

Fair rules for data sharing

This training has five sections, and it takes about 90 minutes to complete them all. You can spend exactly as much time as you need. Each of us learns in our own way and at our own pace, so you can pause, go back and move freely between sections as you like.

Once you have completed all the sections, you can give feedback and apply for a certificate.

-  1. Welcome to the data economy
-  2. A peek into the world of data economy rules
-  3. Data from smart devices offers new opportunities for device users and service providers
-  4. Turning data into business through trusted data distributors and fair rules
-  5. Conclusion
-  Give feedback
-  Order certificate

1. Welcome to the data economy



The data economy is opening doors to a new era where data collection, analysis and sharing will determine a company's success. This training gives you access to the latest EU regulations that creates openings for innovation and equitable data sharing.

Come and find out about the new business opportunities these regulations create for your business!

Data – a success factor for the economy

Did you know that agriculture is already a data economy? In fact, farming has been a kind of data economy for millennia. We've always had to keep an eye on the weather – when to expect rain or the risk of frost. Or whether the soil needs more fertiliser or when to harvest. People have always needed information. Today, as in other industries, the information that agriculture needs is increasingly stored as data in information systems and can be processed automatically. This makes it easier for us to develop new solutions and make better use of our time.

Year after year, industrious farmers have kept track of their activities and harvests. Year after year, they strive to improve their crops and avoid losses. But they often only have accurate information about their own fields. The fields of their neighbours, their competitors, are all around them. If farmers could access data about these fields too, and could combine it intelligently with other available data, they could make better decisions when planning their crops. But you don't share secrets with your competitor, even if it could be mutually beneficial, do you?

This is the stumbling block that is holding back the progress of the data economy lies. Sharing data, even between competitors, would benefit everyone, but who has the courage to do it? The new EU data legislation provides solutions for overcoming the deadlock. It creates rules and mechanisms for the sharing of data and the building of trust between different actors, while respecting competition law. It also ensures an accumulation of benefits for small businesses and clarifies many grey areas.

What is the data economy? —

The data economy is a sector of the economy in which the collection, sharing and use of data is central. Data is a unique commodity in that it does not wear out as it is used. In fact, it becomes more valuable when it is shared and combined with other data. Making it easier to share data between organisations, sectors or even countries, and thereby producing better services, is one of the EU's goals. That is also the focus of this training.

A fair data economy uses data to create services and products that improve people's everyday lives ethically. Businesses of all sizes thrive through innovation. New solutions improve the well-being of society and the environment. Fairness means that the rights of individuals are protected, and the needs of all parties are taken into account. At its best, the data economy benefits everyone equally: people, companies and society.

Pioneering businesses now have the opportunity to get a head start by reaping the benefits of sharing. Changes are expected for all companies in autumn 2025 at the latest, when the new regulation will require more data sharing. Large smart device manufacturers are forced to share the data produced by the use of the devices they manufacture with customers and other companies of their choice. This is when the sharing of businesses' data will really take off. A huge market for value-added services and intermediation services will emerge around it. This means that in the future, farmers, for example, will be able to use data more extensively and efficiently when making decisions related to their crops, for example by having the right to access the data generated by their own tractors and will be able to use analytics companies specialising in agriculture to interpret this data.

Reflection task

There are many things that can be automated by using data. This can make business operations more efficient, such as invoicing, payroll, appointments, SMS and email reminders for customers, or even inventory management.

What kind of daily routine tasks in your business could be more efficient or eliminated altogether if they were automated?

Interview: What is the data economy, Kristo Lehtonen?

In the video, Kristo Lehtonen, Director of Fair Data Economy at Sitra, explains what data economy is. He also explains how data generated by something as mundane as a grocery store visit can be utilised to improve business efficiency.



Test your knowledge

According to Kristo Lehtonen, what are the consequences of sharing data?

The data becomes diluted

- The value of data increases
- Data confidentiality gets compromised

SUBMIT



Data-driven companies are more productive

The data economy is important because companies are increasingly competing on data-driven business models. Businesses that use data are estimated to be more productive than others, and the value added generated by data is as high as €6,000–€11,000 per employee. They should therefore embrace the opportunities offered by the data economy to remain competitive now and in the future.

Content of this training

The aim of this data economy training course is to help you understand what obligations, rights and opportunities the new EU rules mean for you as an entrepreneur or company representative. The new EU rules are designed to benefit European small and medium-sized enterprises in particular and to give individuals more control over their data.



Example

Jeff Citizen has a smart home with smart lighting and smart thermostats that collect data on the home's energy consumption. Before the data regulation, Jeff was unable to use data from the smart devices in the way he wanted, because the device manufacturer could restrict its use. With the new Data Act, he now has the right to his own data and can use it by combining it with other data sources, for example to optimise energy consumption.

This training focuses on the new EU Data Act and Data Governance Act. The Data Act will make different types of data more accessible and usable for different purposes. **The Data Act regulates**

who can use what data and for what purposes. This is revolutionary, because until now, for example, the manufacturer of a smart device (an IoT device that transmits measurement data to the network) has owned the data generated by the use of the device. The user of the device has been unable to use the data in the way they want. The Data Act gives users rights over their own data.

The Data Governance Act regulates ways to increase trust in data sharing between different parties. A new feature is the introduction of data intermediaries, whose operations will be supervised. Parties sharing data will then be confident that data sharing through intermediaries is safe and reliable.

The new rules for the data economy will open up significant new opportunities for people and businesses in the EU. It is worth getting to grips with them today.

The previous part of our training series, the [Basics of EU Data Economy Regulation – Fair Rules for Online Platforms](#), focused on the EU's Digital Services Act and Digital Markets Act. Both started to be used during spring 2024. You can do this training even if you are not familiar with the first part.

Points to remember

1

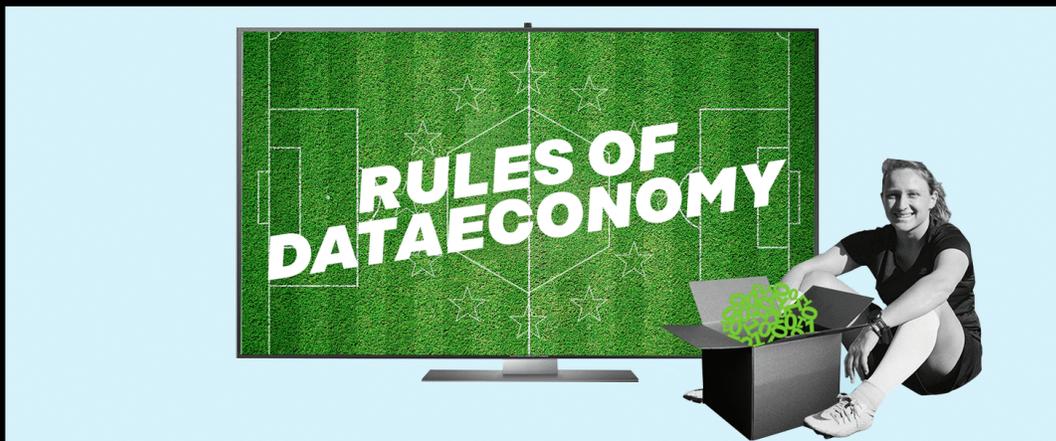
The data economy is a sector of the economy where the collection, sharing and use of data are central. A fair data economy balances the interests of individuals, businesses and society.

2

A fair data economy requires trust between individuals, businesses and public authorities. The EU aims to increase this trust by establishing common rules and standards for data sharing across the EU. New legislation, such as the Data Act and the Data Governance Act, will promote data mobility and open up new opportunities for data sharing.

Continue

2. A peek into the world of data economy rules



So, there are a lot of regulations in Europe that affect the collection and use of data. The new EU rules are designed to benefit European SMEs in particular. They also aim to give individuals more control over the data collected about them.

In this section, we go through the key concepts and explain how the regulations will affect businesses of different sizes.

The Data Act and the Data Governance Act in a nutshell

Here, we focus specifically on the Data Act and the Data Governance Act.

Data Act	Data Governance Act
Data Act, DA	Data Governance Act, DGA
Effective from: 11.1.2024	Effective date: 23.6.2022
Applicable: 11.9.2025	Became applicable: 24.9.2023
<p>Key changes:</p> <p>Users will be able to access and use the data collected by their IoT products.</p> <p>Businesses will have greater rights to change service providers and protection against unfair contract terms when sharing data.</p> <p>In exceptional circumstances, public sector actors can request access to company data.</p>	<p>Key changes:</p> <p>Clear rules for the sharing of public sector data with businesses and the transfer of business data across EU borders.</p> <p>The aim of the regulation is to increase trust in the sharing of data between organisations by data intermediaries and data-altruistic organisations.</p>

Identify your role

You can do this training as an individual, as an entrepreneur or as a representative of a business. The course uses imaginary examples and enterprises to illustrate the significance of the new rules in practice and in everyday life.

Fictional characters



Jean Manager

Jean Manager

A small business manager. The company manufactures various types of equipment for industrial use.



Mary Farmer

Mary Farmer

An agricultural entrepreneur who uses numerous smart devices in his everyday life.

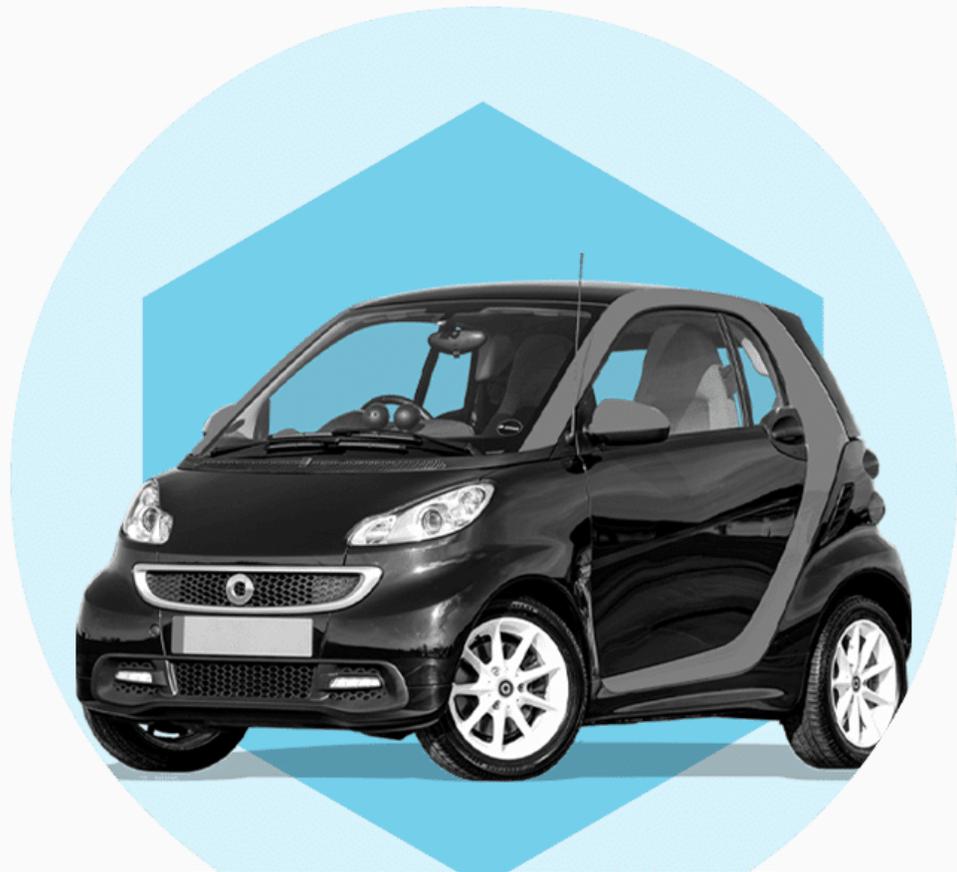


Jeff Citizen

Jeff Citizen

A service user. An ordinary person who wants to know about the impact of the data economy on everyday life.

Fictional companies and people in business stories



SmartTraffic

SmartTraffic

A medium-sized enterprise that manufactures and sells an accessory called CarSensor for monitoring the location and use of a vehicle. The business also offers sensor-related logistics optimisation services.

Customers include transport companies that operate, for example, taxis, trucks and emergency vehicles.

