anti-competitive practices and weak competition in the market. To combat these threats, the DMA contains ex ante obligations that can be applied before any wrongdoing takes place.

Gatekeepers can thus be large companies (such as Google, Apple, Meta, Microsoft, Amazon), although specific examples are not mentioned in the proposal. Responsibility for the designation of gatekeepers would rest with the commission according to the original proposal, but the member states have been pressing for more say in such decisions during the trilogue negotiations.

The DMA proposal sets out criteria for the definition of gatekeeper companies. In short, a company should be considered a gatekeeper if:

1. it has a significant impact on the internal market;
2. it maintains one or more important gateways for customers;
3. it has or is expected to have a firmly established and sustainable position with its activities.

Even if these quantitative criteria are not met, a company can be deemed to be a gatekeeper based on an additional qualitative analysis. Unlike in the context of the electronic communications sector, the criteria for the designation of gatekeepers under the DMA is not based on familiar competition law principles. Therefore, it is unclear how the criteria would work for the range of activities that platforms provide and how the qualitative criteria would be applied in practice. The DMA proposal may also enable the European Commission to regulate conduct and practices considered to give the largest firms an entrenched advantage.

The obligations laid out for gatekeepers in the proposals relate, for example, to the use of data, data access and portability, leveraging access to core platform services, platform neutrality and advertising. Any merger with another core platform service would entail an obligation to inform the commission, regardless of whether it comes under the scope of traditional EU merger control. Not being counted as a gatekeeper company means that there are fewer compliance obligations applicable. However, it is possible that a company previously not considered a gatekeeper could become one in the future. Non-gatekeepers can also profit from the proposals because they have more real opportunities to compete with gatekeeper companies. For example, gatekeepers must refrain from using in competition with business users any data not publicly available, which is generated through activities by those business users.

An important feature of the DMA – and an important difference to the DSA, too – is that in the commission's original proposal, the responsibility for the designation of gatekeepers and the supervision and enforcement of the

DMA lies with the European Commission and not with national authorities. However, as mentioned above, during the negotiations, some member states have resisted the idea that all the enforcement power should be at EU level. The reasons given for EU-level enforcement are that the DMA addresses pan-European (indeed global) firms and conduct, that there are only a limited number of gatekeepers and that national fragmentation of regulations must be avoided.

Fines for breach of duty could amount to a minimum of 4% and up to 20% of the annual turnover for the previous year in the case of repeated offences. To ensure that member states have a role to play, the proposal foresees that the commission consults with a Digital Markets Advisory Committee with member state

representatives before taking certain decisions (on non-compliance and fines, for instance).

Connection to the other four proposals. The DMA proposal is mostly connected to the DSA because they both apply to online digital services offered to customers and give the highest compliance responsibilities for the bigger players (gatekeepers and very large online platforms). The key difference is that the DMA tackles only issues related to gatekeepers, whereas the DSA also focuses on wider societal concerns. Because the DMA focuses more heavily on competition law and is only directed at specific companies, with enforcement happening at the EU level, it differs clearly from the other proposals that rely on national enforcement and are more about data regulation.

DMA in a nutshell

Objective and relevance

- Promote fair competition in digital markets
- Very relevant for SMEs, as it gives them a chance to participate better in the data economy

Who comes within its scope?

- Largest online platforms
- Online intermediation services
- Social networking
- Search engines
- Online marketplaces
- Advertising services etc.

Key definitions

- Gatekeeper
- Core platform service
- Online platform

Key obligations

- Transparency
- Due diligence
- Prohibition of unfair practices
- Interoperability
- Data portability
- Access for business users

Regulator

- European Commission
- Digital Markets Advisory Committee
- Fines of up to 10% of total worldwide turnover and 20% for repeated infringements

2.2.3 Digital Services Act (DSA)

The DSA is part of the same package of legislative proposals as the DMA. The DMA, introduced previously, includes rules that govern gatekeeper online platforms. Some of these services may also fall under the scope of the DSA proposal, but for different reasons and with different types of provisions. The DSA is designed to capture a wide range of digital services providers, with more far-reaching rules for the larger players, whereas the DMA will capture only a very limited number of the largest global players in the market.

The DSA proposal aims to clarify the responsibilities and obligations of online platforms regarding content provision and moderation, as well as the offering of products for sale in online marketplaces, while retaining the key principles of the e-Commerce Directive. The DSA is not intended to replace the e-Commerce Directive but will apply in addition to its national implementations. For the sake of clarity, the conditional exemptions from liability articles from the e-Commerce Directive are incorporated into the DSA.

Digital services include a large category of online services, from simple websites to internet infrastructure services and online platforms. The rules specified in the DSA primarily concern online intermediaries and platforms (online marketplaces, social networks, content-sharing platforms, app stores, online travel and accommodation platforms); the US companies Google, Apple, Meta and Amazon, and potentially the Chinese companies TikTok and Alibaba, although specific examples, are not mentioned in the proposal).

The DSA proposal is particularly relevant for large digital service and online advertising providers. The legislative proposal is based on the principle that “what is illegal offline is illegal online”. It emphasises the need for clearly defined procedures to counter illegal products, services and content on digital services, as well as transparency regarding targeted advertising and recommender systems.

In terms of scope, the obligations introduced in the DSA are comparable to the EU’s historic decisions to introduce regulation of the electronic communications sector and the financial sector. Its potential impact in terms of compliance responsibilities on digital service providers worldwide may be compared to that of the introduction of the GDPR. It is clear from the proposal that the pressure on the compliance departments of companies active in the digital sector will increase significantly.

The DSA proposal contains different obligations for different types of services or providers: in short, the lightest obligations apply to mere intermediary services, after which the obligations become progressively heavier, with the obligations imposed on very large online platforms (VLOPs) being the most stringent. VLOPs are considered to pose risks in terms of the dissemination of illegal content.

A complicating factor is that the definitions employed to distinguish the different categories of service providers, which are the starting point for the proposal, are not clearly aligned. This is particularly important because specific regulatory instruments are included for each category of service provider, so that companies will have to assess, in the context of compliance, which category or categories they fall under to assess which obligations apply to them. An illustration of the confusing definitions is that the DSA and the DMA use different terms/categories of service providers. For example, the DMA uses the term “core platform service”, with a definition that does not logically build on the service categories in the DSA, while the term “VLOP” does not appear in the DMA.

The proposal also introduces a new control mechanism and substantial fines (up to 6% of global turnover). In future, the responsibility for supervision will lie with the national authorities (Digital Services Coordinator), although the commission may intervene in the operation of very large online platforms.

In summary, although the DSA and the DMA are proposed in combination, they are in fact completely different instruments, both in

terms of the parties addressed and in terms of the framework of standards and procedures to be followed. The DMA and DSA are both currently at the same stage of the EU legislative process; the trilogue has been completed for both proposals.

Connection to the other four proposals. The DSA proposal was introduced together with the DMA and is mostly connected to this proposal. Still, these two

proposals have their differences, for example, the DGA is a horizontal instrument that applies to all actors. Additionally, it has a clear connection to the AIA, because targeting and other AI-driven technologies are also regulated in the DSA. The DSA also focuses on protecting the fundamental rights of consumers online, which also runs parallel to the AI Act, which includes measures to reduce consumer safety risks and fundamental rights violations.

DSA in a nutshell

Objective and relevance

- Strengthen the responsibilities and supervision of intermediary service providers to ensure online users less exposure to illegal content and products
- Relevant both for SMEs (participation in the digital economy) and individuals who will gain rights

Who comes within its scope?

- Intermediary service providers
- Social networks
- Online marketplaces
- Hosting services

Key definitions

- Intermediary services
- Hosting services
- Online platforms
- Very large platforms

Key obligations

- Transparency
 - Information obligations
 - Content moderation
 - Accountability; due diligence
 - Risk management
- Online advertising rules

Regulator

- National supervisory authority (Digital Services Coordinator)
- European Commission
- European Board for Digital Services
- Fines of up to 6% of global turnover

2.2.4 Artificial Intelligence Act (AIA)

On 21 April 2021, the commission published its proposal for the AIA to promote technology that works for people. The general purpose of the legislation is to strike a balance between the security of citizens and the development of new, innovative technologies. The AIA aims to ensure that AI systems in the EU internal market are safe and respect existing law on fundamental rights and European values, and to ensure legal certainty for facilitating investment and innovation in AI. This legislative proposal is the first in the EU to specifically bind providers and users of AI applications.

The AIA is largely based on a risk-based approach, differentiating between the uses of artificial intelligence (AI) that create:

1. an unacceptable risk, such as social scoring systems or using AI to exploit children or vulnerable people;
2. a high risk, with examples as diverse as using AI to assess the risk of a former prisoner reoffending, using AI to score exams or using an AI application in robot-assisted operations;
3. limited risk, such as the use of AI systems such as chat bots;
4. minimal risk, which is by far the largest category and includes, for example, the use of AI-enabled video games or spam filters.

The AIA would focus mostly on systems that are deemed to pose a high risk for fundamental rights and safety. A limited number of “unacceptable risk” systems will be prohibited

completely: these systems are regarded as contradicting basic EU values, such as fundamental rights.

The proposal would establish a European Artificial Intelligence Board, consisting of representatives of member states and of the commission. At national level, member states will have to designate one or more national competent authorities and, among them, the national supervisory authority, for the purpose of supervising the application and implementation of the regulation.

Currently, it is still unclear to what extent the AIA would ban certain technologies altogether for public service, such as the real-time use of facial recognition technologies. While the commission’s original proposal allowed for limited use of such real-time biometric identification for specific law-enforcement situations, many MEPs are pressing for a full prohibition of its use. This indicates that heated debates are coming in the next months. If both the council and the parliament do succeed in reaching their positions by mid-2022, then the trilogue negotiations between the European Commission, Council and Parliament can start in the second half of 2022 and are likely to continue into 2023.

Connection to the other four proposals. The AIA proposal was identified by many interviewees as a separate proposal, which has little connection to the other four proposals. It does, however, have some common ground with the DSA, because both proposals deal with the consequences of using AI-generated services, such as targeted advertising.

AIA in a nutshell

Objective and relevance

- Ensure that AI systems are safe and respect EU fundamental values
- Ensure legal certainty to facilitate investment and innovation in AI, strengthen the responsibilities and supervision of online platforms
- Relevant for companies as the rules for participating in this area of the data economy are expressed clearly

Who comes within its scope?

- Providers placing AI systems on the EU internal market
- Users of AI systems within the EU
- Providers and users of AI systems in a third country where the output is used in the EU

Key definitions

- AI System

Key obligations

- *Ex ante* risk assessments
- Respect for fundamental rights
- Transparency towards users
- Post-market monitoring, investigations and reporting

Regulator

- National authority
- European Artificial Intelligence Board

2.2.5 Data Act

The Data Act is the most recent of the Big Five proposals (published on 23 February 2022) and it sets common basic rules on who can use and access data across all economic sectors. According to the commission, this will help to unlock troves of industrial data that are currently unused as well as ensure fairness in the data value chain among all those within the data economy.

In brief, the proposal aims to facilitate access to and use of non-personal data, including business-to-business (B2B), business-to-consumer (B2C) and business-to-government (B2G). SMEs are set to benefit from the proposal's mandatory obligations on data holders to make their data available under fair, reasonable and non-discriminatory (FRAND) terms.

The rights of users to port data would also be spelt out more clearly. In addition, customers of data-processing services (including cloud computing) would also be able to switch service providers more easily.

This proposed legislation, which would introduce obligations for data access by design (or by default), is designed to complement the DGA framework for the sharing of private-sector data with the public sector. It includes the possibility for public bodies and EU

institutions to have free access to data held by enterprises in cases of “exceptional need” such as public emergencies, pandemics or disasters.

Finally, the proposal includes an amendment to the existing Database Directive to specify that databases containing machine-generated data are excluded from the protection of the *sui generis right*.

The regulatory scrutiny board identified multiple open questions in relation to the Data Act. As a case in point, the board called for a clear definition of “data”, more specifically the content and boundaries of this term, as well as clarification of the term “data ownership”. The board also thought that there should be a justification for why the Data Act limits the scope for consumers and companies to data generated by connected products and related services. This *de facto* excludes all data from software/web services, which could have been brought within its scope (European Commission 2022b, p. 6)

Connection to the other four proposals. The DA proposal has much in common with the DGA proposal, as mentioned before. While the DGA proposal introduces a governance framework, the Data Act introduces new substantive rights on data, to solve the question of who is entitled to access and/or control which data.

