CEDPO
CONFEDERATION OF EUROPEAN DATA PROTECTION ORGANISATIONS

Bonn, Bucharest, Dublin, Lisbon, Madrid, Milan, Paris, The Hague, Vienna, Warsaw

Data Act
FAQ for DPOs

EU Digital Strategy Working Group
October 2025

Contact information:
https://cedpo.eu
info@cedpo.eu

Table of Contents

Foreword

It has been seven years since the GDPR came into effect, setting a strong foundation for data protection in Europe. As we move on, the regulatory landscape has continued to evolve to guide Europe towards a responsible digital future. The EU Data Act marks another milestone in this journey. The leaked draft of the Digital Omnibus shows that the Data Act will play an increasingly important role in regulating the digital space in the future.

For now, alongside other recent data laws, such as the Data Governance Act (DGA), the Digital Services Act (DSA), the Digital Markets Act (DMA), the Data Act introduces new obligations and opportunities. As a result, Data Protection Officers (DPOs) are increasingly required to extend their expertise beyond the GDPR, advising on a wider range of data governance and compliance issues.

To support the DPO community navigate these upcoming challenges, CEDPO through its EU Digital Strategy working group has collaborated with its experienced members from across Europe to develop practical and insightful answers to frequently asked questions (FAQs) related to the EU Data Act. These FAQs are specifically focused on addressing topics relevant to data protection.

We extend our sincere thanks to all members of the EU Digital Strategy Working Group (WG) and CEDPO staff for their invaluable contributions.

Contributing WG members: **Thomas Ajoodha, Filippo Bianchini, Lionel Capel, Julie Crawford, Paul Jordan, Paul Lambert, Dr Maria Maloney, Samira Marquaille, Massimo Pappalardo, Jeremiah Russel, Henry Simwinga.**

Dr. Sachiko Scheuing (GDD) & Filippo Bianchini (ASSO DPO)

Co-Chairs of the CEDPO EU Digital Strategy Working Group

Question 1: What is Data Act and what is its aim?

The Data Act is an integral part of the EU's legislative agenda with the objective of advancing the European data strategy, aimed at giving the EU a leading role in a data-driven society. The Data Act supports data to flow freely in a single market across several business, research, and public administration sectors. The Data Act aims to make data more accessible and usable for everyone through data sharing mechanisms. The law mandates Data Holders to make data available under relevant circumstances. At the same time, it empowers Users to benefit from the data they generate, for instance from their IoT devices. Concretely, the Data Act requires that connected products be designed so that users can directly access the data they generate (Art 3 Data Act). At first glance, this sounds similar to data portability and subject access rights under the GDPR. It can be seen as further specification to these rights. In cases where direct access is not possible, the data must be provided to Users quickly when they request it (Art 4 Data Act). The focus of the Data Act is on ensuring fair access to data and protecting user rights while balancing these goals with the protection of personal data.

The Data Act is consistent with existing rules on the processing of personal data, including the GDPR. It can be helpful to sometimes cross-reference the definitions with other relevant EU legislation. For example, the Free Flow of Non-Personal Data Regulation puts in place a key building block of the European data economy, by ensuring that non-personal data can be stored, processed and transferred anywhere in the EU.

Question 2: To whom does the Data Act apply?

The Data Act applies to organisations and persons who are responsible for producing, processing or using, managing, and sharing data derived from smart technology in the EU. In particular, the Data Act governs Data Holders, usually designers, manufacturers or service providers that either generate or can retrieve raw data from these smart technologies. The Data Act has a strong focus on Business-to-Business and Business-to-Consumer but also governs Business-to-Government data sharing.

Small and micro enterprises, along with medium sized organisations that have only been in existence for less than one year, are exempt from the sharing obligation as prescribed by Article 5 of the Data Act.

Question 3: To what type of data does the Data Act apply?

The Data Act applies to all raw and pre-processed data generated from the use of a connected product or a related service that is readily available to the Data Holder, such as the product

data (generated through the use of connected products), related service data (Users' action data), or metadata (data necessary to interpret product data and related service data). Raw and pre-processed data can be both personal and non-personal data. Data that have been heavily processed, such as inferred and derived data (e.g. highly enriched data, audiovisual material) generated using complex algorithms, are not subject to the Data Act.