CEO: Sarah

Engineer: Peter

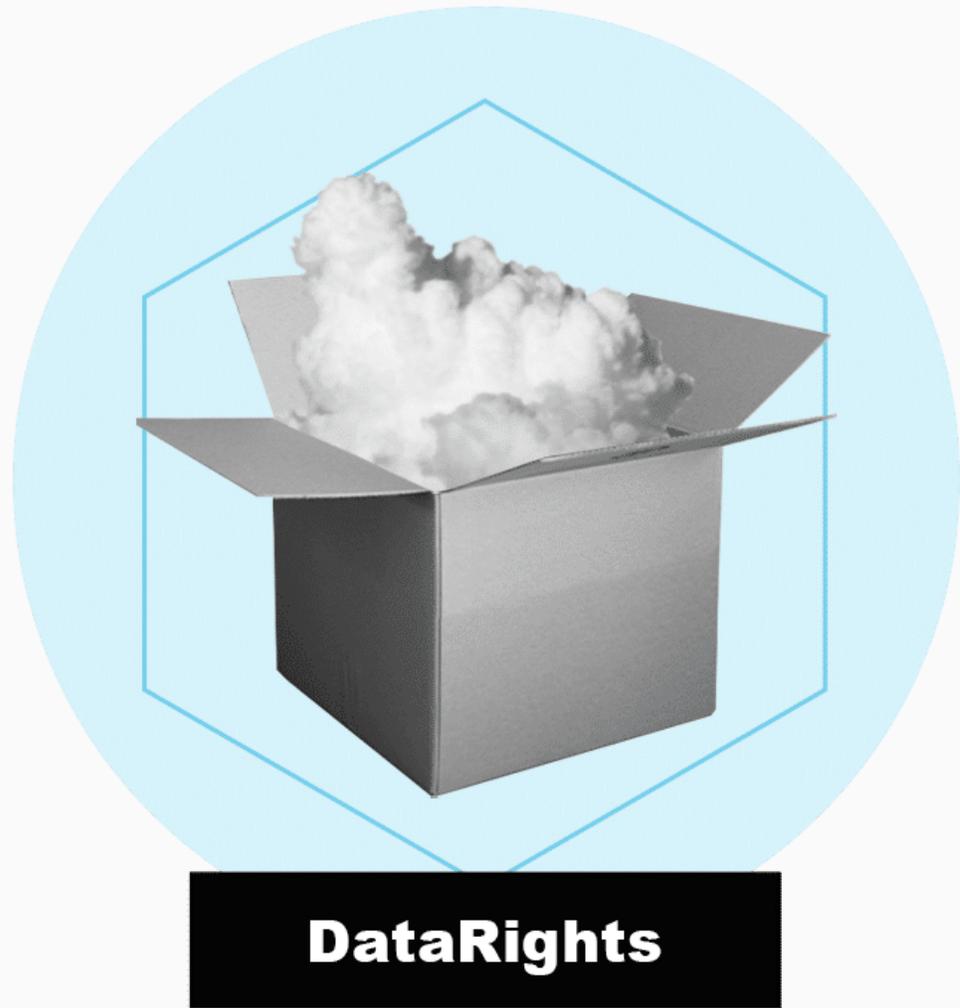


NiceClouds

A startup that provides cloud services.

CEO: Pearl

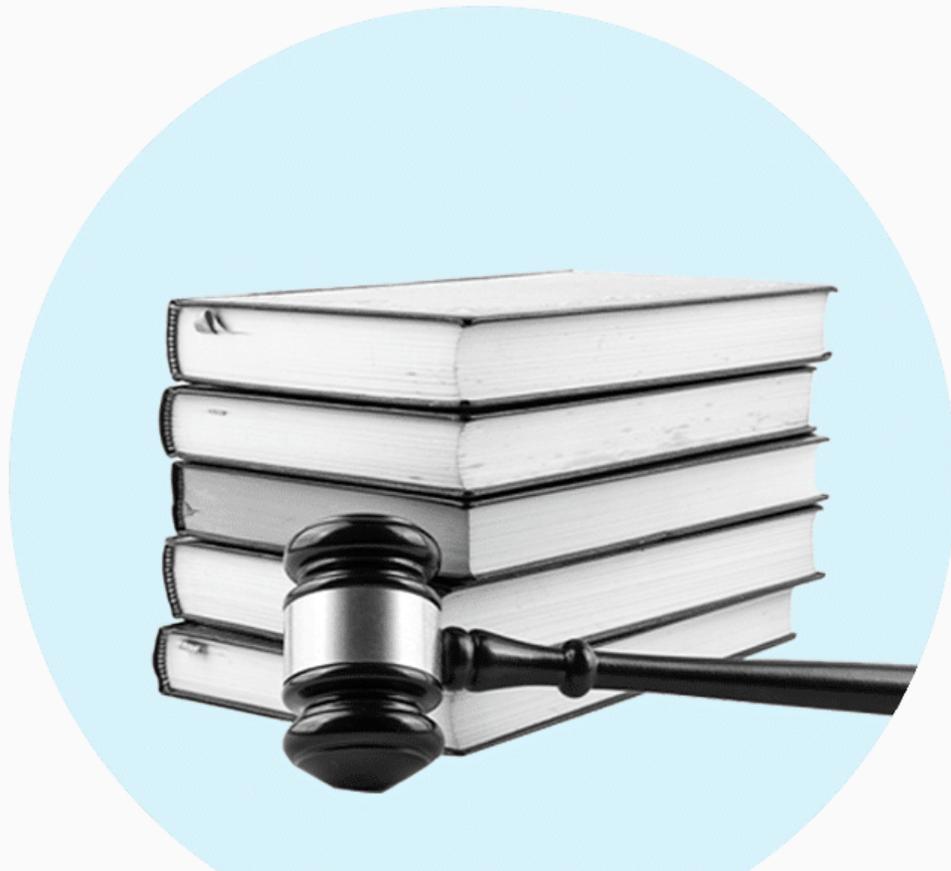
Developer: Mike



DataRights

A startup that helps individuals manage the data collected about them.

Founder: Renata



Freelance lawyer

Freelance lawyer

Freelance lawyer specializing in technology: Atte Torney

Common rules of the game will get data moving

A fair data economy requires trust between individuals, businesses and public administrations, while ensuring that all parties derive value from the use of data. Without trust and value sharing, the collection, processing and use of data will not be fair or widespread. Over the past twenty years, the role of digital services, such as search engines, social media platforms and smartphone app stores,

has grown significantly in each of our lives. Their regulation, however, has not kept pace with this rapid development.

Many of these platforms have become an integral part of the functioning of society and people's daily lives. At the same time, they are often backed by profit-making, international corporations for which the benefits or detriments to users and society are secondary to business.

Individuals are unlikely to want to share their data voluntarily unless they can trust that their data will be processed in accordance with European values and fundamental rights, such as data security and user privacy. Similarly, a company is unlikely to share its own data with other companies or operators if it suspects that its confidential information will be compromised or that the data will give others a competitive advantage at the expense of the company itself.

The EU wants to increase trust in the data economy by establishing common rules for data sharing within the EU. This is in line with the EU's long-standing efforts to strengthen the competitiveness of European businesses in the data-driven global economy. Europe has also sought to catch up with the US and China in terms of control of the digital world and to differentiate itself with its fair rules.



Objectives of the European Commission's 2020 Data Strategy

- Making Europe a global leader in a data-driven society
- Data must flow freely across the EU and between sectors
- High-quality data must be available for invention and innovation
- European rules and values must be respected

The EU has developed many new rules on communications and information technology, competition and the platform economy.

The list below does not need to be memorised, but it gives an overview of the regulation as a whole.

- **Digital Markets Act (DMA):** Ensuring fair competition between businesses in digital markets
- **Digital Services Act (DSA):** New obligations to improve transparency and security of digital services
- **Artificial Intelligence Act (AIA):** Safe and ethical use of AI
- **Data Act (DA):** More efficient use of data from smart devices and cloud services
- **Data Governance Act (DGA):** Wider use of protected public sector data and new models of collaboration
- **Directive on security of network and information systems (NIS2):** Better cybersecurity
- **Single Digital Gateway Regulation:** Improving interoperability between different public sector networks and information systems
- **Open Data Directive:** Re-use of valuable public sector data
- **Free Flow of Non-Personal Data Regulation:** Free flow and transfer of data to professional users
- **Cyber Resilience Act (CRA):** Improving cybersecurity for IoT products
- **Digital Single Market (DSM):** Harmonises copyright practices across EU countries
- **Audiovisual Media Services Directive (AVMSD):** Regulates advertising and content practices in media services

Other regulations related to the data economy.

The data economy is also governed by a wide range of well-known rules. These regulations should be taken into account when planning data-driven business.

- General Data Protection Regulation (GDPR): Protection of personal data, digital trust
- ePrivacy Directive
- Product Liability Directive

- Directive on the protection of personal data processed for law enforcement purposes (also known as the Law Enforcement Directive)
- Regulation on promoting fairness and transparency for business users of online intermediation services
- Information Society Directive: Harmonisation of copyright law
- Database Directive: Protection of databases
- Digital Content and Services Directive
- Sale of Goods Directive
- Trade Secrets Directive
- PSD2, Payment Services Directive in the Internal Market: Sector-specific rules for payment service data use and processing
- Computer Programs Directive: Legal protection of computer programs under copyright law
- eIDAS: Regulation on electronic identification: Providing digital identification to people and businesses
- Directive on the processing of personal data and the protection of privacy in electronic communications: Privacy in electronic communications (to be replaced by regulation)
- Platform-to-Business Regulation, P2B: Directive on promoting fairness and transparency for business users of online intermediation services

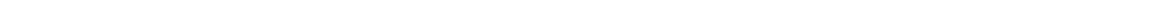
Interview: Why is API economy an opportunity for companies, Ville Peltola?

In the video, Ville Peltola, Data and Artificial Intelligence Manager at Technology Industries of Finland, talks about the importance of application programming interfaces (APIs) in data sharing. In practice, interfaces enable data sharing between organisations. The video explains why businesses should invest in good interface design.



Test your knowledge

What concrete steps does Peltola urge every business to take? (Select two answers)



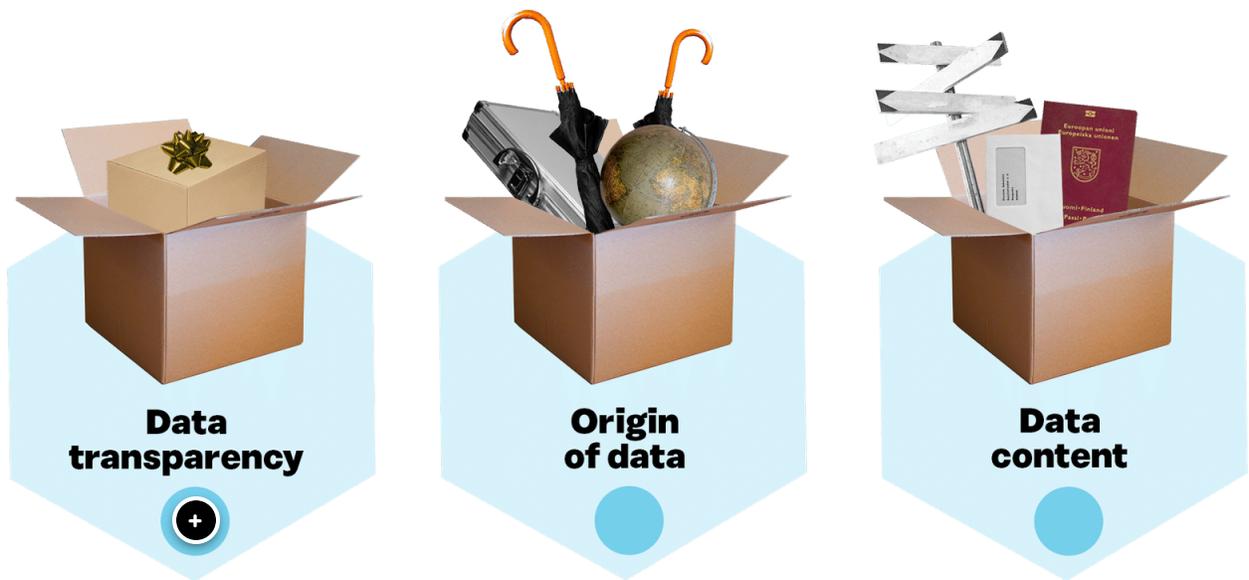
- Make a data inventory
- Start a dialogue with the developer community
- Conduct a survey of information systems