Data Act in a nutshell

Objective and relevance

- Facilitate access to and use of data, including business-to-business and business-to-government in exceptional cases
- Very relevant for SMEs as data portability requirements allow shifting between services; also, citizens will get new rights and old rights will be strengthened

Who comes within its scope?

- Private-sector organisations with sets of industrial data
- Public bodies and EU institutions
- Data-processing and cloud computing services
- Data generated by connected devices and related services

Key definitions

- What constitutes fairness in B2B contracts
- Public interest regarding B2G data sharing

Key obligations

- New rules on access and use of non-personal data
- Data portability obligations and facilitating switching
- Fair, reasonable and non-discriminatory approach in B2B data-sharing contracts
- Data access by design or default

Regulator

A set of standards likely to be developed by the commission through the European Standardisation System

2.3 Synopsis

2.3.1 The Big Five proposals pave the way for a fairer data economy

First, aligned with the vision of the data strategy, legislation is required to harmonise the currently fragmented legislation to fully capture the benefits of a thriving data economy. The proposals in the Big Five are clearly meant to support each other and together they aim to achieve a more competitive model that could serve as a leading role model for other

countries, as the GDPR did in creating a data-protection landscape worldwide.

Second, the current data market with the large players dominating the scene is unlikely to change by itself owing to the rising value of data, network effects and lack of economic incentive. The proposed European model can only work if, on the one hand, the Big Five proposals succeed in creating a new regulatory framework that facilitates growth and innovation and, on the other hand, this framework is supported by investment, research and upskilling.

Third, the GDPR was the starting point for resetting the way the largest players handle their data and has set an example for regulators elsewhere (such as in Brazil, India and California), creating the so-called Brussels effect (Bradford 2020). The perceived success of the GDPR in setting a high global standard for data protection has clearly been used as a benchmark for the Big Five. The GDPR has not helped SMEs and consumers to be less affected by the role of the largest players in the market. The legislative proposals aim to tackle this issue.

The proposals in the Big Five are clearly meant to support each other and together they aim to achieve a more competitive model that could serve as a leading role model for other countries, as the GDPR did in creating a data-protection landscape worldwide.

2.3.2 Questions to answer

While the Big Five proposals are in many ways ground-breaking, some uncertainties seem to lie in the implementation and application of the proposed rules. Most of the proposals are indeed just proposals and thus changes are still possible – especially for proposals that are only in the negotiation stages of the legislative process (the DA, AIA and DSA).

With all five proposals, the lack of clarity of some provisions appears to be a challenge. Concepts such as gatekeeper, intermediary service and online platform are in principle

defined in the proposals, however it is hard to understand who exactly falls under these (or other) concepts. This also leaves quite a lot of power with the member states or the commission to decide on proper interpretations.

The former scenario can lead to unwanted fragmentation, a phenomenon already seen with the GDPR, with basic terms such as the controller being open to interpretation. In the case of the term gatekeeper, the commission also has the option to include companies that do not meet the thresholds. Even within some proposals, further clarifications are necessary; for example, the distinction between different levels of risk in the AI proposal are quite blurred with some AI systems likely to fit into several categories.

Furthermore, the interplay between the Big Five proposals and the existing legislation, such as with data-protection rules, competition law and intellectual property legislation, is not clear-cut. For example, the provisions in the proposed DA on data sharing could have a potential impact on proprietary data protected by the IP, such as trade secrets. While references are made to existing legislation, the proposals still use their own terminology, which makes it harder to interpret the proposals together with the existing legislation.

From this perspective, the complexity of the legal framework is increasing because of overlapping regulatory instruments and the use of terms that are not aligned. This complexity is likely to make it more difficult for businesses and citizens to understand the rules and for industry to ensure compliance. This concern is further fuelled by the fact that the proposals will not be supervised by a single authority in the member states, but potentially by separate competent bodies with overlapping competences.

3 The Big Five proposals in relation to the vision and objectives of the data strategy

In this chapter we will analyse what the Big Five means for different stakeholder groups: individuals, businesses and the public sector in Finland. The purpose is to understand the opportunities the governance model proposed by the commission presents and examine whether it is fit for purpose as presented in the data strategy. The lists are by no means exhaustive but largely a reflection of the stakeholder consultation conducted as part of this study. As a method, both fictitious and real-life examples are used to demonstrate the opportunities presented by the Big Five proposals.

3.1 What do the Big Five mean for individuals?

The European Data Strategy puts individuals front and centre of the data economy policy, recognising their role generating ever-increasing amounts of data. Citizens should gain fair benefits from data-driven business and innovation without compromising their fundamental rights and freedoms.

The Big Five will grant people new, and strengthen already existing, enforceable rights to their data. This represents a paradigm shift for individuals, from being the object or source of data for the benefit of the industry. In addition, the Big Five regulate the data market, which creates indirect benefits for people. For example, the DMA should serve to create competition in the market, resulting in more choice and lower prices for many people.

3.1.1 Access to data generated using connected devices

Right to data portability – what does it mean for individuals?

One significant change introduced by the proposed Data Act is the right to data portability. This right allows people to obtain and reuse data generated by using connected products.

On request, a company is obliged to make available to any individual the data generated by their use of a relevant product or service, without undue delay, free of charge and, where applicable, continuously and in real time. The data must be provided to the person or to a third party, such as to another service provider, depending on the request. Hence, it will make it easier for people to switch between service providers without negative consequences.

Data portability – what if you could transfer your car data?

Data portability means that individuals can copy and transfer their data easily from one service provider to another.

Modern cars are like computers that collect vast amounts of data about the car, its driver and surrounding traffic. Under the Data Act, a car owner could choose to share data generated from using the car with, for example, another car maintenance service provider other than the original manufacturer (European Commission 2021e).

What products come within the scope of the Data Act?

The data in this case refers to any data generated by the use of a connected device, both personal and non-personal data. A connected product means a physical product that can collect or generate data on the use of the product and that can connect the data via the internet. This definition would cover a wide range of products (Article 2 of the Data Act), such as:

- household appliances like smart fridges;
- virtual assistants like Siri;
- connected vehicles like modern cars;
- health and fitness trackers;
- agricultural or industrial machinery.

Moreover, devices whose primary function is to store or process data do not fall within the scope of the Data Act, including items such as laptops, smartphones and cameras.

What is new and what is not?

The core idea behind data portability is not new. The GDPR introduced a similar right but due to its limitations and practical implementation, there has been little progress

with respect to organisations making data available to individuals. Under the GDPR, data portability is limited to personal data processed on certain grounds and where technically feasible.

The proposed Data Act introduces a reinforced data portability right that will apply irrespective of whether it is personal data or not, irrespective of whether the data is actively provided by the individual or not, and irrespective of the ground on which the company processes such data in the first place. Under the proposed Data Act, the right to data portability would be much broader than today.

What can be expected?

This right will have an impact on a broad range of businesses across sectors and oblige them to make available data that once was collected only for the benefit of the business. In practical terms, this right will require technical solutions and investments from businesses to enable interoperability. This might eventually be reflected in consumer prices in the short run, but in the long run it will help to increase competition, innovation and consumer choice and hence lower prices.

3.1.2 Control over ads shown online

Background

Online services, like social media platforms, use “recommender systems”, algorithms that determine what their users see and what information should be promoted to them, like the next product to buy, the next video to watch or the next news item to appear at the top of a user’s social media feed. Larger platforms especially have an important role to play with respect to consumers because of the way users find and access information online. Hence, the commission is concerned that these services could be misused to also amplify disinformation to the detriment of quality news or that the financial imperative to increase clicks could prevail over providing access to reliable information sources. The proposed DSA and DMA aim to address this challenge.

New online rights

The DSA will introduce new enforceable online rights. Under the proposed DSA, people can report illegal content they encounter online or dispute any decision by the service provider to suspend or block access to content they have themselves posted online. Illegal content can refer, for example, to hate speech or defamatory content.

One of the key rights for citizens is the right to be informed. Online services need to tell people when an ad is displayed, who is behind the ad and why an ad was shown to the user. The purpose is to help people learn about the way ads are targeted towards them and give them the opportunity to recognise and decline such advertising in the future.

In addition, VLOPs (such as Facebook and Google) must explain to people why specific content is recommended. VLOPs have to disclose the main parameters of their recommendation systems and provide the option to modify these parameters and even allow people to choose to use the service without these personalised recommendations. The strictest obligations apply to VLOPs, which are deemed to have a strong influence on the content people see through their recommender systems.

Defamation online

A social media account is held by someone from a minority group. One day the person in question notices that his pictures have been put online with defamatory text after he published posts supporting a specific political cause. Under the proposed DSA, this individual can notify online platforms of illegal content online using a notice-and-action mechanism. Illegal content can refer, for example, to hate speech or defamatory content.

Targeted advertising online

Christine is surfing online and encounters targeted advertising. She has been visiting a lot of websites for pet products as she is getting a new puppy next week. Suddenly, advertising for such products turn up on all of her social media pages, also on those only on her phone, although she has made relevant searches only on her laptop. Christine is worried that she is no longer in control of her digital identity. Under the proposed DSA, Christine has the right to receive information from the online service provider to make it clear that the information displayed is an advertisement, who is behind the ad and why the ad was displayed to her.

What is new and what is not?

Targeted advertising is to some extent already regulated by the GDPR and the ePrivacy Directive. The GDPR already establishes, for example, rules on users' consent or their right to object to targeted advertising. The ePrivacy Directive in turn regulates the use of cookies and requires user consent for the use of advertising cookies. The DSA and the DMA mark a step forward in terms of empowering people to control ads displayed on their social media feed, by search engines and online stores.

What can be expected?

While the DSA is a rather fundamental step towards control for users over the recommendation metrics, it has some weaknesses. VLOPs must provide this information in their terms and conditions, but users do not usually read the terms and conditions, and if they do, they are also unlikely to modify or choose an option not based on profiling (Internet Policy Review 2021). Hence, the suggestion to offer that

information on a more prominent part of the website would seem to be a better option going forward (EDPS 2021).

3.1.3 Rules on AI to create trust

What is AI and how is it used today?

AI involves using computers to do things that traditionally are done by people. The following provide a few examples of applications using AI on a daily basis.

- Face ID uses AI for unlocking phones or allows Snapchat to detect a user's face.
- Navigation apps like Google Maps use AI to analyse the speed of movement of traffic.
- Digital smart assistants such as Siri, Alexa and Google Assistant use AI to take voice commands and translate them into actions, such as calling a friend.
- Netflix and YouTube use AI when they propose movies or videos users may enjoy watching next.
- Uber and other taxi apps use AI to determine the price of a ride or the wait time.

How about the future – what could AI bring to people?

AI can assist (and already assists) people in every area of our lives. AI can make routine processes, such as parking a car, easier for people to perform. AI can optimise existing processes, like navigation and use of maps, and enable new connected devices, like autonomous vehicles. AI can be used to improve the speed and quality of public services, like quicker welfare payments.

AI presents new opportunities and efficiencies, and this technology can be harnessed in positive ways to support Europe's green and digital transitions. These have a great potential to make our lives more convenient and provide solutions to issues such as more effective traffic management and reducing environmental pollution.

However, the use of AI also comes with considerable risks and has major implications

for citizens' self-determination and their privacy. Most algorithms are non-transparent, making it difficult for users to understand that AI is used in the first place, how these systems work and how to influence them. Moreover, AI systems can personalise content by assessing a user's interests, but this may not always be done with the user's interests in mind, but rather the financial interests of the companies, as is evident in the case of Cambridge Analytica.

Trust is an essential element for the use of AI

The proposed AIA is the first comprehensive attempt globally to regulate AI. The goal of the proposal is to define clear rules for AI applications and hence to increase the confidence of citizens in the use of AI-enabled products and services. In line with the human-centric approach of the data strategy, the AIA proposal takes a risk-based approach to AI systems. Thereby, AI that intends to manipulate people and cause harm is systematically forbidden.

Second, the new rules for AI aim to create more legal certainty allowing AI providers to access bigger markets, with products that consumers and businesses can have confidence in and will purchase.

Cambridge Analytica and the use without consent

Political consulting firm Cambridge Analytica harvested the data of millions of Facebook users without their consent and performed data analysis on this information for the purposes of influencing elections in the UK and the US from 2014 to 2016. AI played a key role as it was used to automatically test hundreds or even thousands of variations of an ad before deciding which one to present to voters.

Trusting AI

AI could be used in many ways by public administration and businesses. For example, public authorities like the Social Insurance Institution of Finland (Kela) could use AI in determining welfare payments such as housing allowances, student grants or parental allowances in future. Today, AI is not really utilised in actual decision-making because there are no clear rules on the use of AI and many people think that AI is risky. The Finnish Chancellor of Justice has delivered a decision, stating that there was no legal basis for automated decision-making in Kela but that regulatory needs should be identified quickly (Oikeuskansleri 2021).

The proposed AIA might help to create trust, as it tries to define clear rules for AI applications in legislation. It also introduces a risk-based approach and includes transparency obligations. All those measures will increase trust in AI and potentially improve the speed and quality of, for example, public services.

3.2 What do the proposed measures mean for the public sector?

The data strategy recognised public data alongside non-personal industrial data as “a potential source of growth and innovation that should be tapped”. Public-sector data should be available to benefit the public good and others in the data economy. In addition to being a source of valuable data, the public sector is set to benefit from better access to and use of data (such as

better governance and decision-making, and resource-efficient public services).

The Big Five vest new powers and obligations in national regulators but also introduce completely new enforcement bodies, which should be organised at a national level. This will most likely lead to different outcomes in different member states. At the same time, the proposals aim to promote the overall digitalisation of the public sector and facilitate the reuse of data therein.

3.2.1 Reuse of data in the public sector

The DGA facilitates public data sharing between the government and citizens and reuse of this data for the benefit of the development of personalised medicine or advance research to find cures for specific diseases, for example, or for the public sector to improve services. Better access to data will allow more evidence-based decisions and policies to be developed, which again will benefit society at large.

Mobility data in smart cities

Local governments generally consider using mobility data for a variety of purposes. A number of these purposes rely on the insights that the mobility data (once aggregated) provide regarding the mobility of individuals in the territories of local governments. Under the DGA, cities hope to use these insights to make better city planning decisions such as where to put parking locations for bikes, protected bike lanes and traffic lights. The insights may also be of use for related purposes around infrastructure management, city planning and allocation of resources.

This idea about reuse of data is not new in Finland. A good example is the Act on Secondary Use of Health and Social Data enabling reuse of health data in Finland in line with the GDPR.

The rules of the DGA will also trigger an obligation for public bodies to make data available to the private sector for non-commercial and commercial purposes. The DGA should make it easier for companies or non-profit organisations to access these data sets. However, the DGA does not trigger an obligation for public bodies to allow further use of data. Public authorities must ensure that such data remains protected during further use, for example through confidentiality obligations or data aggregation in such a way that it can no longer be attributed to a specific company.

In Finland, public-sector data has been made available through avoindata.fi, provided by the Finnish Digital and Population Data Services Agency (DVV). [Avoindata.fi](https://avoindata.fi) is a service for publishing and utilising open data. Much of the data on the service is published by different government agencies, municipalities and other public administration organisation. However, companies, associations and individuals can also publish open data on the service. It makes all Finnish open data available in one place. Therefore, the DGA will support and further enhance the access to and reuse of public-sector data in Finland.

The reuse of data under the DGA must be reconciled with the Finnish Act on the Openness of Government Activities (621/1999). Under the Act, everyone has the right to obtain information from official documents in the public domain. The Finnish right to access public documents does not now entail the right to reuse the data for commercial purposes. Thus, if the Finnish Act is not reviewed by the legislator, the reconciliation of the two will remain in the hands of different authorities depending on the purpose of the use of the data.

Data sharing in exceptional situations

During the Covid-19 pandemic, aggregated and anonymised location data from mobile network operators was essential for analysing the correlation of mobility and the spread of the virus. Under the proposed Data Act, businesses will need to provide certain data to public authorities in public emergency situations of high public interest, such as floods or wildfires.

3.2.2 Increased use of AI on the public sector

How is the public sector using AI today?

In Finland, the public administration already uses AI. Within the public sector, AI could be used in many ways: to design better policies and make better decisions, improve communication and engagement with citizens and residents, and improve the speed and quality of public services (OECD 2019). Below, we list a few examples of public-sector applications using AI in Finland daily.

- Chatbots and virtual assistants help people by answering their frequently asked questions. For example, the Kamu chatbot used by the Finnish Immigration Service.
- [Omaolo](https://omaolo.fi) uses AI to carry out preliminary analysis of Covid-19 symptoms based on a predetermined questionnaire and gives a recommendation on whether one should take a Covid-19 test.
- AI is used to make an assessment of the need for dental treatment in Finland.

Furthermore, there are interesting government programmes to follow in this respect, like the development of an e-ID for Finnish citizens and residents in Finland (Finnish Ministry of Finance on eID) and the AuroraAI service used to identify which services are most useful to people and to provide them with tailored

recommendations on services they might be interested in (Finnish Ministry of Finance on AuroraAI), to name just two.

In what other ways could the public sector use AI?

In the future, AI will also perform work tasks and duties that we still believe we need people for today. At present, AI is rarely, if ever, used in final decision-making in public administration, such as to determine access to education or grade exams, or to determine welfare payments and immigration decisions. AI systems making decisions in these areas would be classified as high-risk applications under the proposed AIA. As these decisions might have detrimental consequences for individuals, more stringent obligations would apply, including accountability and transparency obligations and thus increased compliance costs. All these measures should increase the confidence of citizens in these AI products but it also sets the bar higher for the potential use of AI by the public administration.

3.2.3 New powers and new authorities

The Big Five provide for the establishment of supervisory authorities and new European co-operation bodies between these authorities (known as European Boards). An important feature of the DMA – and an important difference to the other four proposals – is that the supervision and enforcement of the DMA lies with the European Commission although there are still discussions about also potentially giving a role to national authorities. The other proposals (DGA, DSA, AIA, DA) rely on national supervisory authorities and allow member states to designate one or more authorities for each proposal.

Under the Big Five, the competence to monitor compliance is not clearly afforded to any existing authorities, such as data-protection authorities. Member states can independently establish completely new authorities for some or all four proposals or can designate the powers to existing authorities.

Municipalities and AI

AI could be used in many ways by public authorities. Frontline public services, like public healthcare and comprehensive schools, are organised by municipalities in Finland. Municipalities could use AI to replace certain traditional and manually delivered functions, like customer service, and generate labour and costs savings. In addition, municipalities could examine ways of using AI in decision-making.

The AIA lays out responsibilities for those who use high-risk AI systems and introduces transparency obligations. All those measures will increase trust in AI and potentially improve the speed and quality of public services as well as save costs in the long run.

Table 2: Competences to monitor compliance under the Big Five proposals

Legislative proposal	EU/member state supervision	Supervisory authority	Advisory board at EU level	Sanctions
DGA	Member state	Member state; one or more authorities	European Data Innovation Board	Member state to decide
DMA	EU	European Commission (but discussion still ongoing about the role of member states)	Digital Markets Advisory Committee	Fines of up to 10% of total global annual turnover and 20% for repeated infringements
DSA	Divided between member states and the EU	1. Member state; one or more authorities 2. European Commission will supervise VLOPs	European Board for Digital Services	Fines equating to 6% of global annual turnover
AI	Member state	Member state; one or more authorities	European Artificial Intelligence Board	1. Fines of €10 million or 2% of global annual turnover 2. €20 million or 4% of global annual turnover 3. €30 million or 6% of global annual turnover
DA	Member state	Member state; one or more authorities	N/A	Member state to decide

Some interviewees highlighted enforcement as one of the biggest risks to regulatory failure. This concern is grounded in the experience of the GDPR. The GDPR was criticised as an “enforcement failure” by several interviewees and it was stressed that the commission should learn from its mistakes with the GDPR as otherwise the Big Five will fail to meet the vision and objective of creating a single market for data in the EU.

GDPR supervision and enforcement

National data-protection authorities are responsible for supervising compliance with the GDPR on their territory. Where cases involve cross-border processing (data processing in more than one member state), national authorities co-operate through a one-stop-shop mechanism. The lead authority will lead the co-operation procedure and draft the initial enforcement decision. This will then be reviewed by other relevant national authorities. For the company or public body under investigation, the lead authority will be its point of contact in relation to investigation and enforcement.

The European Data Protection Board (EDPB), consisting of national data-protection authorities, is an independent European body whose purpose is to ensure consistent application of the GDPR and to promote co-operation among the EU member states’ data-protection authorities. One of the key responsibilities of the EDPB is to ensure consistent application of the GDPR across the EU. This has taken the form of publishing general guidelines and reports.

Despite the great efforts to harmonise data-protection rules across the EU, enforcement of the GDPR has created administrative burdens and duplication of costs since each EU member state seems to have their own rules, guidance and interpretation. This means that companies are obliged to tailor their services to 27 member states rather than one uniform set of requirements. One EU parliament official we interviewed in particular warned that the Big Five should avoid the fragmentation on the enforcement and governance level that has been a practical issue with the GDPR.

3.2.4 What would this all mean for Finland?

Finland must designate appropriate authorities to supervise compliance with the DGA, the DSA, the AIA and the DA. The decision is subject to a political process nationally, and below we have illustrated some options detailing how authorities in Finland could be structured.

- **Finland could establish a new authority/ies.** The amount of new legislation will lead to a search for suitable experts. Given that there will be many businesses and public authorities across the EU (and globally) searching for these skilled people, the concentration of know-how in the hands of one new authority could be a better option than the creation of several new authorities. Harmonisation is more likely to be achieved through the centralisation of enforcement and competence pooling.
- **Finland could designate the supervision to an existing authority/ies.** There are regulators with somewhat overlapping competences with respect to the Big Five (the Finnish Data Protection Ombudsman (DPA), the Finnish Transport and Communications Agency (Traficom) and the Finnish Competition and Consumer Agency (FCCA)). Where there are several competent authorities, competence could be afforded as

per each proposal, or each proposal could be divided into two or more authorities based on substance matter. The latter option creates a risk of parallel supervision structures where different competent authorities supervise the same entities performing the same activities without structured co-operation between them.

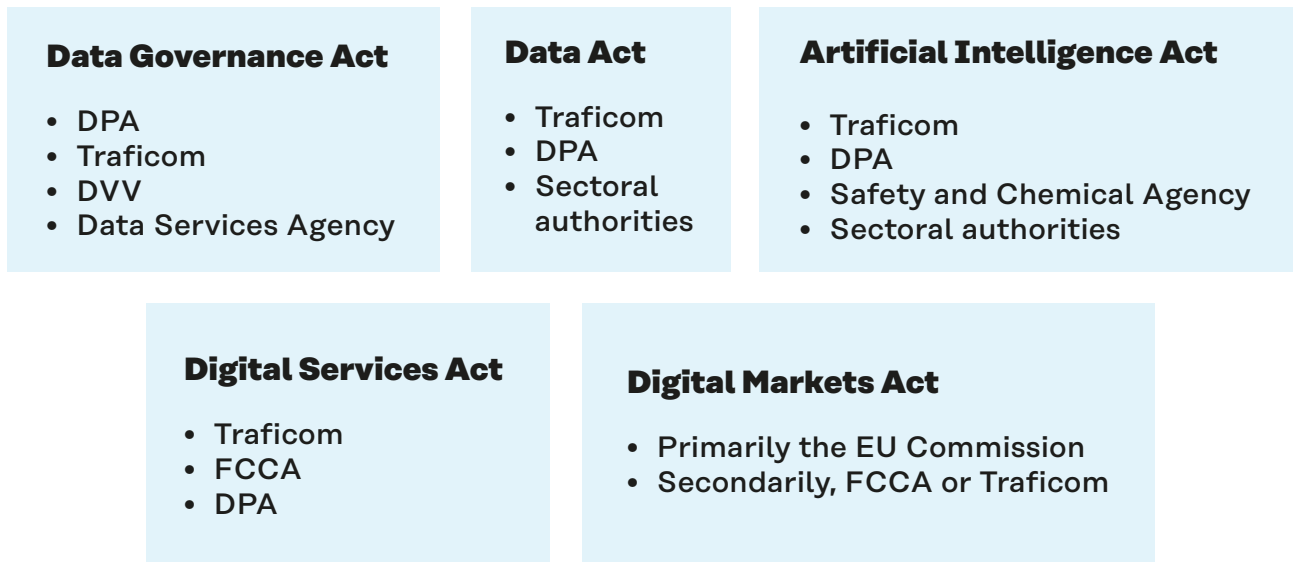
The processing of personal data is central to the activities regulated by the Big Five and, thus, the DPA could be designated as the main competent authority in Finland. While this would ease the interplay between the Big Five and the GDPR, the centralisation of power around the DPA is not without problems. First, this designation would label these proposals as “data-protection proposals” even though this is

not the case. Second, the Big Five would place a heavy enforcement burden on the DPA and its resources.