SUBMIT

Explore the concepts of different types of data

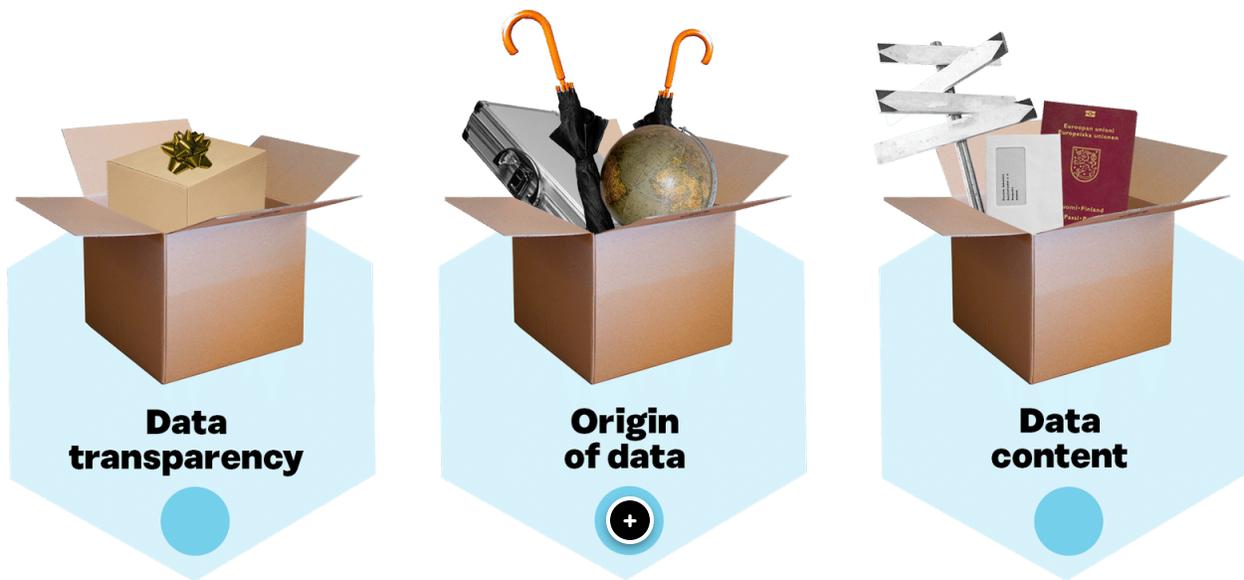
Different actors produce data. The content of the data varies from numbers to images, sound, location data and, for example, sensor data. Learn more about the terminology of data types in the image below. Click on the plus sign to bring up the concepts.





Data transparency

- **Open data:** Data that has been published openly. Openness means that others have the right to copy, modify, refine and further process it.
- **Secure data:** Data that the data controller cannot share openly because of privacy, trade secrets or other reasons.



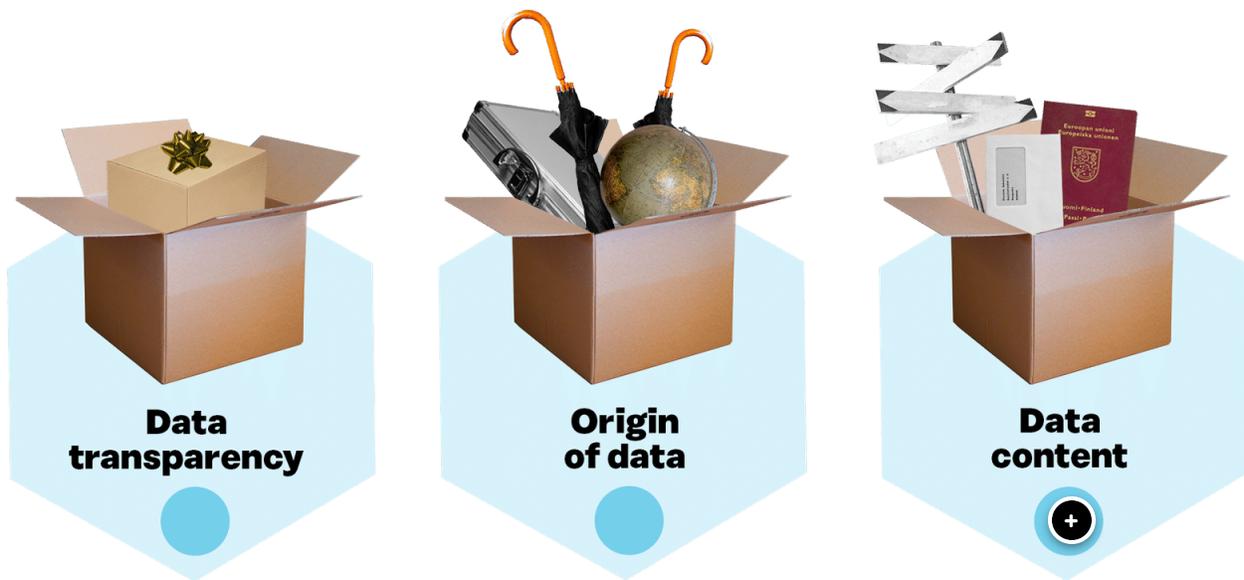
Origin of data

- **Public sector data:** Data collected by the public sector. In many countries, public sector data is also shared as open data. This data can be, for example, statistics, financial data, business data or weather data.

Public sector open data is data that has been published openly for anyone to use.

Public sector protected data, on the other hand, is data that, for one reason or another, cannot be published openly, but to which companies and other actors may be able to access under certain conditions. (We will look at this data and its use in the fourth part of the course.)

- **Business data:** Data generated, collected, or purchased and controlled by companies. The data may include trade secrets and personal data of customers, but also data that could benefit the company or its partners if shared with other actors.



Data content

- **Personal data:** Almost all data collected from society contains personal data. Personal data is any information relating to an identified or identifiable individual. The processing and sharing of such data must comply with the General European Data Protection Regulation (GDPR).
- **Data that does not contain personal data:** Some datasets do not contain personal data. For example, they may have been anonymised, in which case the data has been altered so that no individual can be identified from it. The sharing of such data is not restricted by data protection regulations, as it does not contain personal data.
- **IoT data:** (Internet of Things data) refers to data collected through IoT products such as sensors, smart devices, and other networked devices. IoT products are widely used in both industry and households. IoT products collect data as users use them. The data collected by devices may contain personal data and also confidential information. The Data Act obliges device manufacturers to grant access to IoT.
- **Product data for customers.** (We'll look at this in more detail in the third part of the course.)

Reflection task

What kind of data does your organisation hold? Do you have a data inventory that could help you understand the data you have? Who in your organisation knows the most about the subject?

What rules apply to a small business?

The Data Act and the Data Governance Act improve the rights of businesses and impose few new obligations. They provide clear rules for situations where businesses may have been uncertain in the past.

The most significant new obligation comes is for the manufacturers of IoT products to share data collected by connected IoT products. The user of the device can also choose to grant access to their data to a third party. The obligation does not apply to micro and small enterprises, but only applies to medium-sized and large IoT product manufacturers with at least 50 employees or a turnover or balance sheet of more than €10 million.

If a small business can access the data of users of devices from large IoT product manufacturers, it also opens up new markets for a small business among the customers of large manufacturers. For example, companies can create innovative analytics services or use data to service devices.

See definitions of businesses of different sizes. Click on the plus sign in the image for more information.





Microenterprise

- **Number of employees:** 9 or less
- **Annual turnover:** €2 million



Small business

- **Number of employees:** 10–49
- **Annual turnover:** €10 million



Medium-sized enterprise

- Number of employees: 50–249
- Annual turnover/balance sheet maximum: Net sales €50 million or balance sheet €43 million

Key vocabulary

There are some key concepts in data regulation that are worth knowing.

<p>Data holder</p>	<p>The organisation that manages the database. In the case of IoT products, the data holder is often the manufacturer of the product, but it can also be a retailer, after-sales service provider or similar.</p>
<p>User</p>	<p>Service subscriber or user, sometimes customer. The user, often the owner or renter of an IoT</p>

	product. Can be an individual or an organisation.
Data recipient	The data holder grants the data recipient access to specific data either by providing a copy of the data or through an interface.
Data subject	A database of personal data contains information about individuals. Data protection legislation refers to these individuals as 'data subjects' because their data is stored in a personal data register.
Supplier trap	Describes a situation where, for one reason or another, a customer cannot change their service contract with one service provider.
Trade secret holder	A business or individual who owns information deemed commercially valuable, such as product development or manufacturing process data.



Company story

New data reserves boost business services and operations

SmartTraffic is a medium-sized company that provides logistics services to professional transport operators. As part of the company's service, the customer's trucks, ambulances and taxis are fitted with SmartTraffic AutoSensors, which collect usage data from the vehicle. The data is exported to the SmartTraffic cloud, allowing the customer company to monitor and optimise the use of its equipment.

Peter, engineer at SmartTraffic, is thinking about a new feature for the cloud service. The idea was to compile an accurate database of the fuel consumption of different car models and the maintenance intervals of different parts. Such a database could be a valuable trade secret that SmartTraffic wants to protect.

They get some of the data from AutoSensors, but they also need a lot more usage data from different car models. Peter and lawyer Atte Torney meet.

SMARTTRAFFIC

"Hey Atte! You'll probably have time to read my email about planned new features. How can we secure this new database that we are going to build?" Asks Peter.

"If you have built a database, it is already protected in accordance with the EU Database Directive. This means that you have an exclusive right to the database, which means that others cannot make it publicly available without your permission. In practice, any database that is more than a simple list is protected as a database in the EU. And a database can also be protected on the basis of trade secrets."

"Good. I'm wondering, could we somehow get data from state and municipal vehicles? Doesn't the government publish open data?"

"According to the Open Data Directive, EU countries should share as much data openly as possible. This means data from ministries, agencies, municipalities and publicly funded organisations."

"So, we could get data collected from municipal vehicles on this basis?"

"Not necessarily. For example, the location history of municipal ambulances may show, for example, the addresses of individual health visits. Then we are already dealing with people's personal data, and of course it can't be shared as open data. Let's not forget the data protection regulation, the GDPR, which must always be taken into account," Atte points out.

He continues: "But this new data management act can make a difference. It sets the ground rules for allowing public sector actors to give companies access to data that cannot be openly published in a controlled way. In this case, it's important to note that personal data cannot be shared outright. In practice, such data would first be anonymised in an appropriate way."

"Aha, that sounds good!" Peter enthuses.

"The Data Governance Act also stipulates that a public sector operator cannot grant access to protected data to anyone on an exclusive basis, but that everyone must have access to data under the same conditions. In other words, your competitors would have access to the same data if they wanted."

"Hm, that doesn't sound so good now. But the data we need will still be available?"

"Not necessarily. The Data Governance Act only tells you the rules by which protected data is shared. It does not dictate the data to be shared. These matters are decided by public sector actors themselves. This is, of course, because of the Open Data Directive, and also because of the high-value datasets defined in the EU,

the opening of which will become mandatory in 2025. It is worth checking both open and protected data catalogues to see what data is available. If there is no suitable material, you can contact the appropriate agency directly. They may simply not have thought that there was a demand for certain data in companies," Atte concludes.

"Okay, thanks. This will get me further. And I have a few other ideas. I'll tell you about them later," says Peter.

Test your knowledge

True or false? Data-related regulations do not apply to SMEs.

True

False

SUBMIT

Points to remember

1

With the Data Act and the Data Governance Act, the EU aims to strengthen the position of SMEs in particular and improve the ability of individuals to control the data collected about them.

2

The Data Act's obligations on data sharing for IoT products only apply to medium-sized and large companies. Smaller ones will have the opportunity to create new services around the data from larger companies' IoT products.

3

The provisions and principles of the Data Governance Act apply to all companies. It is designed not to be burdensome for SMEs. The Data Governance Act offers SMEs new opportunities for sharing and using data. At the same time, it provides clear rules for managing and sharing data.

4

The Data Act will come into force in September 2025. The Data Governance Act took effect in September 2023.

5

The data economy is also governed by many other regulations, such as the GDPR and the Open Data Directive. These provisions aim, among other things, to protect personal data, promote data mobility and guarantee consumer rights in the digital environment.

[Continue](#)

3. Data from smart devices offers new opportunities for device users and service providers



Smart home lights, voice-controlled entertainment devices, advanced tractors and factory assembly equipment are all IoT devices. They collect and return data to the manufacturer for processing. The Data Act creates a service market around data for IoT products. The device manufacturer must guarantee the customer access to the data collected by the customer during the use of the purchased device. Customers can more easily

switch service providers and choose additional services from other companies in addition to the manufacturer's services.

In this section, we focus on the data generated by IoT products and related services. The Data Act introduces new rules for its use. We'll take a look at the other innovations introduced by the Data Act in the next section.

Under the new Data Act, data holders of IoT products (often device manufacturers) must ensure that customers have access to the data collected by the device and prepared for sending to the device manufacturer. If necessary, the device manufacturer must transfer this data to a third party selected by the customer.

However, the obligation does not apply to micro and small enterprises manufacturing IoT products, as it could be too burdensome for them. If a small company manufactures an IoT product as a subcontractor for a larger company, the large company is obliged to share the data collected by the device. In other words, even a subcontractor must manufacture its equipment in such a way that the data it collects can be accessed and shared with other parties if necessary.



IoT products include, for example:

- All advanced vehicles that collect and transmit sensor data about their environment and activities to the manufacturer.
- Sensors that measure soil properties on farms, tractors, weather radars.

- Smart thermostats used in the home, such as smart TVs, robot vacuum cleaners, and voice-controlled assistants. These devices monitor their surroundings and send metrics to the manufacturer's cloud service.
- Equipment on a production line in factories that transmits data about its operation, wear or use.
- IoT products include IoT devices and related services.



Mary Farmer

Example

Mary Farmer: "I've been able to improve the efficiency of our farming by optimising the amount of nutrients in our fields more accurately than before. Today, we regularly analyse the data collected from our soil sensors by companies specialising in agricultural data. Before, our data was only left with device manufacturers, and I couldn't use it as extensively. Now I can decide for myself who to order the analyses from and what data I share with them."

Reflection task

Will the change in IoT products affect the way your business operates? Will you have new obligations, or will you have access to IoT data yourself in the future?

Interview: How can a company use IoT data in its business, Karin Nars?

Karin Nars, CEO of Dinolift, a manufacturer of elevating work platforms, explains the added value of data for the company. She also gives her tips to other device manufacturers on how to utilise data.



Test your knowledge

The Data Act opens up the data collected by device manufacturers to competitors. How does Nars advise device manufacturers to prepare?

- Protect data with intellectual property rights.
- Pilot and develop new services together with customers.

SUBMIT

This is how the customer can access the data of their IoT product

The user receives the data collected by the device for their own use.

The user of an IoT device, whether the owner or lessee of the device, a private person or a company, is entitled to receive the data generated by the use of the device and transmitted free of charge. The manufacturer may provide access to the data directly from the device or through a separate online service. In order to gain access to the data, users must identify themselves appropriately in the online service.

The change applies only to medium-sized and large manufacturers of IoT devices and providers of services connected to them.

Where the data generated by the use of an IoT product contains personal data, the data may only be disclosed to the individual or to the holder of that personal data.

Example

Jeff Citizen: "For a long time now, car servicing has not been possible just by opening the bonnet. The service technician must connect the diagnostic device to the vehicle's data bus, because a lot of fault data is collected, and adjustments are made using software. In the past, I could only use an expensive branded service that has had access to the data bus provided by the car manufacturer. But now access to data has been opened to everyone, so I can choose the most suitable one from a wide range of garages."



Jeff Citizen



Company story

What to do when a customer requests access to data in their IoT product?

Peter, engineer at SmartTraffic, wonders what to do about a customer's request for access to all the data collected from their cars. He talks to his team and the company's CEO. They turn to Atte Torney, who knows about the new EU data rules.

SMARTTRAFFIC

"So, you've received a request from someone who wants to use the data collected by your product. Your AutoSensor is a connected product, isn't it?" Atte begins.

"Connected in what way?"

"I mean the Internet of Things – IoT. This includes smart devices that are connected to the internet in some way and can transmit data they produce when in use. The new legislation applies to such IoT products and the associated services that enable them to operate."

"Sounds like our AutoSensor."

"As you are already a medium-sized company, you are subject to these obligations under the Data Act. In practice, in certain situations, such as when requested by a customer, you must give them access to a significant amount of the data generated by your device. This applies to data and metadata generated by the device, approximately in principle. We can check the details later."

"So, the Data Act only applies to medium-sized businesses?"

"The rules on customer access to IoT product data apply to medium-sized and large businesses. Many other rules apply to all companies, regardless of size."

"Hang on, can data be requested by private customers or business customers?"

"Both. Of course, if you have personal data in your data, you keep GDPR in mind all the time, don't you?"

"Yes, let's keep it in mind. In this case, the individual has requested access to their data. But they also wanted us to share that data with a data intermediation service called NiceClouds. Can they demand that? Shouldn't the data only be given only to them, and that's it?"

"The user of your AutoSensor can both request access to the data generated by the device and share it with a third party."

"You mean with another company? Can they request something like that?"

"Yes, the user can request both access to and sharing of data. And they can also authorise the data intermediation service to make the request on their behalf."

Peter is confused. He has never heard of any data intermediation services before.

Atte continues: "A company can register as a data intermediation service provider that transmits data between different services on behalf of individuals or companies."

"And what is the benefit of such a data intermediation service?"

"The advantage is that they can provide a reliable and safe platform for sharing data," says Atte.

Peter is concerned about the new rules, because SmartTraffic does not yet have ready-made solutions that would allow the data of individual users to be neatly separated.

"There's still time. The new rules are not yet binding."

Peter breathes a sigh of relief. "Yes, we'd like to give access to the data right away, but that's just not possible when we have a stack of technical and security mechanisms still to be tested. But we still have time?"

"Yes. The legislators also understood that adapting to the Data Act would take time and effort. The new requirements will not apply until September 2025, and the obligation to provide direct access from the device to the customer will not come into force until autumn 2026."

"Great, so we have time to do this properly. Thanks, Atte!"

Test your knowledge

Which statements are true?

Small companies don't have to give their customers access to the data of the IoT product they manufacture.

Both business and individual customers can request access to data collected by an IoT product.

Data intermediation services are companies that buy data, form data packages, and sell them to the highest bidder.

SUBMIT

IoT products must be manufactured in such a way that the customer can access the data.

IoT products must be designed and manufactured so that the customer has as wide access as the manufacturer to the data they collect, produce and send. The manufacturer must provide unsolicited access to the data, simply and securely. If the customer does not receive the data directly from the device, the data holder (often the manufacturer) must provide an electronic solution. The customer must have access to the data with the same quality and scope as the manufacturer. Access must be immediate and free of charge. If the device transmits data continuously and in real time, the customer must also be given such access.

The customer must also be able to give a third party of their choice direct access to the data to.

Example

Mary Farmer: "Now that we have the data from the soil sensors in the field and our own weather station, it is easier for us to analyse the overall situation regarding the effects of weather and fertilisation on yields."



Mary Farmer

The data collection and processing of an IoT product must be clearly stated.

All companies offering the product (manufacturers, renters, dealers, installers or service providers) must provide the following information to the customer in a transparent and comprehensible manner:

- A description of the data generated by the use of the device and the amount of data generated
- Whether or not data is collected continuously and in real time
- Instructions on how the customer can access the data generated by the device
- Whether the manufacturer or service provider intends to use the data itself or through a third party of its choice, and the purposes for which the data will be used?
- Information about the data holder, company name and geographical location
- How the customer can effectively contact the data controller
- How to request data sharing with a third party of your choice
- A reminder that the customer has the right to complain to the authorities about any detected breaches of the Data Act

In certain situations, a device manufacturer may refuse to share data from IoT products

Data sharing can be restricted to prevent serious harm.

If the sharing of data compromises the legal safety of the product, which may cause serious harm to human health or safety, the sharing of data may be restricted or prevented by mutual agreement between the data holder and the users. Information about the restriction will be reported to the national authority, which is also contacted in case of disputes.

Trade secrets do not need to be disclosed, although data containing them should be shared.

Although the Data Act requires data to be shared, this does not mean that trade secrets need to be compromised. The Data Act strikes a balance between the protection of trade secrets and access to data. Data containing trade secrets is shared with the customer only after confidentiality has first been ensured. This is done through an agreement between the manufacturer and the customer. The agreement specifies data protection, data use controls, permitted data use patterns and data encryption practices.

When data is shared with a third party under the customer's authorisation, data containing trade secrets may only be shared if strictly necessary. Even then, it is agreed that confidentiality will be preserved.

In the absence of an agreement, the manufacturer is not required to grant access to the data and access already granted may be suspended. The manufacturer may also refuse to share data if access to a particular trade secret is highly likely to cause serious and irreversible economic damage.

Example

Jean Manager: "I was a little worried about how the obligation to share data might jeopardise the business. Fortunately, we have sufficient ways to ensure that trade secrets are protected even when sharing data. Contracts can be used to specify permitted uses, appropriate audits and reports to us on the use of data, and sufficient damages if the other party breaches its obligations."



Jean Manager



Company story

Are trade secrets safe?

Peter Engineer at SmartTraffic has found that the usage data collected by the company's devices and the value-added services made from them are worth keeping secret. He is concerned about the new data-sharing obligations and the protection of trade secrets. He decides to talk to Atte Torney, once again.

SMARTTRAFFIC

Atte first checks whether there are any trade secrets in the data. Peter had already clarified that the data was not protected by a patent. It was not widely known in the industry, it was a commercially valuable secret, and the company had tried to keep it secret.

"So, you have checked that data is a trade secret, in accordance with the Trade Secrets Directive?"

"The Trade Secrets Directive, right! And now we're wondering if we can refuse to share data when customers demand access to it under the Data Act."

"Let's see. The Data Act should keep trade secrets safe. But there's no general exception that allows you to refuse to share data, even if trade secrets are involved."

"Sounds crazy."

"But neither does it mean that trade secrets have to be disclosed. Trade secrets will remain secret."

Peter looked a little more relieved.

Atte continues: "Data containing trade secrets can only be shared if the holder of the data, meaning your company, and the user, meaning your customers, guarantee the confidentiality of the trade secret at an adequate level. Security measures must be in place before data is shared. They are particularly important when data is shared with third parties."

"How would this actually work?"

"As the owner of a trade secret, you first need to identify what data needs to be protected as a trade secret. Remember to consider not only the data, but also the metadata associated with it, the information describing the data. You should also agree with the customer what technical and organisational safeguards are necessary to keep the trade secret confidential, even if the data is shared."

"Okay. In other words, we need to identify what data is confidential and suggest how confidentiality should be safeguarded," Peter repeats aloud.

"Exactly. Such measures can include, for example, the use of restricted interfaces designed to allow the controlled sharing of only certain data. Access to this data can even be granted to specific users. Other measures include agreeing on rules for the use of the data. The European Commission will provide templates for confidential data sharing terms and conditions that you can use."

"What if we can't reach an agreement with the user?"

"In that case, you can refrain from sharing data containing trade secrets. Or you can block access to the data if access has already been granted. You would have to give written reasons to the user. The national authority must also be informed. The user can appeal to the authority, which takes the final decision on sharing the data," Atte explains.

"There is something to consider here. Is this the only reason to refuse to share data?"

"You can also refuse in certain exceptional circumstances. In such cases, you must be able to demonstrate that sharing the trade secret, with all safeguards in place, would very likely cause you serious economic harm."

"Meaning what?"

"That you would suffer serious and irreversible financial loss. The threshold for using this argument is quite high. The user of your device can complain to the national authority, which will then decide whether and under what conditions you should share data. Alternatively, you and the user can resolve your dispute through a national dispute resolution body, which can provide a quick, inexpensive and simple solution."

"That's quite a lot to bear in mind. Thanks for this, Atte", says Peter and returned to the trade secrets that awaited him.

Test your knowledge

Is the following statement true or false? Trade secrets will not prevent data sharing once appropriate safeguards have been agreed between the data holder and the data user.

True

False

SUBMIT

The customer has the right to share the data generated by the IoT product with other companies



As a customer, you can share the data collected by your IoT product with a third party.

As a customer, you can share the data collected by your IoT product with a third party.

The customer has the right to give access to the data collected by their IoT product to a third party. The manufacturer of the device must make the data available for such use in a form that is as precise as that which it offers to the customer.

Only medium-sized and large enterprises are obliged to do this, as is the case with the aforementioned obligation to share with customers.

According to the Data Act, data cannot be shared with gatekeepers, meaning the digital giants such as Meta, Microsoft or Alphabet. This is to ensure that gatekeeper companies do not download all the data for themselves. [The EU maintains an updated list of gatekeepers](#). For more information on gatekeepers, see the [Basics of EU data economy regulation – Fair rules for online platforms](#) in this course series. However, the customer or a third party may choose to use the services of gatekeepers to process the data.

Example

Mary Farmer: *"I finally have access to the data from smart devices from different manufacturers on my farm. I can*

buy analytics services from operators in my area who have local knowledge and an interest in serving a small farm like mine."



Mary Farmer

The third party can only use the data for the purpose agreed with the customer.

The third party to whom the customer chooses to give access to the data of their IoT product may only use the data received in accordance with their agreement with the customer. They may not redistribute the data or otherwise make use of it.

Those who have received data cannot use it to develop a competing product. Nor can a third party claim exclusive rights to the data. However, the provision of a competing ancillary service, such as after-sales service, is permitted, as is the purpose of the Data Act.

Example

Jeff Citizen: *"I shared the exercise data collected by my smartwatch with my physiotherapist so that he could use it during my treatment. It was an easy decision, because I knew that she could only use the data for the purpose we agreed and that at the end of my treatment, she would delete all the data she received as agreed."*



Jeff Citizen

Sharing customer data with a third party of the customer's choice must be agreed fairly.