Traficom is most likely best equipped with the needed skills and resources. Traficom oversees telecoms regulations and the ePrivacy Directive (partly) and acts as the point of contact under the NIS Directive, among other things. Hence, Traficom has the technical know-how and most likely the broadest expertise and skill set in terms of digital services in Finland.

The FCCA is currently predominantly a competition and consumer protection authority. Therefore, it could have the best understanding for DMA enforcement, but could be lacking experience when it comes to the other areas of law.

Figure 4: Options for authorities for organising compliance supervision in Finland



Case example: enforcement of rules on cookies in Finland

When it comes to cookie rules under the ePrivacy Directive, there is an overlap in terms of regulators in Finland. Traficom is the competent authority when it comes to enforcing the Act on Electronic Communications Services (917/2014, ECS) which includes legislation on cookies (Section 205 of the ECS). The DPA is the competent body when it comes to enforcement action in relation to personal data processing, for example monitoring the publishing of the consent needed to process certain cookies (and similar technologies).

This led to different recommendations and decisions being issued by each authority regarding cookies. In the end, the ambiguity led to the matter being brought before the Helsinki Administrative Court in Spring 2021. The Administrative Court of Helsinki has confirmed in its recent rulings (Decisions H1515/2021 and H1516/2021, issued on 8 April 2021) that Traficom is the competent authority when it comes to enforcement of Section 205 of the ECS, the so-called cookie provision. These rulings are examples of the types of silos and unwillingness to co-operate that ultimately may be created as a result of divided supervision and enforcement.

Case example: enforcement of the NIS Directive in Finland

One example of divided powers among authorities is the implementation of the NIS Directive in Finland. While Traficom acts as Finland's point of contact for engagement with EU member states, the monitoring has also spread to several sectoral authorities in Finland:

- Transport – Traficom
- Energy supply – the Energy Authority
- Healthcare – Valvira
- Financial sector – the Financial Supervisory Authority
- Financial market infrastructure – the Financial Supervisory Authority
- Water supply – ELY Centres
- Digital infrastructure – Traficom
- Digital services – Traficom

The division of power between authorities is common in Finland, but as the case examples show, not without challenges under existing law. With the Big Five coming, the challenges of overlapping enforcement will multiply, leading to fragmentation of the vision and objectives of the data strategy.

One co-ordinating authority

An additional option could be to designate a single authority to co-ordinate and monitor uniform application in Finland. This could take several different forms.

First, each proposal could be designated to one or more authorities based on substance matter, but one authority would act as a co-ordinator, ensuring that authorities consult each other in matters of mutual concern, for example when new instructions are prepared, cross-border investigations are initiated or sanctions are imposed. This co-operation should not be voluntary but based on clear provisions in national law.

Second, sanctions under the Big Five could be imposed by a separate sanctions board consisting of relevant officials of each supervising authority. The idea behind a sanctions board is not new in Finland but was introduced by the Finnish Data Protection Act (1050/2018). However, in this case the sanctions board would consist of competent authorities ensuring that all relevant perspectives and the overall objectives of the Big Five are considered when imposing sanctions.

Third, another idea suggested by stakeholders in the study was the introduction of a respective Finnish Board for each proposal. These Finnish Boards would have the same function as the European Boards introduced by some proposals. Finnish Boards could ensure the coherent and harmonised application of the Big Five in Finland in line with the European Data Strategy and guidance provided by the European Boards.

3.3 What do the proposed measures mean for businesses and especially for SMEs?

The data strategy recognises the importance of securely opening up business data for the public good and to boost data-driven business in other companies. Businesses are set to benefit from better access to data (for decision-making, for example) and opportunities (such as developing tools for data producers to increase control over their own data, fairer market conditions or building on the scale of the single market for data).

The Big Five will entail a wave of new obligations but also new opportunities for the private sector in the EU. At its best, the Big Five can help to create an environment of trust which again will play an important role in promoting new business opportunities.

3.3.1. Levelling the playing field may increase competition

Most interviewees highlighted the importance of the DMA and the DSA in levelling the playing field in the digital market, which would allow SMEs to emerge and compete without the large players dominating the market unfairly. This finding is in line with the public consultation on the Digital Services Act Package by the European Commission. In the public consultation, most challenges were perceived to be due to an imbalance in bargaining power between platforms and business users, which is considered to hamper competition, foster uncertainty in relation to contractual terms and result in the lock-in of consumers (European Commission 2020e).

Similarly, the proposed DA could potentially level the playing field. First, it introduces the reinforced data portability right and hence businesses will be obliged to provide the data generated by connected products to their users (individuals and businesses). This would ultimately give users more choice in terms of service providers and increase competition in

the market. Second, the proposed DA encompasses a range of measures supporting SMEs, for example by granting a shield from “unfair contractual terms” imposed by a party with a significantly stronger bargaining position and the prospect of new model contractual terms for businesses to negotiate data-sharing contracts.

Competition in the email sector and bundling restrictions

Email provider EP is offering a non-bundled emails service, meaning that the email service is offered as a freestanding service and not as a part of another service. EP had a hard time finding customers, as many of them have bought phones that come with pre-installed email services. So far, EP's services have mostly been used by people who have special knowledge of bundling and want to support a smaller provider; their product was thus in no way competing with bundled email services.

The proposed DMA will level the playing field by restricting bundling through forced sign-ins. Also, EP will gain access to all the relevant app stores. This new development should help EP to expand and allow consumers to choose the best provider for themselves.

3.3.2 Changes will not impact everyone in the same way

Broadest impact on companies

Participants in the study highlighted the AIA and the DA as being key proposals to follow. The AIA will have a broad impact on businesses as it will apply to any provider and user of AI, irrespective of their size. SMEs will not be exempted from obligations under the AIA. The proposed DA also has a broad scope. It would apply to basically all the players in the Internet of Things (IoT) value chain, with particular focus on the IoT product manufacturers and the suppliers of related services.

The largest companies are regulated heavily

The DMA and the DSA set the strictest obligations on largest digital players in the market. The DMA only applies to the very largest firms, although SMEs can also benefit from the new obligations placed on “Big Tech”. However, a range of online services will be affected by the due diligence and transparency obligations set out in the DSA, such as internet service providers, cloud services, messaging services, marketplaces and social networks.

Meanwhile, the DGA is set to introduce a new business governance model and will apply to businesses wishing to act as intermediary service providers or as data altruism organisations.

What can be expected in terms of implementation?

The resources and budget needed will be of similar magnitude to the GDPR. A proper compliance project will take time. It may require technical solutions (such as data portability and interoperability), documentation (related to transparency and accountability, for example) and an overall accountability framework within a company, including responsible persons and training, just to name a few key implications for any business.

A preparation checklist for businesses

1. Start today.
2. Name responsible persons and identify relevant stakeholders.
3. Allocate budget and resources for your compliance project.
4. Map where your business is today (current legislation vs new proposals).
5. Identify the key proposals for your business but understand that the Big Five form the big picture, supplemented by sectoral legislation.
6. Prioritise actions and start executing.

Table 3: The Big Five contain exemptions and support for SMEs

Proposal	EXEMPTIONS OR SUPPORT FOR SMEs?
DGA	No (but indirect impact on SMEs).
DMA	Yes (indirectly, as bigger companies are submitted to stricter rules).
DSA	Yes, exemptions. Start-ups and small companies exempted from the transparency and due diligence obligations (Articles 13 and 16-24). This may be expanded to medium-sized companies during the negotiations.
AIA	Yes, support. Start-ups and small companies can get the following support (Article 55) <ol style="list-style-type: none"> 1. Priority access to the AI regulatory sandboxes to test AI systems in development and pre-marketing phases. 2. Specific awareness raising activities. 3. Dedicated channel for communication to provide guidance and respond to queries about the AIA.
DA	Yes, exemptions and support. Start-ups and SMEs are exempted from B2C and B2B data-sharing obligations (Chapter II) and from making data available to the public sector in exceptional circumstances (Chapter V). Support is afforded to start-ups and SMEs to protect against unfair contractual terms unilaterally imposed on them (Article 13) and they may benefit from the deployment of model contractual terms (Article 34).

More compliance projects

Despite some exemptions and support afforded to start-ups and SMEs, legal complexity will be increased because of the Big Five, and this is likely to make it more difficult for businesses, especially SMEs, to understand the rules and comply with them. This complexity will increase legal compliance costs as it is likely that the compliance work will require specialised knowledge that SMEs can only obtain through external legal counsels and consultants. Larger companies have in-house counsels and resources to access legal support when necessary. Some of the interviewees representing businesses estimated that the costs will be of similar magnitude to the GDPR.

Most of our interviewees highlighted that the main concern in this respect is related to enforcement. There is a risk of having to adapt their services to potentially 27 different sets of rules (even if the use of regulations as opposed to directives will harmonise the legal frameworks to a large extent), which does not just inhibit growth across the EU, but also globally. Unco-ordinated national enforcement creates additional hurdles for smaller businesses and start-ups, who will face significant compliance

costs in order to comply with all the different legislations.

3.3.3 Business opportunities

The Big Five will not, as such, create new business but they may help to create an environment of trust, which again will play an important role in promoting new business opportunities.

The opportunities may lie on the horizon for those who seek to act as data intermediaries or data altruism organisations under the DGA, or businesses who seek to expand their business, for example by utilising AI. Although many interviewees stated that the AIA is in many ways controversial, the rules on AI may still increase confidence and trust among consumers and make it easier to sell and promote AI applications to businesses and increase their acceptance by consumers.

Based on interviews and literature, we have already seen examples of new business opportunities and opportunities to scale up existing business. We have illustrated a few examples below.

Examples of identified business opportunities

MyData Operator

Vastuu Group is the first MyData operator in Finland. A MyData operator is a provider of infrastructure for personal data management and a key element in creating sustainable ecosystems for the fair and ethical use of personal data. The platform has a key role in managing consent and identification of persons. A MyData operator does not collect data but creates trust between the parties disclosing and using data. The DGA creates a framework for data intermediaries and thus builds trust in the service.

Fighting Covid-19 with data altruism

The German Robert Koch Institute launched a Corona Data Donation App in April 2020. Users can share their health data created by fitness trackers like Polar or Fitbit, for example. The intention is to map hot spots of the pandemic, by analysing the donated data. The app collects health data from the users' wristband fitness devices in anonymised data packages and then merges it with other data sources to understand how the virus may spread. Despite over 500 thousand users, the app has attracted criticism over fears associated with the vague term "data donation". The DGA should make it easier to collect data from the participants for voluntary purposes by creating the framework for data altruism organisations.

Personal data banking – a way to secure data storage

Consumers disclose large amounts of personal data daily without giving much thought to its value. A company called Orbiter aims to give consumers more control over how their data gets used.

The product Identio.one provides the consumer with a verified, digital identity. Identio.one enables the consumer to give third parties consent for using their personal data (and to withdraw their consent). In short, it acts as the "data broker," between the consumer and companies wanting to use their data. The DGA creates a governance framework for action undertaken by Orbiter – and many others.

AI governance and transparency

Saidot is a platform which is designed to enable organisations to develop and deploy AI products in a responsible way by applying governance, transparency and accountability practices. The AIA would help Saidot to expand and help businesses and consumers to trust AI.

Secure data sharing in a supply chain

ONCITE enables companies to process and store data on site before exchanging it via a public cloud – while ensuring data sovereignty throughout the whole process. This can help to increase trust with other businesses and to encourage B2B data sharing that is needed for new innovations and business models. ONCITE is a compact computing centre based on cloud technology. The user interface of the system monitors and controls any exchange of data between two partners. It is expected that the Data Act will create a governance system for this type of data sharing to take place in an even more regulated and safe format.

Facilitating secure B2B sharing

Deutsche Telekom developed a solution for encouraging data access using the Telekom Data Intelligence Hub. This hub enables companies to exchange their data through a secure business ecosystem. The hub is intended to serve as a digital connection between companies and a source for commercial data acquisition. The platform offers users tools for analysis, acquisition, exchange and processing of data.

The hub aims to share data B2B: this type of data sharing is currently not happening enough due to trust issues and a lack of safe and secure platforms for data sharing. It is expected that the Data Act will create a governance system for this type of data sharing to take place in an even more regulated and safe format.