If a company is required by law to share its data, the Data Act prohibits unfair contract terms. For example, in the case of IoT products, the law requires the device manufacturer to share its data with the customer or a third party of the customer's choice. The contract may specify the fees, the scope of access and the manner of use in such a way that the needs of the data holder, meaning the device manufacturer, the customer and the third party, are taken into account in a proportionate manner. The manufacturer of an IoT product cannot charge the user of its product for sharing data.

The data holder must comply with the so-called FRAND principles: Fair, Reasonable and Non-Discriminatory.

Examples of unfair terms are:

- Gross deviation from good commercial practice, such as setting an unreasonably high price for data and its sharing.
- Limitation of the responsibilities of the stronger party.
- The right of the stronger party to terminate the contract unilaterally.
- Restricting the use of data against legitimate interests, such as contractual terms prohibiting the use of data in business operations.



SmartTraffic

Company story

Unfair agreements do not have to be accepted

Peter Engineer at SmartTraffic is developing a new service idea. More data is needed for the fuel consumption and maintenance database of vehicles. The public sector did not immediately provide the necessary help, so Peter is now considering the possibility of gaining access to private individuals' vehicle usage data. Peter's idea is that individual drivers could become customers of SmartTraffic without installing

CarSensor. They could share their vehicle's IoT data for SmartTraffic's product development use through the car manufacturer's cloud service, in exchange for a small monthly fee.

This requires an agreement with each car manufacturer on the boundary conditions and pricing for data usage. SmartTraffic has started negotiations with the first major car manufacturer. Peter recalls hearing that unfair unilateral terms are banned in the EU, so he decides to talk to Atte Torney about it.

SMARTTRAFFIC

"Atte, could you take a look at this draft agreement that we have received and comment on it? Do you see any problems with it? Are there any of those unilaterally dictated terms and conditions that you once told us about over lunch?"

"It looks like a big company has dictated the contract to you. According to the Data Act, such an agreement cannot bind SmartTraffic, as it is not fair," says Atte.

He continues: "Your company was unable to change anything in the contract proposal and has to accept the terms of the contract in a take-it-or-leave-it situation. The Data Act defines this as an unfair agreement."

"So, what types of contractual terms aren't fair?" asks Peter.

"Under the Data Act, a contract term is unfair if it deviates significantly from good commercial practice. The Data Act gives several examples of unfair terms. In this contract, the car manufacturer has limited its liability for the damage it causes to almost nothing, and that in itself is an unfair term."

"The automaker has also absolved itself of its responsibility if it breaches its own obligations. Is that unfair too?" asks Peter.

"Yes. It has unilaterally dictated the terms and says that there will be few sanctions for it even if it breaches the agreement. That's not fair."

"Well, what about this clause that says they can terminate the contract after just three days without giving a reason, while SmartTraffic's ability to terminate the contract does not start until three months later?"

"That would also be an unfair condition under the Data Act. In this case, the other party can unilaterally terminate the contract with an unreasonably short notice," says Atte.

"Are there any other terms here that could be unfair?"

"There are many. According to the contract, the car manufacturer would be allowed to use SmartTraffic's data, including trade secrets, quite extensively. Under the Data Act, it is unfair for one contracting party to unilaterally dictate terms and conditions that give it excessive access to the other party's data, especially if it is sensitive material protected by intellectual property rights or trade secrets is involved."

"What about pricing? The pricing of data usage is disclosed in the contract, but they are free to change their pricing without justification," says Peter.

"That's also unfair. A clause that allows the party that dictated the terms to significantly change the price of the contract or other important matters without sufficient reason is considered unfair, and the other party cannot terminate the contract in such a situation."

"Thanks for this. Well, I wonder if we can't make our contract fairer simply due to the Data Act."

"Yes, but remember that unfair terms do not make the whole contract null and void. Other conditions would still apply. But for the sake of clarity, it might be worth trying to renegotiate the contract rather than continuing with this one, some of which applies and some of which does not. You just get into arguments about it," says Atte.

The device manufacturer can only charge reasonable fees for sharing data on the device.

The device manufacturer, who is the data holder of an IoT product, may request reasonable compensation for sharing data on the device. Compensation cannot be requested from the customer, but only from a third party with whom the customer intends to share the data. If the third party is an SME or a not-for-profit research organisation, the compensation may not exceed the actual costs of data sharing.

Example

Jeff Citizen: *"I wanted to get the data of my robot vacuum cleaner just so that I could study it out of interest. Fortunately, the data is available free of charge, so this sort of hobby is possible."*



Jeff Citizen

The device manufacturer's data is also protected by a third party.

Since sharing data with a third party under the Data Act also requires the third party to act in a mutually agreed manner, the device manufacturer, meaning the data holder, may make use of various technical protections, smart contracts and similar restrictions in addition to legal agreements, as long as they do not interfere with the proper use of the data.

If the recipient of the data has acted fraudulently or in breach of the Data Act, they must destroy the data on request and cease using any products, services or data derived from it. Under the Data Act, the following are prohibited:

- Providing incorrect information to the device manufacturer, i.e. the data holder
- Using coercive measures, such as threatening to breach an agreement
- Exploiting technical security vulnerabilities
- Using the data for purposes not agreed with the customer
- Sharing the data with others without the permission of the data holder.



Company story

What can a third party do with customer data?

NiceClouds is a cloud computing SME that offers its customers analytics and visualisation tools in addition to data storage. Many SmartTraffic customers have started transferring their data to the NiceClouds cloud. NiceClouds is thinking about what opportunities and responsibilities this brings them. Pearl CEO has sought advice from lawyers and talks with her developer.

NICECLOUDS

Mike, developer at Nice Clouds, starts: "Quite a few of our customers have recently asked if they could transfer their SmartTraffic data to us at NiceClouds. This is good for the demand for our cloud service, but there is also potential in the data itself."

"Interesting! Tell me more," says Pearl.

"Customers use our visualisation tools to look at their data. Now that we have a lot of traffic data, we could develop visualisations for exactly that kind of data and perhaps even develop new value-added services."

"Sounds good. Do you have a concrete idea?"

"We are accumulating quite a lot of data from SmartTraffic. If we know what the data is, we could even order similar devices from an equipment manufacturer that could be sold to customers at a lower price than SmartTraffic's product. This would give us a better margin on our service because we wouldn't have to pay SmartTraffic for the data."

"We really can't. We're not allowed to use the data we receive to develop such competing devices. The Data Act is very clear about that. This prohibition cannot be circumvented even by agreement."

"Right. It would have been a bit too easy if that hadn't been forbidden."

Mike thinks for a moment. "But could we, say, develop a predictive maintenance service that would work better than the SmartTraffic service? Would that be ok?"

"The Data Regulation prohibits the development of competing devices, but they specifically want competing services to emerge. So, developing the service is ok. But we must remember that we can't use the data we have to deduce the weaknesses of SmartTraffic's services and exploit them, nor can we use subcontractors to develop the service, which means that we have to develop the service ourselves."

"So, there's a restriction on the use of subcontractors?" asks Mike.

"Yes. We have this data because customers have ordered a service from us. Only IoT product customers have free access to their data. We can only use the data in accordance with the contract with the customer and have to delete the data when it is no longer needed. If we develop a new service, we can, of course, offer it to customers with new contracts and new subcontractors, but until then, the data cannot be passed on from us."

"Aha. There are all kinds of restrictions to take into account here, especially if we would like to use data to develop a new service or with other companies," Mike concludes.

Test your knowledge

Which of the following statements correctly describes NiceClouds' rights and obligations in relation to customer data?

- NiceClouds can use customer data to develop competing devices, as long as it does not share the data with third parties.
- NiceClouds can develop a predictive maintenance service that competes with SmartTraffic, but it may not use the data directly to develop competing devices, in this case sensors.
- NiceClouds can use customer data for any purpose as the data is stored in their cloud service.

SUBMIT

Points to remember

1

The data sharing obligation of the Data Act applies to IoT products (IoT devices and related services) that collect and transmit data to the device

manufacturer.

2

Customers have the right to access and use the data collected by the IoT product they have purchased. They may also grant third parties the right to exploit the data on behalf of the customer.

3

Medium-sized and large enterprises are obliged to share data on their IoT products. Micro and small enterprises are not required to do so.

4

If a customer has given a third party the right to use the data from their IoT product, the third party may only use the data for the purpose agreed with the customer. The data cannot be used to develop products that compete with the device manufacturer.

Continue

4. Turning data into business through trusted data distributors and fair rules



Even if a company wants to share its data and gain access to data from others, it can be difficult to do so in practice. It may require skills that the company does not have. And for companies to be willing to share data with each other, they need to be able to trust their partners.

In this section, we look at the aspects of the Data Act and the Data Governance Act that apply to all businesses. We explain

how companies can use public sector data in their operations, the situations where the public sector can access business data, and the new data sharing services.

Companies should share data across value networks. The more and more diverse the data in the network, the better the chances of making new types of information available. It can be used, for example, to develop existing businesses or create new ones.

Common rules for the use of data are needed to prevent misuse. Because a company's network may also include competitors, data is often not shared very enthusiastically. For this reason, the EU's Data Act and Data Governance Act introduce a number of reforms to strengthen the fair use of data by businesses and across society.

One solution to this are the new **data intermediation services**. These are registered and more closely supervised companies that can act as trusted partners to support business-to-business data sharing. In this section, we will take a closer look at them.

One of the areas that may emerge with the new regulations are the so-called **data-altruistic organisations**. Data altruism refers to the sharing of data for purposes of public interest. These may include, for example, research purposes, such as medical research. Data provided voluntarily can be of great value in advancing research or developing better health and environmental products and services.

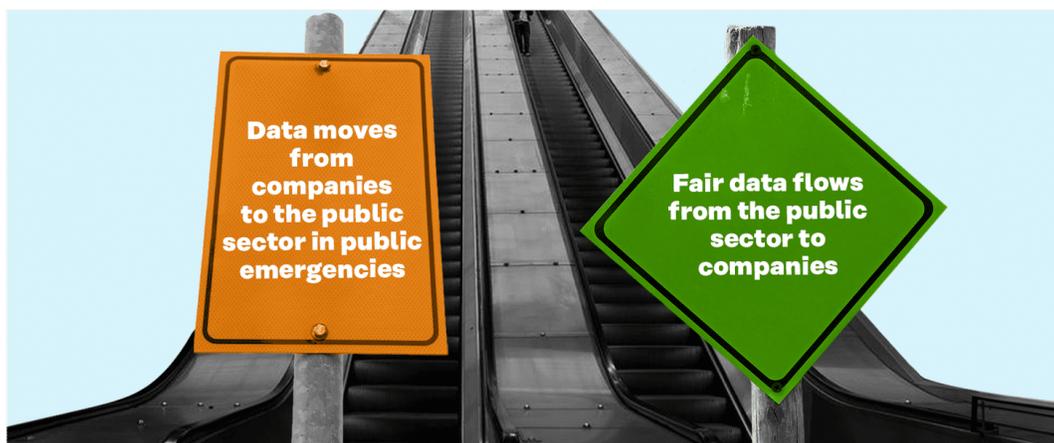
Collecting data for research purposes can be quick and easy in the digital age, but a lack of trust is often an obstacle to data sharing. You can think how willing you would be to share your genetic information with an organization called, say, Charity NGO, about which we only know its flashy website. The new regulation will allow individuals and companies to share their data in the public interest. The disclosure of data for research purposes, for example, takes place free of charge. It is up to new data-altruistic organisations to make this data available. These are not-for-profit operators

that are strictly controlled. Data altruism is expected to increase as individuals and businesses can trust an EU-registered and supervised entity.

The Data Act and the Data Governance Act create clear rules for many situations that were previously a grey area. Such as:

- Under what circumstances can public sector claim access to business data?
- When and by what principles can the public sector share or sell confidential data to businesses?
- How should companies respond to requests for legal assistance from outside the EU when someone demands the details of their European client?

Resolving all these situations is now clearer than before.



Data intermediation services are hubs for data sharing

The data intermediation service is a trusted operator.

The Data Intermediation Services Provider (DISP) acts as a neutral party between data holders and actors using shared data. They play a key role when data needs to be transferred between multiple parties. The parties may be businesses, private individuals, public authorities or other organisations. Data is transferred in accordance with the authorisations, permissions and agreements of the different parties.

Data intermediation services will be registered in a common EU register and their operations will be monitored.

Example

Jeff Citizen: *"I wouldn't share my personal data with just anyone. But if the company is a registered intermediation service, I'd be more confident that my data will not be misused or sold on."*

Mary Farmer: *"In order to optimise farming, it's important to be able to see more data than just that from your own field. This allows us to assess, for example, the need for fertiliser. In a way, I'm competing with my neighbours in optimising food production, so I don't want to share all the tricks with them, such as fertiliser timing. A reliable farmer data intermediation service ensures that no secrets are shared. At the same time, we all get information about the surrounding fields in a mutually agreed way and can make better use of our own measurement results."*



Jeff Citizen



Mary Farmer

The data intermediation service can share data between companies in the industry.

A proxy service can receive data from companies and share it with other companies. It is profitable for an intermediation service to focus its operations on a specific industry, because in order to be able to play its role, the intermediation service needs to understand industry-specific standards and practices.



What is a data intermediation service?

A data intermediation service is a commercial service provider registered in the EU that supplies a service to a wide range of data holders and data users. In order to be recognised as a 'data intermediation service provider identified in the Union', a commercial operator must fulfil all the conditions of the Data Governance Act, such as:

- The intermediation service may not use the data it transmits itself
- The intermediation service must be a separate legal entity, meaning an organisation
- The data generated by the use of the intermediation service may only be used for the development of the service
- The intermediation service shall ensure that its service, pricing and terms are fair, transparent and non-discriminatory.

The Data Governance Act describes three types of data intermediation services: business-to-business intermediation services, data intermediation services for individuals' personal data, and data cooperatives.



Company story

Data transmission can offer new business models

Pearl CEO at NiceClouds is thinking of starting a new business model. She is interested in setting up a data marketplace where companies can buy industrial data from other companies and put their own data products up for sale. She has heard that the Data Governance Act will allow organisations that transmit data, such as data marketplaces, to register as data intermediation services in the EU. She wonders what benefits this could bring to business. The CEO asks technology driver Atte Torney for advice.

NICECLOUDS

"Hi Atte, can you advise on how NiceClouds could become a data intermediation service?" Pirjo asks Atte on the phone.

"Sure! First, the company must meet the requirements defined in the Data Governance Act for the data intermediation service. It shall also register with the register of intermediation services."

"What are the requirements?"

"First of all, the entire business of the intermediation service is subject to regulation. If you have other business activities, it would be a good idea to register as a separate legal entity, such as a subsidiary, as an intermediation service. The intermediation service, pricing and terms of service shall be fair, transparent and non-discriminatory. The transmitted data must be handled with appropriate security and the record of data transmission activities must be updated in real time. Have you planned to set up a separate legal structure for data intermediation?"

"We didn't plan for it. Establishing, registering and fulfilling the requirements of a new organisation sounds like quite a lot of work. What's the use of all this?"

"With registration, companies can trust the service more. However, data sharing is voluntary for companies, and many may be concerned about the misuse of the data. So, the data is not shared. Registered intermediation services comply with the data sharing rules and are also more strictly enforced."

Pearl nods: "We have considered different options for the business model of the data marketplace. Does the regulation impose any restrictions on how data transmitted through us can be processed?"

"The Data Governance Act prohibits intermediation services from using the data they transmit for their own purposes or from reselling it. However, intermediation services can offer different services to both data holders and data users. Technically speaking, these services may include temporary storage, curation, transformation, anonymisation and pseudonymisation of data. The intermediation service may charge its customers a service fee for these services."

"Thank you, this helped us understand our options better", Pearl replies.

Test your knowledge

Which of the following statements correctly describes the requirements for data intermediation services?

- The data intermediation service must operate as a separate organisation and register in a register maintained by the EU. It can use the data it transmits for its own purposes.
- The data intermediation service may not use the data it transmits for its own purposes. It may charge its customers a service fee, for example, for storing and converting data.
- A data intermediation service may operate as part of a larger organisation. It does not need to be registered in any EU register.
- A data intermediation service does not need to be transparent about the services it provides. It can price them and set its conditions of service as it wishes.

SUBMIT

A data intermediation service can help individuals manage their own data.

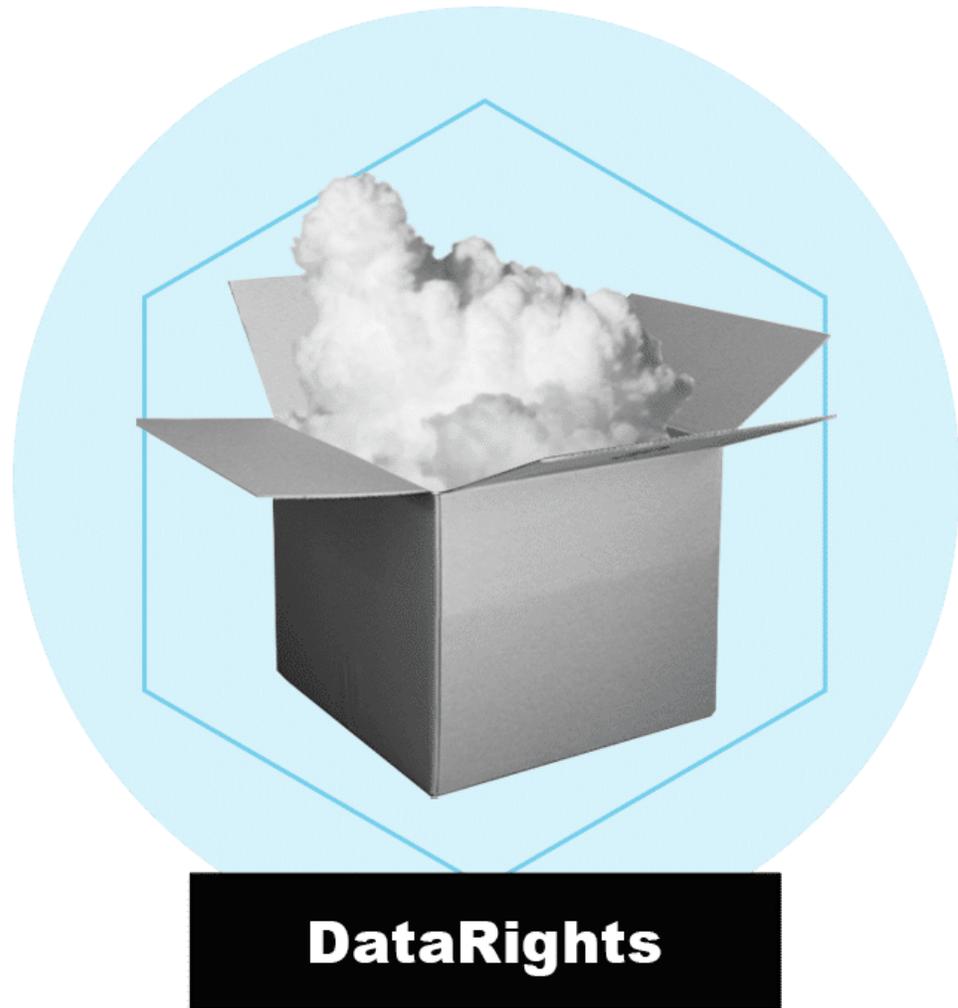
As a Personal Information Management Service (PIMS), the intermediation service may receive data on private individuals who are its customers. It transmits information to various companies in accordance with customer regulations.

Example

Jeff Citizen: *"I have collected all my health data from the public health service, my own activity trackers and other health services in one intermediation service that I trust. Now that I have a physiotherapy session, I have been able to give my physiotherapist access to this data for the duration of my treatment."*



Jeff Citizen



Company story

A data intermediation service can make it easier for individuals to manage their own data

DataRights is a new company that aims to give individuals better control over their data. Their customers can control which of their data is sent to the services they use. For example, an address change is made in one place and information is sent to where it is needed. Similarly, profiling and advertising permissions for all social media services takes place in one easy place. In other words, it helps users of digital services to

manage their own data. The company asks technology driver Atte Torney for help in registering as a data intermediation service provider recognised in the EU.

DATARIGHTS

Renata Founder at DataRights, asks: "Could Atte explain what data protection requirements we need to comply with? We help consumers manage their own data and share it with other service providers."

"Before collecting data from individuals, they must be provided with the necessary information about the purpose and conditions of collecting the personal data."

"Ok. Of course, we want to do this so that users understand what information they are sharing and that they don't share more information than necessary," says Renata.

"Have you considered that users should also be able to withdraw their consent to sharing data about them? It has to be as easy as granting it."

"Yes, we are currently planning how to make it as easy as possible. Another question: Can we also transfer data to a service outside the EU if our users request it?"

"Personal data can be transferred if the requirements of the GDPR are taken into account and users are aware of their rights."

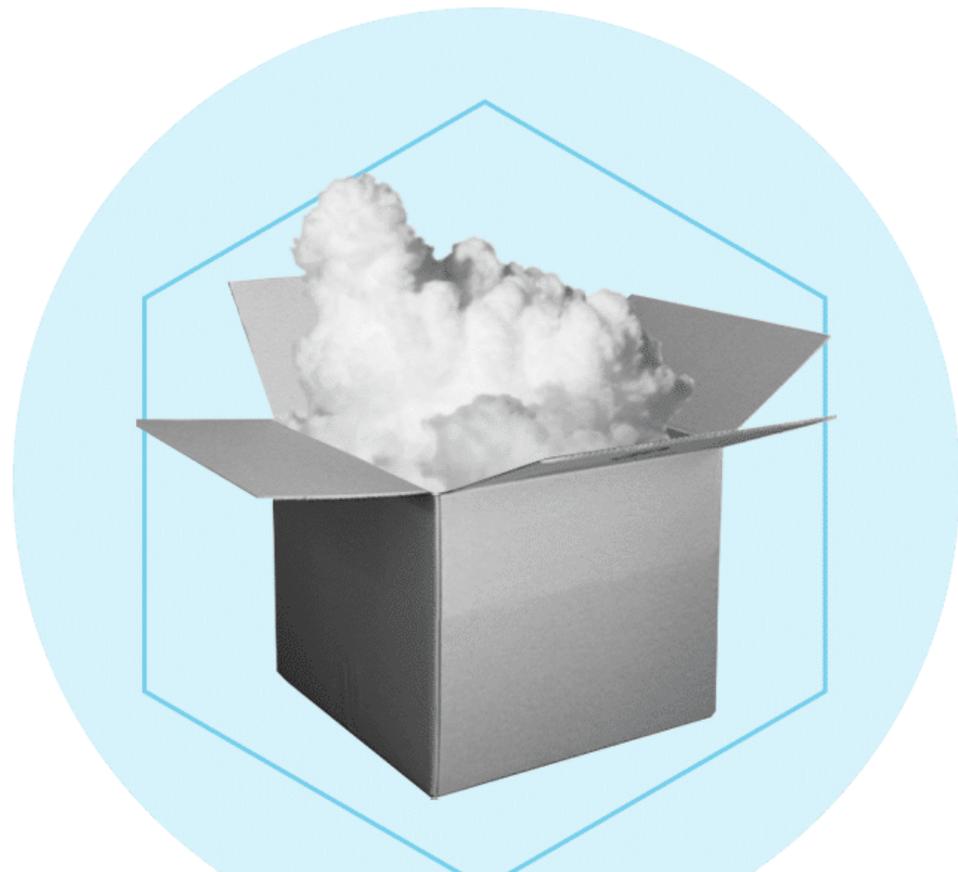
"Good to hear. If we register as an EU-identified data intermediation service, will our activities be monitored differently?"

"Yes, the authority will monitor and supervise data intermediation service providers. If necessary, the authorities may request the intermediation service to provide a report on its operations and how the service meets the requirements of the Data Governance Act. If the investigation reveals shortcomings, the intermediation service must correct them immediately. In serious cases, the authority may require the termination of the intermediation service."

A proxy service can operate as a data co-operative, representing the interests of its members in the service of the company.

Intermediation services are often for-profit enterprises, but they can also take the form of cooperatives. The aim of the cooperative is to promote and represent the interests of its members. The members of a data co-operative may be individuals or micro, small and medium-sized enterprises (MSMEs) who can benefit from having their interests represented.

The data cooperative manages its members' data according to common rules and their interests. It can act as an intermediary between its members and different undertakings.



DataRights

As a co-operative, a data intermediation service can focus on promoting the interests of its members

DataRights' CEO Renata continues her discussion with technology legal hotshot Atte Torney. Renata is registering her company as a data intermediation service identified in the EU, but she is still considering the company format.

DATARIGHTS

"It seems that our operations could be described as Personal Information Management Systems, or PIMS. What is the difference between PIMS and a data cooperative?"

"The difference is quite big: PIMS is a company, a data cooperative is a co-operative enterprise."

"Does this choice affect the requirements that will come with the Data Governance Act?"

"The same requirements apply in both cases, though the operations of the co-operative are based on the Co-operatives Act. A cooperative works to achieve the financial goals of its members. In other words, a data cooperative promotes using data rights, ensuring benefits for members and ensuring the protection of members' privacy," Atte replies.