3.4 How well do the Big Five meet the objectives of the European Data Strategy?

Table 4: The objectives of the data strategy and how the Big Five proposals contribute to them

Aims of the data strategy	Big Five contribution
To make Europe a global leader in a data-driven society	<ul style="list-style-type: none"> Regulating the largest players, even those originating from outside the EU (the “Brussels effect”) The DMA promotes fair competition and contestable digital markets by setting new obligations for gatekeepers and enforcing those obligations with heavy sanctions. The AIA is the first comprehensive regulation targeting Artificial Intelligence and could act as an inspiration for other countries as well (in the same way as the GDPR).
Free flow of data within the EU and across sectors	<ul style="list-style-type: none"> Encouraging data sharing among all data economy participants The DGA enables data sharing via data intermediation and data altruism for the public good. To that end, it aims to increase trust in the use of the services. DA enables data sharing B2B but also B2G in exceptional circumstances (such as a pandemic).
Availability of high-quality data to create and innovate	<ul style="list-style-type: none"> Ensuring that data is shared and available for AI systems, for example The DGA facilitates the use and sharing of data and provides wider access to public-sector data. The DGA supports the use of specific technologies (like AI) and drives the type of data collaborations necessary to support AI projects and innovation.
European rules and values are respected	<ul style="list-style-type: none"> A paradigm shift from responsive and sector-specific legislation to more general ex ante regulation to ensure that European values (like data sovereignty) are upheld The DGA and the intermediation services (such as trust services) could provide SMEs and individuals with greater transparency and control over their data. The DSA, the AIA and the DA set transparency obligations that further support those in the GDPR to empower individuals and make existing rights even more enforceable. The DMA and the DGA try to strengthen European values also among services that are not originally offered by European companies.

3.4.1 How do the Big Five support the data strategy?

The objectives of the data strategy are clearly present in the Big Five, and they all support the data strategy with different measures to encourage data access and trust. The success of the proposals will depend on achieving a legislative environment that works together harmoniously.

3.4.2 Synopsis

The underlying goals of the European Data Strategy should be seen in the broader context

of Europe’s geopolitical ambitions to assert the EU’s “digital sovereignty” and “technological leadership”. The EU appears to have been emboldened by the perceived success of the GDPR in setting a high global standard for data protection and has the ambition to set similar benchmarks for digital and AI regulation.

New compliance obligations for companies. The sheer complexity of the regulatory landscape that will result from these five new proposals, in addition to the data-related legislation already in place at EU level, will require enormous compliance efforts on the part of European businesses. Enterprises

that can adapt quickly to the new regulatory reality stand to reap the greatest rewards in terms of increased consumer trust and market confidence. Others may struggle to adapt in sufficient time and will need to rely on support and guidance from public authorities.

Overlapping responsibilities in the public sector. Legal departments of corporations and public administrations may struggle to navigate through the overlapping responsibilities and obligations arising from the Big Five. Proposals such as the DA cannot be understood from the perspective of one legal discipline (data protection, intellectual property or competition law, for instance) alone; a holistic approach is required. Few enterprises will have a complete picture of regulation across all parts of the data value chain, and for the public sector it is even more difficult to understand a great variety of business models paired with new and overlapping legislation.

Fairer B2B relationships. While several of the proposals, like the DA and the DGA, have specific provisions concerning public administrations, B2B relationships remain at

the core of most of the initiatives. It is consistent with other areas of regulation to apply the FRAND concept to such relationships.

Dilemma. Many business practitioners would be likely to argue that the best way to support innovation is to avoid burdensome legislation that could stifle risk-taking and experimentation in the marketplace. However, the EU has taken a very different approach. It is betting on the idea that introducing a wave of new legislation to create a more level online playing field between the largest global tech companies and SMEs will eventually lead to growth in a thriving market that offers greater choice to consumers. The eventual success of the EU's strategy to legislate its way to creating new data-driven markets is still unknown. Rules do not create new business, but at the very least they may inspire trust. It is also possible that the rules will lead to what is known as the Brussels effect, whereby the Big Five legislative package will inspire other countries to proceed with similar legislative projects, thereby giving early adopters an advantage.

4 Recommendations and next steps

There is a general need to understand thoroughly and holistically the new legislation and the obligations it imposes. The general public need to know their rights and the rights need to be easily exercisable. Suitably skilled persons and data experts need to be trained, and this is a task of national importance if Finland wants to profit from the European Data Strategy. A skill shortage could not only endanger the overall target of the European Data Strategy, but also worsen Finland's position in the digital economy. Finally, a national co-ordination group between all the relevant authorities is essential and urgently needed.

4.1 General recommendations

Based on the workshops and the many interviews with stakeholders, several red threads emerge. First, there is an enormous need among all stakeholders to understand what the Big Five mean for them. In the workshops, it was apparent that the stakeholders had particular areas of expertise, but very seldom did they possess the holistic picture. Once the legislation is applicable, all stakeholders need to understand what the obligations for them are, irrespective of which legal act they are coming from. And the general public need to know their rights and the rights need to be easily exercisable.

Connected to this point, it became clear that the amount of new legislation will lead to a search for suitably skilled persons – data experts. As such positions do not currently exist and the legislation is so new that it is only sparsely taught at universities, those data experts need to be trained on the job. This will be a task of national importance if Finland wants to profit from the European Data Strategy. A skill shortage could not only endanger the overall target of the European Data Strategy, but also worsen Finland's position in the digital economy. We therefore highly recommend taking steps to increase

professional training based on case studies, workshops, classes or e-learning study.

Third, details can still be influenced both in terms of how some of the acts will be passed (the AIA, the DA) and in terms of what types of implementing measures and codes of conducts will be developed. Therefore, it is important to co-ordinate efforts between all the various interested parties in Finland. This concerns the actual set-up of the public sector, but even more the participation standardisation efforts in the private sector. The public sector will have a very important role in guiding the development here.

4.2 Recommendations per stakeholder group

4.2.1 Recommendations for the public sector

For Finnish authorities, recommendations on how to react to the change the Big Five bring fall into two categories: recommendations on how best to implement the new legislation and how to supervise it; and recommendations on what other measures authorities could take to support individuals and the private sector.

We recommend a national co-ordination group on specific initiatives, consisting of all relevant authorities, such as the DPA, Traficom, the FCCA and the DVV, among others. While the setting up of authorities, the assignment of competences or even the funding of new authorities and organisations like a Finnish (Data Innovation) Board are political questions and many factors need to be considered, the co-operation between the authorities concerned is essential irrespective of the final institutional set-up. We recommend starting with this co-operation as soon as possible. Starting now will help train the first generation of data civil servants under the new legislation, which will be very much needed in two years.

To fulfil the additional duties under one of the acts of the Big Five, more budget will be needed, which is something that needs planning.

Another set of recommendations concerns the support of SMEs and individuals. Here one big problem is the lack of co-ordination of guidance. Neither citizens nor SMEs will be particularly knowledgeable about individual legal acts but will instead look at the bigger picture. To address this issue, we recommend a mandatory co-operation procedure between national authorities, stipulated in national law, to avoid diverging guidance.

Other public authorities should see the changes that the European Data Strategy brings as an opportunity to actively shape the data economy through guidance, instructions and co-ordination, rather than being just reactive. This leadership role will require training and also the political will to be an active participant in the data economy.

4.2.2 Recommendations for the private sector, in particular SMEs

We recommend working on codes of conduct and standard contractual clauses, which are foreseen in the AIA and the DA, for example. Such work is also relevant to connect to the existing legislative acts, like the Free Flow Regulation, which also use these types of

governance instruments. These instruments should be worked out with interest groups and industry associations to ensure they are focused on existing issues and will be taken up widely. While some work can be done in Finland, more often it might be more effective to work at the European level on standards and codes of conduct. Here, the co-ordination of efforts within Finland (involving universities, companies and the public sector, for instance) might help to gain influence at the European level.

Further, we recommend creating legal support for start-ups and SMEs by providing hands-on guidance, free training and templates for transparency and accountability obligations to meet the compliance requirements. The role of the authorities tasked with implementing and overseeing all or parts of the legislation is very critical here.

4.2.3 Recommendations for individuals

We recommend taking measures to increase the understanding of this legislative project by creating awareness about citizen's rights and opportunities.

Many of the Big Five create new rights for individuals – for example, the DA creates data portability rights. Without knowledge about those rights, these remain largely meaningless. Often citizens do not know who is responsible for these rights and requests might be directed to various Ombudsmen's offices. Therefore, we believe that a mixture of communication and co-ordination measures between the authorities might help to increase general public awareness. This could be paired with measures from authorities, like guidelines for clear terms of service in line with the DSA.

The data economy as shaped by the Big Five could bring opportunities for citizens by using data altruism to promote causes people care about. This could include more general causes, like energy consumption to help gain an insight into protecting the environment, or specific data altruism projects, such as rare disease data pooling. It should be made as easy

as possible, and we recommend increasing public awareness. One possible idea for implementing this could be through “Elements of Data”, an e-learning course similar to the very popular “Elements of AI” online course.

4.3 Further studies and research on the topic

Given that the acts proposed in the European Data Strategy are partly still in the legislative process and that other factors (political, economic, security) are currently changing fast, it is fairly easy to find areas that need to be examined more.

4.3.1 Monitoring the implementation process across the EU

There is a profound difference between the way that various concepts work on paper and the way in which they are integrated into the marketplace. While the Big Five take the form of regulations – legal acts that are directly applicable in all member states – the experience of the GDPR implementation has demonstrated that the common rules can still be subject to specificities across the 27 member states. Any differences or anomalies would be very interesting to map and analyse. In this case, we recommend not only looking at differences, but rather looking at the different legislation for inspiration for Finland.

4.3.2 Assessment of impact and the interplay between the various instruments

Once the Big Five regulations are finalised and implemented, additional studies will be required to assess whether they have achieved their stated aims and have influenced the data economy in the positive ways foreseen in the European Data Strategy. In particular, it will be worth examining how these legislative instruments work together in real life, how they

inter-relate, and if any issues arise regarding overlaps or lack of alignment between the various regulations. In this context, looking at other communications of the European Commission might be helpful, like the Europe’s Digital Decade communication of 9 March 2021, which presented a vision of and targets for Europe’s digital transformation. These types of studies could look also at the European Digital Decade policy programmes and their implementation via the Digital Compass.

4.3.3 Focus on specific use cases

While this study looked at the whole strategy holistically, we believe that future studies and research are needed on specific use cases. These types of studies would fall into two groups: business development based on user journeys and sector-specific studies.

The need for case studies on user journeys arises when one questions what the Big Five proposals mean for a specific business case; for example, research on rare diseases or the development of AI technologies for a specific purpose, which would require enormous amount of data in the energy sector. As these examples illustrate, not all the Big Five proposals are relevant in specific cases; typically, it is one of the proposed acts, supplemented by either existing or proposed legislation. Given that there could theoretically be endless use case-based scenarios – every public or private organisation could submit their own – the key question is how to find the relevant cases that should be developed through further study.

In our view, two measures might help in this area. First, international co-operation. While there are always local variants – in Finland the Act on Secondary Use of Health and Social Data, for example – there is also a lot of common ground. Through co-operation with other think tanks and interested organisations, a lot of value can be shared. Second, we suggest that Sitra conducts analyses of important use cases in close stakeholder co-operation.

The sector-specific case study would analyse particular sectors, such as energy, health or manufacturing, assessing what type of data is typically processed in each sector and where opportunities are for data spaces. This would include looking at the required standards and interoperability. One possible outcome of

the study could be a code of conduct for the sector or at least a part of the sector.

For this type of study, we recommend assembling specific panels made up of a mix of relevant stakeholders and enterprises that could assess the influence of the Big Five proposals on any given sector in Finland.

5 Sitra's conclusions: Seizing the future opportunities today

To seize the opportunities of the EU data regulation in society and in business, a variety of actions are needed. The regulatory environment must be clear and business-friendly and data regulation should be proactively influenced as early as possible. Public and private-sector participants need to share a vision of a fair data economy. Finland must develop diverse measures that allow it to be recognised as an attractive model country in the data economy. Understanding the basics of the data economy needs to become a new civic skill, and skills need to be developed on a broad front.

According to Sitra's interpretation, the fair data economy is one of the three themes that will change society the most in the future. The existing data economy is not yet fair, which is why there is a need for value-based actions to balance the situation from the perspectives of individuals, companies and society. This view is also emphasised in the European Commission's data strategy and the five key legislative proposals discussed in this report.

The data strategy and the five significant legislative proposals represent change and a new era in EU policy. The European Commission promotes Europe's competitiveness, and an internal market for data that is built on European values, by harmonising legislation between the member states and requiring that all companies, regardless of their size and home country, are subject to the same rules.