"I guess I haven't quite figured out the difference."

"Perhaps an example will help. In many countries, there are courier services where individual workers deliver food and other things to customers according to the platform's instructions. The big controversy is whether these couriers are employees or not. A data co-operative could start representing its members with such a platform and negotiate the terms and conditions for the use of data. A data co-operative is stronger the more members it has. Similar activities in the form of a company would only be about business and providing good service to customers, but the main goal would not then be to represent the interests of users."

Data altruistic organisations advance the public interest with data

A data altruistic organisation seeks to support public interest goals.

Data altruism is the voluntary sharing of data, without compensation, for reasons of public interest. The public interest may relate to such things as medical research or environmental protection.

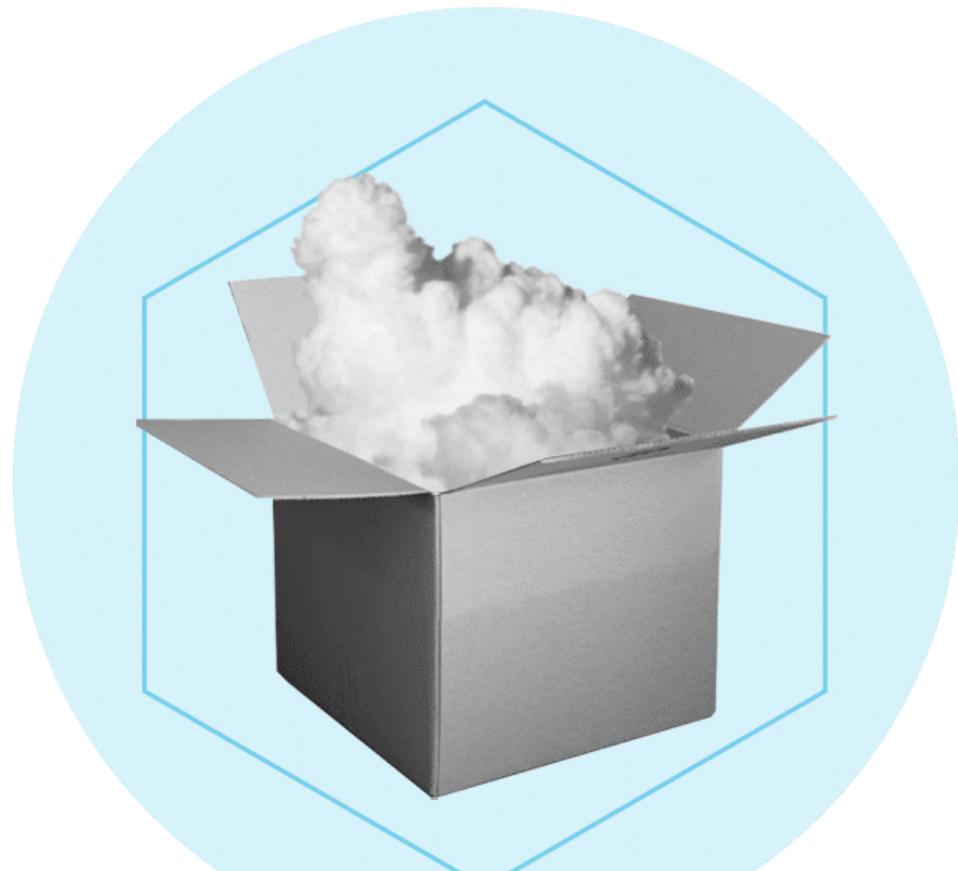
Registered Data-Altruistic Organisations (RDAOs) will be registered in a register maintained by a Member State. Data altruism may be practiced without registration, but in this case the activity is not monitored and regulated like registered data-altruistic organisations. Such a "wild" operator may not be as trustworthy as a registered and regulated operator.

For an organisation to be approved as a data-altruistic organisation, it must meet strict criteria. The main ones are:

- It must be a not-for-profit organisation and independent of commercial operators.
- It must engage in data-altruistic activities.
- It must follow the rules laid down by the European Commission, which includes the collection of consent as well as technical safety requirements.
- It shall keep particularly careful records of data processing rules, persons handling data, and the duration and purposes of the processing.
- It must inform the persons who have provided their own data particularly accurately and clearly about the use of the data.
- It shall report annually on its activities and data processing. The report shall also itemise the potential revenue from data.
- It may not use the data for purposes other than those of general interest.
- It cannot use misleading marketing practices.

Consent is obtained in a consistent way across the EU.

Consent to the collection of data by an individual or business is given using a consent form developed by the European Commission. Its different sections can be used or not used depending on the situation and sector. Consent can only be given for some purposes of use and processing operations. Withdrawing consent must be as easy as giving consent.



DataRights

Voluntary sharing of data promotes research

Renata, founder of DataRights, wonders what the best way would be to organise a service where users could manage their own personal data. He talks to technology lawyer Atte Torney.

DATARIGHTS

Renata: "Thank you for your earlier advice on data intermediation services. I am still wondering about data-altruism. Should we register as a data intermediation service or as a data-altruism-based organisation?"

"A data altruism-based organisation is always a not-for-profit organisation. Does this describe how DataRights works?" asks Atte.

"No, we are a for-profit company. So that was an easy answer. But could you explain if there are any other differences between the two?"

"The tasks of both may be superficially similar in that they strengthen the rights of individuals and the management of their own data. The main difference is that the activities of an organisation based on data altruism can be broader than that of a data intermediation service. Whereas an intermediation service can only transmit data between different actors according to contracts, a data-altruism-based organisation can process data on behalf of data holders and users when there is a public interest."

"Can a data-altruism organisation reward its users for providing data?"

"No, data altruism is voluntary. Data is shared, for example, to promote medical research," replies Atte.

Reflection task

Have you ever considered donating your data for public benefit in healthcare research, for example?

Right to change data processing service

It will be easier to transfer data from your old service to a new one.

Individuals and businesses are free to change the provider of their data processing services. Data processing services include, for example, cloud services or corporate IT maintenance.

In order to change the service, the customer must be able to transfer their data from their old service to a new one. When a customer requests a data processing service to transfer data relating to them, the data processing service provider must provide all contractual data in a transferable and suitable format for further use.

The time between the request for data transfer and the start of the transfer itself must not exceed two months. The transfer must be carried out within 30 days. Where necessary, the service provider shall assist in the process and remove the customer's data from its own systems after the transfer. The quality of service received by the customer must not be affected during the transfer process. The service provider must inform the customer of any service interruptions and maintain data security during the process.

Service providers must not create obstacles to the transfer of data. Contracts must clearly define the rights of the customer and the obligations of the service provider in the event of a transfer. All parties involved must cooperate and act in good faith in order to streamline the process.

Where it is possible to use common standards for data transmission, these should be given priority. Otherwise, common machine-readable file formats should be used.

Example

Jeff Citizen: *"In the past, I couldn't even consider changing my smartwatch, because over the years data had accumulated in a database of the one and same company. But now I get the data in a usable format, and I can get my next watch freely from whomever I want without losing my data history."*

Jean Manager: *"We put our Windows O365 platform provider out to tender. The transfer to the new provider took place quickly without any problems. All documents, user rights, everything, were transferred without a hitch."*



Jeff Citizen



Jean Manager

Continue

Clear rules for transferring data between a business and the public sector

Secure data held by the public sector will be shared fairly with businesses.

Each EU country has a single information point, which acts as its official designated body and maintains a register of available secure datasets. At EU level, lists of all EU countries are compiled in one place for easy access. If you wish to access a particular item, you make the request through the information point of the EU country concerned.

The Open Data Directive already encourages the public sector to publish as many datasets as possible as open data. Secure datasets complement open data.

A public sector operator publicly explains the terms and conditions and practices under which access to protected data can be granted. The terms and conditions shall be non-discriminatory, transparent, proportionate, objectively justified and shall not restrict competition. They may include requirements for protective measures, meaning measures taken to ensure that data is protected, for example, against unauthorised access, leakage, loss and damage.

For example, in the case of personal data, only anonymised data may be accessed. If the company has received the necessary consent from all data subjects, access to personal data is also possible. Each dataset is protected as necessary.

The transfer of data outside the EU requires approval from the supervisory authority, consent from the data subjects and possibly a separate agreement between the company and the authority.

The party receiving protected data is bound by professional secrecy and its operations must comply with intellectual property rights. It must also ensure that data cannot be used to identify individuals, for example by combining it with other data sources.

The public sector operator may verify that the use of the data is not fraudulent, and that the confidentiality of the data is not compromised. The use of results generated by the use of protected data obtained by companies may be prohibited if the results infringe the rights or interests of others.

Reflection task

What types of secure public sector data could your company use? What kind of business opportunities would this open up?



Company story

Is it possible to involve public data in innovation activities?

After hearing about the possibility of the Data Governance Act to obtain public sector data from EU countries for business development, SmartTraffic started to think about using traffic data on main public roads in product development. SmartTraffic's goal is to make their CarSensor an international export product. They would like to use public sector traffic data to develop an artificial intelligence solution that could optimise the management of customer companies' fleets, taking into account all other traffic, congestion and the like. Sarah, CEO of SmartTraffic, wants to better understand the opportunities offered by public

information resources. So, she contacts the national single information point, the body that maintains protected datasets.

SMARTTRAFFIC

"Hi, I would like to understand what public sector data we could use in our company's business. Where can I find out more?" Sarah begins.

The information officer replies, "Thank you for contacting us. We are happy to provide more information, but first we need information about what kind of data we are talking about. Is your company interested in open data – data that is publicly available to everyone?"

"Not exactly."

Sarah talks about SmartTraffic's business and adds: "I've heard that the new Data Governance Act would allow access to traffic data held by public authorities, but I'm not sure what data that is."

The official clarifies: "If data cannot be published openly, for one reason or another, but the authority still wants to make it available to businesses, secure access to it can be obtained in accordance with the principles of the Data Governance Act."

"So, does the regulation tell us what data a company can get from a public authority?"

"No. The regulation stipulates how the authority must make data available if it decides to do so. For example, an authority cannot grant exclusive rights to anyone. Conditions for re-use must be non-discriminatory. Each authority also considers what data it makes available to companies and on what terms. Lists of these datasets have been compiled at national and EU level. If some of the data you need is not on the lists, you can of course contact the authority in question and inquire about the possibility of making this data available to businesses."

In the event of a public emergency, the public sector may need access to company data that is necessary to deal with the situation.

Public authorities and certain EU institutions, such as the European Commission and the European Central Bank, may require companies to provide the necessary data in the event of a public emergency or other exceptional need. Public emergencies may include, for example, natural disasters, major accidents or serious security threats.

In a public emergency, micro or small enterprises may also be required to access data. In less severe crises, only medium-sized and larger companies may be required to provide data.

In the event of a **public emergency**, the data required must be handed over largely without compensation (although micro and small enterprises can claim compensation). In extreme situations, the data disclosed may also contain personal data, for example in the event of a natural disaster, where the authorities need quick access to data to facilitate the rescue of people.

In less **exceptional cases**, the data holder, such as a business, may be compensated for the processing and anonymisation of the required data. Furthermore, the business cannot be required to provide access to personal data. Such situations include measures of public interest defined by law, such as the mitigation or recovery from a public emergency, or the production of official statistics.

Public actors may request access to data if the necessary data is not available by any other means within the required timeframe, such as purchase from the market or amendment of legislation.

The request must be accompanied by the following information:

- Exceptional need,
- The purpose of the data request,
- Reason for the choice of data holder,
- The data required (including metadata necessary for interpreting and using the data),
- The timeframe for data disclosure,
- The legal basis of the request,
- The purposes and duration of the use of the data,
- Where possible, an indication of the date on which the data will be withdrawn from public sector systems,
- A list of other public sector bodies, EU institutions, agencies and third parties with whom it is planned to share the requested data.

In general, a public actor must assist the data holder in not inadvertently infringing the law when responding to a data request.

The public actor shall make the data request in writing in concise and clear language. It should clearly define the type of data required for access. The request must relate to data that is in the company's possession. The

request shall be proportionate to the exceptional need. In addition, the public operator shall undertake to ensure the protection of trade secrets in its request for data.

As a general rule, the required data should not contain any personal data. Where necessary, a public operator may request data relating to individuals from which no individual can be identified but must ensure that the protection of personal data is maintained.

If the trade secrets of the data holder, meaning the company, are at risk, it must identify the data containing trade secrets. In such cases, the public operator must do everything necessary to preserve the confidentiality of trade secrets.

The requesting public body may share data with another public body in order to achieve its original objective. The company must be informed of the sharing of data without delay.

A public actor may also share the data it receives for research purposes. The use of research must be consistent with the public actor's original need related to an emergency or crisis.

A public operator may require the disclosure of trade secrets only when strictly necessary in the event of an emergency or exceptional situation.



Company story

Leveraging corporate data in a public emergency

A coronavirus-like virus infection is spreading to Finland. A national epidemic has not yet been declared, but there is a risk that the disease will spread. The authorities have requested the medium-sized enterprise SmartTraffic and other companies in the sector to access traffic data that could be used to assess and anticipate the effects of different restrictions on traffic flows more accurately than basing calculations on statistics that are more than a year old. SmartTraffic's CEO Sarah contacts technology lawyer Atte Torney to say that the company has received a data request from a public institution.

SMARTTRAFFIC

"Hi Atte, can you advise us on how to respond to that data request? Do we really need to provide access to data that is under our control?" Sarah asks.

"Basically, yes. If there is a clearly justified exceptional need where the data in your possession is necessary and cannot be obtained elsewhere, you shall give the public operator access to it."

Atte continues: "First of all you have to distinguish between exceptional circumstances or an emergency. In my opinion, a situation where a public entity tries to prevent a pandemic can be classified as exceptional circumstances, meaning that it is a matter of mitigating the state of emergency."

"Yes, this criterion, or "exceptional need", is mentioned in this data request right at the beginning," says Sarah.

"Um, exactly. In this case, a public authority may only request access to data that does not contain personal data. In other words, SmartTraffic is not allowed to disclose personal data, nor can it be required to do so."

"Don't these requests usually apply to large companies? We are a medium-sized company. Does this requirement also apply to us?"

"Yes. In other exceptional situations, such as the current mitigation of the state of emergency, only micro and small enterprises are exempt from data disclosures. But in the event of an actual emergency, they could also be required to access the data."

"How do we know that the request is reasonable, or are there any criteria for the data request that we should know about?"

"The data request must meet the requirements set out in the Data Act. For example, a data request must be well-founded and contain all the information required by the Data Act," explains Atte. "In this case, I think all the formal criteria are in order," he adds.

"Okay, good to know. If the requested data contains trade secrets, are they safe?"

"The data request must respect the rights of the data holder, i.e. you, and the requestor must commit to ensuring the protection of trade secrets," explains Atte.

"I understand that we have no choice but to agree to the request," says Sarah. "There is some work to be done here. Is it possible for us to be compensated for this?"

"Yes, it is. Medium-sized and larger enterprises are only required to meet data requests related to the actual public emergency without compensation. In other situations, the work is compensated. Other exceptional

needs are always compensable work. The compensation must cover the actual cost of complying with the request."

"One more question. Can a public authority share our data with other public actors?"

"This is possible, but data may only be shared for the same purpose, which is to prevent a pandemic, and you must be informed. The data request should include information about the parties with whom your data is planned to be shared," explains Atte.

Test your knowledge

When does a company have to disclose data to the public sector without compensation?

- Whenever public sector demands it.
- Only in case of emergency. Even then, micro and small enterprises can claim compensation.
- Always, except in the case of data containing personal data.
- When data is requested to produce official statistics.

SUBMIT

Clear rules for situations where non-EU countries require company data.

Companies may also impose data access or transmission requirements from outside the EU concerning protected public sector data or customer data collected through data intermediation. This may be the case, for example, in the context of a criminal investigation in another country. In this case, the request must be based on a court decision and/or judgment of that country or a decision of the administrative authority of that country.

Before responding to a request, the company must consider whether the request is sufficiently precise, meaning justified. The company must also inform the original data holder upon request, except in the case of law enforcement.

Data transfers outside the EU must be kept to a minimum. The submission of data containing personal data is always also subject to the rules of the GDPR. The company must ensure that the confidentiality of the data is maintained, as advised by the authorities and by agreement with the relevant parties.

Data can only be submitted if the use of the data is sufficiently secure in the receiving country. There must be an agreement between the destination country and the EU or an individual EU member state that defines the acceptable use of the data. In the absence of such an agreement, data can only be submitted in certain special circumstances.

Some companies hold very critical data, the uncontrolled sharing of which could pose a threat to national security. Such data could include, for example, data related to energy infrastructure. When distributing critical data or data containing trade secrets, a company may seek advice from the authorities under the Data Act.

In general, when responding to a request, all appropriate steps must be taken to ensure that access to or transfer of data does not violate EU or member state law.

Points to remember

1

New data intermediation services are reliable and supervised actors that transfer data for use by different actors according to commonly agreed rules.

2

Individuals and companies may voluntarily make data available in the public interest without charge. New data-altruistic organisations will ensure that data is handled securely.

3

Protected public sector data can be shared with businesses under non-discriminatory and transparent rules. This complements the open data already provided by the Open Data Directive.

4

Public actors and certain EU institutions may require companies to access data in exceptional or emergency situations. The disclosure of data mainly takes place without compensation, but in certain situations companies may be compensated.

5

Businesses and individuals have the right to switch data processing services, such as cloud services. Service providers shall enable the transmission of data within a set time limit in a format that is well suited for further use.

Continue

5. Conclusion



In this section, you can review the main content of the training.

The EU aims to build a fair data economy with common rules

The EU's new data regulation aims to build a fair data economy. The aim of this training has been to clarify the impact of the new regulations, the Data Act and the Data Governance Act, on businesses, especially SMEs.

The size of an enterprise affects whether or not it is bound by regulations. The rule of thumb is: the larger the company, the more obligations it has. There are exceptions, and the GDPR, for example, imposes obligations on all types of enterprise, regardless of size.

Data Act	Data Governance Act
Data Act, DA	Data Governance Act, DGA
Effective from: 11.1.2024	Effective date: 23.6.2022
Applicable: 11.9.2025	Became applicable: 24.9.2023
<p>Key changes:</p> <p>Users will be able to access and use the data collected by their IoT products.</p> <p>Businesses will have greater rights to change service providers and protection against unfair contract terms when sharing data.</p> <p>In exceptional circumstances, public sector actors can request access to company data.</p>	<p>Key changes:</p> <p>Clear rules for the sharing of public sector data with businesses and the transfer of business data across EU borders.</p> <p>The aim of the regulation is to increase trust in the sharing of data between organisations by data intermediaries and data-altruistic organisations.</p>

As more data becomes available, companies will have the opportunity to create new

additional services around smart devices

Companies that manufacture IoT products must clearly explain the collection and processing of data on their devices.

Companies manufacturing, selling, and installing IoT products should openly and clearly inform their customers about the data collected by the product during use, the amount, how it is collected and how it can be accessed. The customer must be able to know whether the company will use the data itself or share it with third parties, and what the data is used for. In addition, customers must be given access to the data and instructions on how they can share their data with others if they wish. They should also be informed of how to complain about possible breaches of data regulations if they become aware of them.

More opportunities for customers to decide how data is used in their IoT product.

Customers are entitled to receive the data generated by the use of their IoT product free of charge. The company can grant them access to the data either directly from the device or through a separate online service. This only applies to medium-sized and larger companies selling IoT products or related services.

Customers can also give access to their data to third parties.

Customers are entitled to grant a third-party access to their data. The third party may only use the data it receives within the scope of its contract with the customer and not for other purposes. When data is shared with a third party, the Data Act defines how the parties can agree on the sharing of data. For example, the contract may cover pricing, scope of access and data usage patterns. The agreement must be fair to all parties.

In some situations, the IoT product manufacturer may opt out of data sharing.

The manufacturer may opt out of data sharing in certain exceptional circumstances. The manufacturer may restrict or prevent the sharing of data, for example to prevent serious harm, if the sharing of the data compromises product safety and may therefore cause serious harm to people's health or safety.

Data containing trade secrets will only be shared when confidentiality is assured, meaning when the data holder and user have reached an agreement on safeguarding confidentiality through various safeguards and measures.

Data sharing and access will improve with the new rules

Switching data processing services becomes easier.

The Data Act will make it easier for companies to switch data processing services, such as cloud services. This is to avoid problematic supplier traps. The data processing service must comply with the time limits for data transfer specified in the act. Where necessary, it must assist in the process of switching services and delete the customer's data from its own systems after the transfer.

Data intermediation services support reliable data sharing.

Data Intermediation Services Provider (DISP) aims to provide solutions for companies so that a lack of trust or practical challenges in data sharing are no longer an impediment.

Data intermediation is a new business model. A company wishing to become such an operator must be registered in the EU register. The authorities supervise the operation of intermediation services, and companies can trust that the intermediation service does not, for example, use the data it transmits itself.

Individuals can also use the services of an intermediation service to transfer their own data from one organisation to another.

Data altruistic organisations promote the public interest with data.

Data altruism is the voluntary sharing of data without compensation for purposes in the public interest, such as medical research or environmental protection. Organisations based on data altruism, meaning that they collect data for such purposes, must meet strict criteria. For example, the organisation must be a not-for-profit and independent actor. Data altruism can be practised even without registering an organisation, but inclusion in a register maintained by the state indicates the reliability of the organisation.

Businesses will be able to make greater use of public sector data.

Until now, the Open Data Directive has encouraged the public sector to publish as many datasets as possible as open data. The Data Governance Act sets out fair rules for businesses to gain access to **protected data made available for re-use by public authorities** that cannot be released as open data.

Public bodies will specify the terms and conditions under which protected data can be accessed. Terms and conditions must not discriminate or restrict competition and must be justified. Protected data must be protected against unauthorised access. Data containing personal information may only be used with the consent of the person to whom the data relates or if data has been anonymised.

Public entities may require access to company data in exceptional circumstances and emergencies.

Public entities and EU institutions can require companies to provide important data in exceptional circumstances or emergency situations. In an emergency, all companies, regardless of size, may have to hand over data, mainly without compensation. In exceptional circumstances, medium-sized and large companies may be required to provide data, and in these situations, they may receive compensation. Data is requested only if it is not otherwise received. It must be handed over fairly and safely.

Data can be shared with countries outside the EU, but only in secure situations.

Non-EU countries can only access data in strictly regulated circumstances, such as criminal investigations, and only on the basis of a court order. The customer must be informed before disclosing the data. The processing of data containing personal data must comply with the requirements of the GDPR. Data will only be transferred if there is an agreement in place in the destination country that guarantees the safe use of the data, and companies can turn to the authorities to ensure security. In all situations, appropriate safeguards must be in place to ensure that data sharing or transfer is not carried out in breach of EU or individual member state law.

[Give feedback](#)

Give feedback

Congratulations, you have now completed the entire training! Next, you can give us feedback on the content and implementation of the training. At the same time, you will reflect and assess your own learning experience.

Your feedback will not only help you to implement the things you learned in practice, but also us to make even more impactful trainings.

Feedback and self-assessment

Assess your own learning experience and the implementation and content of the training by responding to a short survey.

GIVE FEEDBACK

Share what you learned and keep on learning

When you soon receive a certificate, the training will be over but another kind of a learning path is just beginning! Now, you can put what you learned into action and can also motivate others to learn.

- **Inspire** others by your own example.

- **Discuss** openly what you learned.
- **Challenge** your colleagues to join the training.
- **Share on social media** your thoughts of the training or your certificate
#eoppiva #learningisforeveryone
- **Subscribe to the newsletter** to be informed of new eOppiva trainings.
- **Study more** from eOppiva's extensive range of trainings.

[Order certificate](#)

Order certificate

Congratulations!

You have now completed the training and can order a certificate of your achievement! Order the certificate right away to make sure that your achievement is saved.

Choose the right option below based on whether you are working for Finland's central government.
(If you are not certain about the answer, you can check it here: [eOppiva user organisations.](#))

I work for the Finland's central government (record the achievement and download certificate)

As an employee of a central government organisation, you can record the achievement and download the certificate this way:

- Use the link below to log into the eOppiva Moodle
(you will need a working Virtu user ID or user ID created using your work e-mail address).
- Enter the course key: **FAIR**
- Mark the training as completed. If you wish, you can also download a certificate on Moodle.

TO EOPPIVA MOODLE

I do not work for the Finland's central government (order certificate)

To receive the certificate by e-mail, do this:

- Order the certificate right away so that your achievement will not be lost!
- Click the “Order certificate” link below and enter your contact information on the form.
- You will be sent a certificate of completing the training by e-mail.

[ORDER CERTIFICATE](#)



Thank you for your participation!

Workgroup:

Tarmo Toikkanen, leading specialist, Sitra

Pinja Heimala, specialist, Sitra

Tone Knapstad, doctoral researcher, University of Helsinki

Beata Mäihäniemi, researcher, University of Lapland

Sanna Toropainen, doctoral researcher, University of Helsinki

Production: eOppiva 2024

Copyright to the training belongs to the working group. Please do not use the training materials without permission.

Learning is for everyone.