According to Sitra, current data economy is unfair due to the fact that the interests of digital giants are overemphasized over individuals, SMEs and society. A clear conclusion from, for example, Sitra's Digipower investigation is that individuals have far too little control or visibility over the use of their own data (Sitra 2022c). New legislation, such as the Big Five, are needed to make the market function better

and to increase competition, innovations and consumer choice.

Individuals are at the core of the human-driven data strategy, and the five key legislative proposals are largely aimed at creating benefits for individuals in the form of stronger data rights and better services. In value chains and ecosystems that are in line with the principles of a fair data economy, individuals will have the right to control and use the data they produce. Legislation is only one aspect of the realisation of rights. Individuals will also need awareness and understanding of revenue models and operating models in the data economy, and their own opportunities to exercise influence.

Companies will benefit from regulation that affects the data economy. While companies are the primary subjects of regulation, regulation will create opportunities for a significant proportion of firms. On the one hand, they will be subject to new obligations concerning the realisation of individual rights, the transparency of operations and the pressure for reform in the face of intensifying competition. On the other hand, regulation will affect the opportunities of all companies to operate on an equal footing in the data market, and regulation will also improve the availability of data (B2B).

In particular, regulation will provide SMEs with improved opportunities to participate in the market (through fairer contractual terms, for instance). Changes in the regulatory environment will provide firms with a wealth of opportunities, and they will need to be offered support and tools for identifying and seizing those opportunities.

The public sector will also benefit from the improved availability and usability of data (B2G). However, the legislative proposals also involve national monitoring obligations that will need to be reconciled with the existing areas of responsibility. The public sector will also be subject to expectations with regard to promoting the renewal of business activities through, for example, investments and the co-ordination of actions.

A GSM moment

New data legislation is the “GSM moment” for Finnish companies. New EU regulation requires that data moves without stating how. There is now demand for Finnish leadership with this regard.

A similar leap in development was taken in the tele markets when the goal was to enable a phone user to call their friend who was a user of another operator. When this interoperability was required from the teleoperators, they had no other option than to adopt the GSM standard that enabled interoperability and shared databases about subscribers and visitors. Today, we face a similar situation. The more Finnish companies are engaged in creating future rules, the bigger is the likelihood that these form the basis of EU-level rules and standards.

The identified action proposals

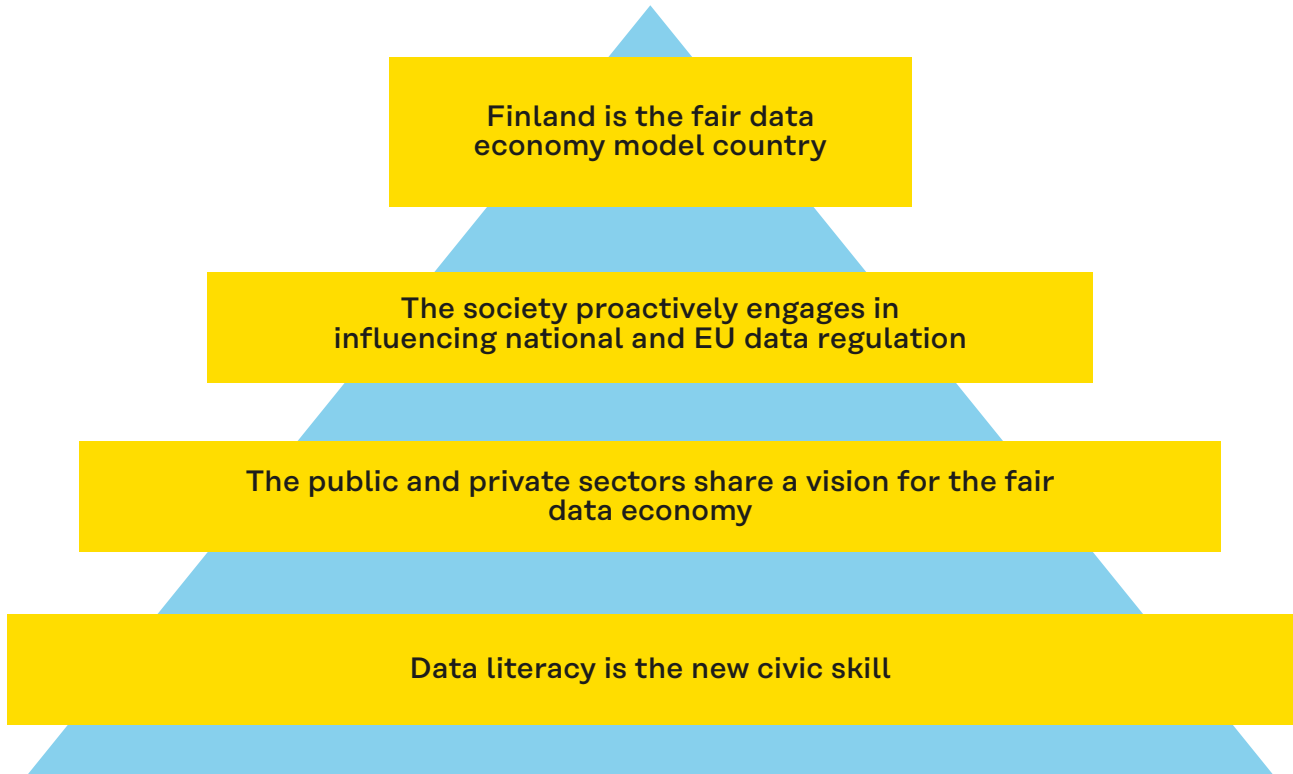
The stakeholder discussions held as part of the preparations for this report highlighted the opportunities the initiatives create for Finnish companies and their competitiveness, and the need to seize the opportunities as early as possible. This is a question of changes that challenge the parties involved to look at the existing structures and governance models in a new light.

Managing the changes created by the regulatory developments pertaining to the data economy will call for measures that can be roughly divided into two categories.

- 1.** Private and public-sector participants need to be actively involved in the planning and implementation of regulations that affect the data economy at both the EU level and nationally.
- 2.** Private and public-sector participants must recognise the opportunities presented by the regulations that affect the data economy and start preparing now to take advantage of those opportunities.

In this report, we have identified four sets of actions, which are discussed below.

Figure 5: Sets of actions to seize the opportunities of EU data regulation



1. Finland needs to develop diverse measures that allow it to be recognised as an attractive model country in the data economy. There is intense competition within the EU for value created by companies and for highly competent data economy professionals. Russia’s aggressive war in Ukraine has changed the operating environment and the European security climate, and it has stimulated discussion about Finland’s national risk. To attract business, investment and highly competent professionals, Finland needs to differentiate itself and accelerate the fair data economy in the EU by setting an example through a clear and effective regulatory environment as well as by taking measures to incentivise and promote business activity. While the Netherlands has been a leader in legislation governing

intellectual property rights and Estonia has been at the forefront of digitalisation, Finland could pursue a position as a model country for the fair data economy by acting as an arbitrator in disputes, for example. This calls for smooth and streamlined processes and the highlighting of best practices. One example of this is Finland being one of the first EU member states to prepare a national digital compass and thereby setting an example for others.

1.1 The regulatory environment must be made clear and business friendly.

Finland must not develop its own rules in addition to EU regulations. On the contrary, the public sector must help companies that operate in Finland take advantage of the legislation by making the

regulatory environment easy to understand. Navigating the world of data regulation should be as easy as possible. The existing national data regulations are fragmented, and they should be summarised in a compact form in the public sector to clarify the national regulatory environment and the related opportunities for various parties. One example of an action of this type would be to collect packages of regulations in a user-friendly service (in the Edilex digital library, for example) to promote intelligibility, comparability, link recognition and machine readability.

1.2 Investments should provide incentives for seizing the new opportunities in the data economy. Effective regulation alone does not attract highly skilled professionals and companies. RDI funding needs to be aligned with the opportunities presented by the regulatory environment and the benefits of seizing those opportunities. RDI funding should be allocated to support measures that promote goals aligned with the EU's data strategy in Finland and seize the opportunities presented by regulation. The technical aspects will require investment, co-operation and rules; the portability of data is an opportunity for companies, but different data formats may be a problem, which makes it necessary to facilitate sharing and ensure the compatibility of data.

1.3 Data economy sandboxes need to be developed. Companies need testbeds, data accelerators and other practical approaches (such as an AI sandbox) that support the growth of business. They will help understand what the changing regulatory environment means in practice.

1.4 Public services must uphold users' rights to their data. Managing one's own data is an idea that deserves to be endorsed, but it is difficult to implement at present. Public services should be developed around

the one-stop-shop principle and enable the realisation of companies' and individuals' rights concerning data. A good example of this is taxation, which has been made easy for both individuals and companies. In addition, the Act on the Openness of Government Activities will need to be amended to provide individuals with the ability to access their data in digital form and oblige other parties to take action concerning their data in the manner desired by the individual in question.

1.5 The national development of the data economy must be measured and benchmarked against other countries.

The development and choices of benchmark countries, both in the EU and elsewhere (such as the United Kingdom, China and the United States) need to be monitored, and best practices need to be implemented in Finland where applicable (the way the authorities are organised, the reform of structures, etc.). At the national level, it is necessary to establish consistent indicators for monitoring the development of the data economy (cf. the Digital Compass) and, in particular, the way the regulation is received by companies so that support and other measures can be targeted in as timely a manner as possible (cf. GDPR).

2. Public and private-sector participants need to share a vision of a fair data economy.

Identifying and promoting the appropriate measures requires a nationally shared vision and bold future-oriented thinking. Merely focusing on regulation is not enough. Instead, there is a need for political commitment that has a strong focus on the economic policy perspective to promote measures that support the realisation of the vision. One example of this is the preparation of the Digital Compass in Finland, which was carried out in co-operation between the public sector and the private sector.

2.1 Co-operation needs to promote action and experimentation. There is currently a divergence between the public and private sectors with regard to public procurement. This needs to be addressed in the development of functions that are critical to society (such as digital identity or cyber security). Co-operation could be implemented, for instance, in the form of bold testing and experimentation that takes into account the diversity of companies, ranging from small enterprises to the engines of the data economy, and the different roles that organisations have in the data economy (as producers of data, intermediaries, hardware manufacturers, refiners, etc.).

2.2 National co-ordination needs to ensure a long-term approach to co-operation: At present, the efforts to promote the development of the data economy are led by government ministries, with stakeholders being engaged through hearings and departments. National co-ordination should also be strengthened and steered at the political level to ensure the continuity of the efforts. Examples of this include the Ministerial Working Group on Developing the Digital Transformation, the Data Economy and Public Administration, and the co-ordination group for digitalisation. Taking into account the scope of the work and the limited resources, the co-ordination effort also needs to be supported in other ways that promote actions that are aligned with the shared vision between private and public-sector participants.

2.3 The rules need to be monitored and enforced to keep the data economy moving. The European Commission proposes severe sanctions that, in practice, are likely to be mainly targeted at large operators outside the EU and their harmful practices. Effective monitoring and enforcement ensure a fair and equitable market, and sanctions can be used to

protect the position of companies that operate fairly. At the same time, however, sanctions may inadvertently serve as a deterrent to other companies, which is detrimental to the thriving innovation activities envisaged in the data strategy. Besides sanctions, other means (such as suspending the operations of companies that violate the rules) should also be considered to support effective monitoring and enforcement.

3. Data regulation should not only be reacted to; it should be proactively influenced as early as possible.

A shared vision creates a foundation for the direction in which policy that influences the data economy is developed, both nationally and at the EU level. The opportunities to exercise influence are different for the five legislative initiatives. As the initiatives have different timetables, they are expected to enter into force in Finland at different times.

3.1 A big-picture view of data regulation needs to be maintained and inter-dependencies identified. The interoperability and quality of data are key ideas underpinning the data strategy. They also need to be reflected in the regulation of the data economy and the reconciliation of the regulatory initiatives. In the working groups that participated in the preparation of this report, the stakeholders highlighted the AIA and GDPR as examples of deficiencies in the reconciliation of regulatory initiatives. They both have their own monitoring mechanisms, which creates overlap in monitoring. These deficiencies and overlaps are partly the consequence of siloed preparatory processes. It is necessary to maintain and continuously sharpen a big-picture view of regulation that concerns the data economy. This needs to include the five key legislative proposals as well as other regulations related to the data economy (such as ePrivacy and eIDAS). Companies and the public sector are

subject to pressure to reform not only because of the data economy and the digital transition but also because of factors associated with security policy and the sustainability crisis, and the relationships between these pressure factors need to be identified and addressed simultaneously.

3.2 The openness of data in the public sector needs to be developed. The operating environment needs to be clarified, especially from the perspective of companies, and close co-operation between the public sector and the private sector plays a key role in this. The openness of the processing of public-sector initiatives needs to be improved so that the information supports the development of a situational picture of the national regulatory environment and impact assessment.

3.3 Efforts to exercise influence at the EU level need to start at an early stage. Because the initiatives have different timetables, the opportunities to influence them vary, and it is important to engage a broad range of stakeholders in the related negotiations. It is also necessary to actively anticipate and assess future areas of regulation in Finland (such as Web 3.0) and to influence the European Commission's agenda. Finnish public and private-sector participants also need to be actively involved in other co-operation. For example, establishing standards at the EU level should be a business-driven process, which requires the development of a new structure and system. Co-operation between public-sector participants also needs to extend to the EU level, which calls for the reform of structures and making Finnish expertise available.

4. Understanding the basics of the data economy needs to become a new civic skill, and skills need to be developed on a broad front. The basics of the data economy should become a new European civic skill. For

example, Germany published a national data strategy in 2021 with the objective of creating a national “data culture” and developing the data literacy of organisations and individuals (Sitra 2022a). For individuals to reap the full benefit of the rights and freedoms enabled by the new regulations, there is a need for interoperable services that allow users to realise their rights. There also needs to be demand for these services. The creation of data-driven business requires investments in SMEs and start-ups at the national and EU levels to ensure that they have the capability to produce services and products that take advantage of the rights of the individual. Products and services introduced to the market may help users realise the opportunities their data holds. As a whole, this requires broad awareness and understanding of the data economy, value chains and the opportunities presented by regulation.

4.1 Individuals must recognise the value of their data. Individuals need to have an understanding of their rights as data economy participants, their role as part of the value chain and the value of their data (for example, personal data is comparable to paying in money). When individuals understand the financial significance and utility of data, they may be more willing to seize their rights and to demand that companies and the public sector deliver services that respect their rights (allowing competitive bidding between different services, for instance). Awareness and trust among individuals also support the realisation of data altruism, which may promote projects that strengthen individual well-being (such as research in rare diseases). For data altruism to be realised in practice, the disclosure of information must be made as easy as possible through, for example, gamification and campaigns (“donate speech”).

4.2 Companies need practical examples and support. Companies will prioritise their obligations and the means to fulfil

them, while also ensuring that their services are as user-friendly and accessible as possible. The change presents a diverse range of companies with various opportunities, with regard to platforms and IoT devices, for example. This is why it is important to produce information for companies, such as examples of pioneers and tools for different groups of companies. Company management and governance bodies need to use future-oriented thinking and develop their competences and procurement processes.

4.3 The public sector needs to lead with its expertise. Legislative proposals

will create the need for official roles at the national level, and the planning of the related resource allocation and organisation needs to be initiated. The lack of competence is consistently listed in stakeholder discussions as a hindrance to the effective use and deployment of data among public authorities. This needs to be addressed by means of training and the allocation of human resources, for example. One potential solution would be to establish a centre of expertise to support the public authorities by helping them understand the big picture of data regulation, develop their competences and seize the opportunities involved.

References

Material that Bird & Bird used but did not quote in the report is marked with an asterisk.

EU legislation

Cybersecurity Act. [Regulation \(EU\) 2019/881](#) of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification. Last accessed on 1 March 2022.

GDPR. [Regulation \(EU\) 2016/679](#) of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC. Last accessed on 7 January 2022.

ePrivacy Directive. [Directive 2002/58/EC](#) of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. Last accessed on 30 March 2022.

Free Flow Regulation. [Regulation \(EU\) 2018/1807](#) of the European Parliament and Council on a framework for the free flow of non-personal data in the European Union. Last accessed on 1 March 2022.

NIS Directive. [Directive \(EU\) 2016/1148](#) of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Last accessed on 1 March 2022.

Open Data Directive. [Directive \(EU\) 2019/1024](#) of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information. Last accessed on 1 March 2022.

PSD2. [Directive \(EU\) 2015/2366](#) of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market. Last accessed on 1 March 2022.

EU official sources

European Commission 2022a. [Data Act – Questions and Answers](#). Last accessed on 27 March 2022.*

European Commission 2022b. [Regulatory Scrutiny Board Opinion: Data Act \(SEC\(2022\) 81\)](#). Last accessed on 21 April 2022.

European Commission 2021a. [Shaping Europe’s Digital Future](#). Last accessed on 27 March 2022.*

European Commission 2021b. [Proposal for Digital Services Act \(COM/2020/825 final\)](#). Last accessed on 27 March 2022.*

European Commission 2021c. [Proposal for Digital Markets Act \(COM/2020/842 final\)](#). Last accessed on 27 March 2022.*

European Commission 2021d. [Proposal for Artificial Intelligence Act \(COM/2021/206 final\)](#). Last accessed on 27 March 2022.*

European Commission 2021e. [Inception Impact Assessment on the Data Act](#). Last accessed on 28 March 2022.*

European Commission 2021f. [Europe's Digital Decade: digital targets for 2030](#). Last accessed on 19 May 2022.*

European Commission 2020a. [European Data Strategy \(COM/2020/66 final\)](#). Last accessed on 27 March 2022.

European Commission 2020b. [Factsheet on the European Data Strategy](#). Last accessed on 28 March 2022.*

European Commission 2020c. [Proposal for Data Governance Act \(COM/2020/767 final\)](#). Last accessed on 27 March 2022.*

European Commission 2020d. [Commission Work Programme 2020 A Union that strives for more \(COM/2020/37 final\)](#). Last accessed on 28 March 2022.*

European Commission 2020e. [Summary Report on the open public consultation on the Digital Services Act Package](#). Last accessed on 10 March 2022.

European Commission 2017. [Building a European Data Economy \(COM\(2017\) 9 final\)](#). Last accessed on 31 March 2022.

European Parliament 2021a. [ITRE report on the Proposal for Data Governance Act PE691.139v04-002](#). Last accessed on 27 March 2022.*

European Parliament 2021b. [IMCO Report on the Proposal for Data Markets Act PE692.792v02-00](#). Last accessed on 27 March 2022.*

European Parliamentary Research Service (EPRS) 2021. [NIS2 Directive: A high common level of cybersecurity in the EU](#). Last accessed on 31 March 2022.

Other sources

Act on Secondary Use of Health and Social Data. [26.4.2019/552](#), the Finnish Ministry of Social Affairs and Health. Last accessed on 14 March 2022.

Act on the Openness of Government Activities. [21.5.1999/621](#), the Finnish Ministry of Justice. Last accessed on 31 March 2022.

Act on Electronic Communications Services. [7.11.2014/917](#), the Finnish Ministry of Transport and Communications. Last accessed on 31 March 2022.

Amnesty International 2019. [Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights](#). Last accessed on 25 January 2022.

Bradford 2020. [The Brussels Effect: How the European Union Rules the World](#). Oxford University Press, New York. Last accessed on 19 May 2022.

European Data Protection Supervisor (EDPS) 2021. [European Data Protection Supervisor opinion 1/2021 on the Proposal for a Digital Services Act](#). Last accessed on 27 January 2022.

Finnish Ministry of Economic Affairs and Employment 2017. [47/2017](#), Finland's age of artificial intelligence – Turning Finland into a leading country in the application of artificial intelligence. Last accessed on 12 March 2022.*

Finnish Ministry of Finance on AuroraAI. Implementation of the national AuroraAI programme. Last accessed on 5 March 2022.

Finnish Ministry of Finance on eID. Questions and answers about digital identity. Last accessed on 9 March 2022.

Finnish Parliament 2021. U-kirjelmä 1/2021, Valtioneuvoston kirjelmä eduskunnalle komission ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi (datahallintösäädös). Last accessed on 31 March 2022.*

Internet Policy Review 2021. Regulation of news recommenders in the Digital Services Act: empowering David against the Very Large Online Goliath. Last accessed on 11 March 2022.

OECD 2019. Hello, World: Artificial Intelligence and its Use in the Public Sector. Last accessed on 19 May 2022.

Oikeuskansleri 2021. Kelan automaattinen päätöksenteko. Last accessed on 21 April 2022.

Sitra 2022a. Suomen vahvuudet, haasteet ja mahdollisuudet datatalouden rakentamisessa (only available in Finnish, “Finland’s strengths, challenges and opportunities in building the data economy”). Last accessed 19 May 2022.

Sitra 2022b. Tekoälyn käyttömahdollisuudet julkisella sektorilla. Last accessed on 25 April 2022.*

Sitra 2022c. Tracking digipower – How data can be used for influencing decision-makers and steering the world. Last accessed 31 May 2022.

Sitra 2021. The future of European companies in data economy. Last accessed 20 April 2022.

Zuboff 2018. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: Public Affairs. Last accessed 19 May 2022.

Business use cases

International Data Spaces (Deutsche Telekom). Telekom Data Intelligence Hub – Creating Value from Data. Last accessed on 31 March 2022.

European Medicines Agency. Medical devices. Last accessed on 9 May 2022.

International Data Spaces (ONCITE). ONCITE – Sharing Data in the Supply Chain. Last accessed on 9 May 2022.

International Data Spaces (Orbiter). Personal Data Banking – Reinventing the Internet With Trust and Data Sovereignty. Last accessed on 9 May 2022.

Robert Koch Institute. Corona Datenspende. Last accessed on 15 March 2022.

Saidot. Secure your AI trust and compliance with Saidot. Last accessed on 15 March 2022.

Vastuu Group. Lyhyesti MyDatasta. Last accessed on 15 March 2022.

Annex 1: Abbreviations

Abbreviation	Definition
AI	Artificial intelligence
AIA	Artificial Intelligence Act
B2B	Business-to-business
B2C	Business-to-consumer
B2G	Business-to-government
Big Five	Data Governance Act, Digital Markets Act, Digital Services Act, Artificial Intelligence Act and Data Act together
DA	Data Act
DGA	Data Governance Act
DMA	Digital Markets Act
DPA	Finnish Data Protection Ombudsman
DSA	Digital Services Act
DVV	Finnish Digital and Population Data Services Agency
GDPR	General Data Protection Regulation
ECS	Act on Electronic Communications Services
EDI	Directive on Personal Data Protection in Law Enforcement
EDPB	European Data Protection Board
EECC	European Electronic Communications Code
ENISA	European Union Agency for Cybersecurity
EU	European Union
FCCA	Finnish Competition and Consumer Agency
FRAND	Fair, reasonable and non-discriminatory
IoT	Internet of Things
NIS Directive	Network and Information Security Directive
NIS2 Directive	Network and Information Security Directive 2
OTT	Over-the-top
PSD2	Payment Services Directive 2
SME	Small and medium-sized enterprise
Traficom	Finnish Transport and Communications Agency
VLOP	Very large online platform

Annex 2: Existing data legislation

Name of the Act (short)	How does it relate to data?	Complete reference
GDPR	Regulates personal data protection.	General Data Protection Regulation: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
Open Data Directive	The Directive on open data and the reuse of public-sector information sets out minimum rules on the reuse public sector and publicly funded data.	Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information.
Regulation on data protection in EU Institutions	The GDPR does not apply to EU institutions. Thus, the aim of this regulation is to fill this gap and regulate personal data processing inside the EU.	Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.
Law Enforcement Directive	The GDPR does not apply to situations where law-enforcement authorities act as controllers. Thus, the aim of this directive is to fill this gap and regulate personal data processing in law-enforcement situations.	Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision.
Product Liability Directive	Comparable in some ways to AI Regulation; to be reviewed.	Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the member states concerning liability for defective products.
Platform to Business Regulation	Promotes the same aims as the Big Five proposal in online intermediation services.	Platform to Business Regulation, Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services.
Infosoc	Harmonising copyright law across the EU.	Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society.
Database Directive	Protection for databases.	Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases.
Copyright Directive	Reviewing copyright law in the light of the Digital Single Market project.	Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC.
Digital Content Directive	The directive gives more specific protection for consumers that enter into agreements with traders in relation to digital services or digital content.	Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services.
Electricity Directive	Aims to provide rules on data exchange for consumer energy management systems.	Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU.
PSD2	Regulates data usage and handling in payment services.	Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.
Trade Secrets Directive	Regulates the protection of trade secrets, which can include data-driven products.	Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.
Computer Program Directive	Legal protection of (possibly data-intensive) computer programs under copyright law.	Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs.
eIDAS Regulation	Harmonises the use of electronic identification (eID) and trust services.	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

Annex 3: Cornerstones of the current framework

General Data Protection Regulation

The GDPR can be described as one of the most prominent pieces of data regulation, even on a global scale. It became applicable in 2018 and regulates the processing of personal data generally. It establishes principles for processing, a legal basis for processing, the rights of data subjects, rules for the parties involved in the processing, rules for international data transfers and administrative rules on enforcement.

Many of the data-protection principles are also reflected in the Big Five legislative proposals. For example, transparency and fairness (Article 5(1) of the GDPR) are relevant in all of the Big Five. Another example is accountability (Article 5(2) of the GDPR), a key principle under the GDPR. It means that those processing personal data need to be able to demonstrate compliance with the rules. The GDPR also gives data subjects the right to data portability (Article 20 of the GDPR). This right is further enhanced in the proposed DMA (COM 2020/842/EU, Article 6(1)(h)) and in the DA (COM 2022/68/EU, Articles 3-5). Furthermore, the GDPR regulates automated decision-making (Article 22 of the GDPR), which is very relevant for the proposed AIA, which covers in its current version algorithmic decision-making.

Regulation on the Free Flow of Non-personal Data

The Free Flow Regulation was introduced in 2018 to create a legal framework for the processing of non-personal data. It aims to ensure the free flow of data within the EU by restricting data localisation and including rules on making the data available to businesses in the EU. Most importantly, the regulation includes a ban on data localisation, that is, rules that restrict data processing to a specific territory in

the EU, with the notable exception of public security. Any new localisation requirements must be notified to the European Commission (Article 4 of the Free Flow Regulation).

This regulation has many similar objectives to the DGA and DA proposals. However, both of those legislative proposals are wider and in part apply to protected data, such as personal data. They also go into more detail. Apart from the rules on data localisation, the mechanisms proposed in the legal act remain modest, for example the proposal of self-regulatory codes of conduct and the proposal to suggest points of conduct.

Directive on open data and the re-use of public sector information

The Open Data Directive sets out minimum rules on the reuse of public-sector and publicly funded data. It is an update of a directive, issued after the first Open Data Directive was published in 2003 and changed in 2013. It promotes the use of public-sector information, existing documents held by public-sector bodies of the member states. One innovation of the Open Data Directive was the introduction of the concept of high-value datasets – especially useful data sets that are made available for the public.

The Open Data Directive has much in common with the DGA, which creates a framework for sharing public-sector data (COM 2020/767/EU, p. 7). As a regulation, the DGA is generally applicable, whereas the Open Data Directive is implemented differently in the member states, resulting in different types of data being made accessible. In addition, the DGA also applies to protected public-sector data, which is a big improvement compared to the Open Data Directive, which does not cover such types of data.

Network and Information Security Directive and Cybersecurity Act

The NIS Directive was the first EU-wide legislation on cybersecurity. It aims to protect critical infrastructure and includes specific notification obligations, for certain digital services, such as cloud computing services or online search engines, among other things. Currently, the NIS Directive is being updated by the proposed NIS 2 Directive, which aims to increase the scope of the responsibilities by including telecoms providers and social media platforms (EPRS Briefing 2021, p. 7). The NIS and NIS2 Directives are essential to protect data sharing and processing envisaged by the Big Five. By increasing cybersecurity and co-ordination in this area, the NIS legal acts increase trust in the data economy.

The goal of the Cybersecurity Act of 2019 is to strengthen the EU Agency for Cybersecurity (ENISA) by giving it more resources as well as tasks. ENISA will, for example, co-ordinate and maintain the European Cybersecurity Certificate (Article 1 of the Cybersecurity Act), a certificate designed to boost trust in and the security of cybersecurity products, services and processes. This aligns well with the goals of the NIS Directive and the NIS2 Directive.

Payment Service Directive 2

The PSD2 is an example of sector-specific data regulation. It legislates payment services as well as payment service providers. The PSD2 overlaps in some areas with the GDPR, as personal data is generated and collected when using payment services. The PSD2 includes requirements for banks to allow third parties to access customer account and transaction data with the customer's consent (Article 64 of the PSD2). The overarching goal is to support financial technology providers, which refers to building

services and application around bigger financial institutions. The key common factors for the GDPR and the PSD2 are to stress the importance of individual choice for any data sharing, thereby giving consumers control over their own personal data.

The PSD2 also has similarities with the new proposed Data Act. The proposal states that when a user wishes to transfer data to other providers, the data holder should ensure that data is shared in fair, reasonable and non-discriminatory conditions. This is like the provision in the PSD2, according to which banks are obliged to transfer data to third-party service providers through an Open Application Programming Interface. Service providers should also ensure that outgoing customers maintain “functional equivalence” after switching to another provider.

Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector

The directive regulates data protection in electronic communications. Its scope includes cookies, traffic data, email marketing and confidentiality of information. The directive is outdated by technical development, in particular the development of other communication services which might not use mobile networks. There is a lot of fragmentation among EU member states as a result of the chosen legal instrument (a directive instead of a regulation). An ePrivacy regulation is supposed to replace the current directive, but the legislative process for the regulation has been slow and is still ongoing. The regulation will replace the directive in the future, but currently the directive applies simultaneously with the GDPR. A trilogue has been announced for spring 2022.

Annex 4: Summary of the Big Five

Data Governance Act (DGA)

- Promoting availability and reuse of protected public-sector data (personal data, IPRs, confidentiality)
- Aims to build an alternative to the current business model for Big Tech platforms with the help of data-sharing intermediaries
- New rules regarding voluntary sharing of data (data altruism)
- Enforcement by member states

Data Act (DA)

- Complements the DGA
- Aims to foster data sharing between businesses (B2B) and businesses and governments (B2G)
- Key obligations include fairness in B2B data-sharing contracts, data portability and new rules/ access for co-generated data
- Exemptions for SMEs
- Enforcement by member states

Artificial Intelligence Act (AIA)

- New rules for the development and use of AI-driven products and services
- AI systems are classified based on a risk-based approach from unacceptable risk to minimal risk
- Applies to providers and users of AI, irrespective of their size
- Enforcement by member states

Digital Markets Act (DMA)

- Aims to achieve fair competition
- Only applies to the largest players, called gatekeepers
- Key obligations on transparency, interoperability, data portability, prohibition of unfair practices
- Rules depend on the role of the company in the digital economy
- Enforcement by European Commission

Digital Services Act (DSA)

- Complements the DMA
- Heaviest compliance set on very large platforms (VLOPs) and some exemptions for SMEs
- Key obligations include transparency, content moderation and online advertising rules
- Enforcement mainly by member states but the European Commission can also act against VLOPs

Annex 5: Interviewees and workshop participants

Interviewees

- **Malte Bayer-Katzenberger**, Policy Officer, European Commission
- **Werner Stengg**, Cabinet expert for the Executive Vice-President Vestager, European Commission
- **Dragos Tudorache**, Member of the European Parliament, RE/RO
- **Axel Voss**, Member of the European Parliament, EPP/DE
- **Andreas Schwab**, Member of the European Parliament, EPP/DE
- **Annika Linck**, EU Policy Director, European Digital SME Alliance
- **Ida Sulin**, Senior Lawyer, Association of Finnish Municipalities
- **Eliska Pirkova**, Europe Policy Analyst and Global Freedom of Expression Lead, Access Now
- **Alberto Di Felice**, Director for Infrastructure, Privacy and Security Policy, Digital Europe
- **Svetlana Stoilova**, Advisor, Business Europe

Workshop participants

- **Minna Aalto-Setälä**, Lawyer, Finland Chamber of Commerce
- **Laura Francke**, Lawyer, Finnish National Agency for Education
- **Markus Hautala**, Chairman of the Board, Findynet Cooperative
- **Janne Järvinen**, Mission Lead (Digitalisation), Business Finland
- **Jari-Pekka Kaleva**, Chief Policy Advisor, Neogames
- **Jari Konttinen**, Senior specialist, Service Sector Employers PALTA
- **Päivi Korpisaari**, Professor, University of Helsinki
- **Riikka Korvenoja**, Lawyer, Fintraffic
- **Jukka Kyhäräinen**, Programme Manager, Finnish Ministry of Foreign Affairs
- **Susanna Lindroos-Hovinheimo**, Professor, University of Helsinki
- **Viivi Lähteenoja**, Special advisor on data policy, City of Helsinki
- **Joonas Mikkilä**, Digital and Educational Affairs Manager, Suomen Yrittäjät
- **Beata Mäihäniemi**, Postdoctoral researcher, University of Helsinki
- **Amanda Mäkelä**, Senior specialist, Finnish Ministry of Justice
- **Juho Mäki-Lohiluoma**, Advisor, Confederation of Finnish Industries
- **Jussi Mäkinen**, Director on EU regulation, Technology Industries of Finland
- **Hanna Niemi-Hugaerts**, Executive Director, TIEKE Finnish Information Society Development Centre
- **Outi Piirainen**, Head of Legal at Technology and Development, Yle
- **Olli Pitkänen**, Chief legal officer, 1001 Lakes
- **Sebastian Pohja**, Legal counsel, OP Financial Group
- **Antti Poikola**, Head of Data Economy, Teknologiateollisuus

- **Maria Rautavirta**, Director of unit, Finnish Ministry of Transport and Communications
- **Olli-Pekka Rissanen**, Senior specialist, Finnish Ministry of Finance
- **Rasmus Roiha**, Managing Director, Finnish Software and e-Business Association
- **Kreetta Simola**, Senior ministerial adviser, Finnish Ministry of Transport and Communications
- **Eva-Stina Slotte**, EU affairs adviser, Association of Finnish Municipalities
- **Ville Sointu**, Head of emerging technologies, Nordea
- **Jutta Suksi**, Senior legal counsel, VTT Technical Research Centre of Finland
- **Kirsi Suopelto**, Head of digitalisation, Finance Finland
- **Anu Talus**, Data Protection Ombudsman, Finnish Ministry of Justice
- **Hannele Timonen**, Chief specialist, Finnish Ministry of Economic Affairs and Employment
- **Satu Tuomikorpi**, Senior Policy Specialist, CSC It Center For Science
- **Mika Tuuliainen**, Chief Policy Adviser, Confederation of Finnish Industries
- **Satu Vasamo-Koskinen**, Senior specialist, Finnish Ministry of Economic Affairs and Employment

About the authors

Francine Cunningham (Regulatory & Public Affairs Director in Brussels) assists companies facing an unprecedented wave of new EU regulation that will have an impact on every business operating in the digital and data-related economy. She helps companies navigate complex EU decision-making processes and understand the practical application of the law to their sectors.

Marjolein Geus (Partner) joined Bird & Bird as one of the founding partners of the Dutch office back in 2001, and since then she has become the team leader in communications, technology and media. Today, she is Chair of the Global Tech & Comms Group and head of the international Sector Regulation and Consulting practice. She has been a member of the firm's Global Board since 2010.

Tobias Bräutigam (Partner) is the head of the Privacy and Data Protection group in Helsinki, where he advises local and international clients on complex privacy issues. As a Docent of Information Law at two universities, he also contributes to privacy publications on data-protection issues. He is accepted as a Fellow of Information Privacy (FIP) by the International Association of Privacy Professionals. He has also been appointed to the Expert Board of the Office of the Data Protection Ombudsman for this term as Deputy member of the Chair.

Maria Aholainen (Associate) is an associate in the Privacy and Data Protection and Technology & Commercial groups, based in Helsinki. She works with a broad variety of clients on privacy and data protection and telecoms regulation matters.

Floora Kukorelli (associate) works in Bird & Bird's Tech & Comms group in Helsinki, where she works with local and international clients on matters related to data protection, (tele)communications, consumer law, data regulation and commercial contracts. She has a special interest in for artificial intelligence, data protection questions in the healthcare sector and in the employment context.

Meeri Toivanen (Specialist) is an LSE Law graduate working at Sitra in the Roadmap for a Fair Data Economy team. Specialised in trade and competition policy, she works closely with stakeholders on understanding the opportunities of data regulation.


SITRA

SITRA WORKING PAPER 7.6.2022

Sitra working papers provide multidisciplinary information about developments affecting societal change. Working papers are part of Sitra's future-oriented work conducted by means of forecasting, research, projects, experiments and education.

ISBN 978-952-347-276-1 (PDF) www.sitra.fi
ISSN 2737-1042 (electronic publication)

SITRA.FI

PO Box 160
FI-00181 Helsinki,
Finland
Tel. +358 294 618 99
 @SitraFund