The Data Act also differentiates raw data from inferred or derived data. In case the raw data is personal data, GDPR applies in addition to the Data Act.

Register of Processing Activities (RoPA) will be a good place to start in determining if the Data Act is applicable to your organisation.

Question 4: What are the different types of actors under the Data Act?

The Data Act defines the following three types of main actors: the Data Holder, the Data Recipient, and the User.

A **Data Holder** refers to an individual or an organisation that has lawful access to raw data, from connected products or related services, and has the authority to grant access to it. Essentially, a Data Holder is a person or legal entity with the right or obligation to use or share data generated or collected during the delivery of a related service. In practice, Data Holders are typically businesses, such as manufacturers of connected products or providers of related services, that manage smart devices and hold customer data collected through these devices. This role is arguably the most critical under the Data Act. Any organisation, whether public or private, that controls data generated by connected products and services, is considered a Data Holder.

The responsibilities of a Data Holder include facilitating access to the data and ensuring the ability to transfer data to other service providers in a user-friendly format, as specified by the act. They are also prohibited from imposing unfair contractual terms on users regarding access to their data and their rights to data portability.

A **Data Recipient** refers to an individual or organisation that receives raw data from a Data Holder at the request of the User. Essentially, a Data Recipient is a natural or legal person, other than the User, to whom the Data Holder provides data, including third parties acting on a user's request or in compliance with a legal obligation.

In practice, Data Recipients are typically legal entities such as companies, public authorities, research organisations, or not-for-profit organisations. There are specific boundaries in place to restrict large providers, or "gatekeepers" under the Digital Markets Act, from acting as third parties in certain data-sharing arrangements.

In essence, a Data Recipient is an entity that receives data from a Data Holder with the intention of using it for business or professional purposes. This could involve companies analysing User behaviour data, providing cloud storage for data generated by connected devices, or offering

data-driven services. The key distinction is that a Data Recipient uses the data for commercial or organisational purposes, rather than for personal use, as a data User might.

A User refers to an individual or organisation that owns or has the right to use a connected product or receive related services. Essentially, a User is the natural or legal person who owns, rents, or leases a smart device.

In practice, the User is typically the customer of a smart device. It's important to note that individuals who use the device but are not party to the agreement, such as family members, are probably not considered Users.

Question 5: What is non-personal data?

The Data Act defines non-personal data as any data that does not fall under the category of personal data, as specified in Article 2(4) of the Data Act. While the GDPR refers to anonymous data as information that cannot be linked to an identified or identifiable natural person in Recital 26; it does not explicitly define non-personal data.

The Regulation on a Framework for the Free Flow of Non-personal Data within the European Union introduces non-personal data in Article 1 as "data other than personal data." In comparison to the definition of personal data in Article 1, non-personal data can be understood as any information that does not relate to an identified or identifiable natural person (the 'data subject'). The EU Commission's 2019 Guidance on the Regulation on a framework for the free flow of non-personal data supports this interpretation.

Furthermore, the Commission classifies non-personal data into two categories:

(1) data that originally did not pertain to an identified or identifiable natural person, and
(2) data that were initially personal but were later anonymised.

Temperature readings of a building is an example of (1), and average age of students in a classroom is an example of (2).

It is important to note that anonymisation of personal data is different from pseudonymisation. While anonymisation involves processing data so that it cannot be attributed to an individual, pseudonymisation refers to data that can still be attributed to a person through additional information. It is also important to note that pseudonymised data becomes anonymous data when in hands of organisations that have no means to reidentify the data subject1.

Examples of non-personal data include aggregated or anonymised datasets used in big data analytics, precision farming data that helps optimise pesticide and water usage, and data on maintenance needs for industrial machinery. However, if technological advancements enable the re-identification of anonymised data, such data would be considered personal data, and the GDPR would then apply.

[1] Judgement of 4 September 2025, EDPS vs SRB, C-413/23 P, ECLI:EU:C:2025:645

Question 6: How shall I treat a file that contains both personal data and non-personal data?

Most of the data covered by the Data Act is classified as 'non-personal,' as it pertains to industrial products and services rather than individuals. However, it is not uncommon for this data to be mixed with personal data. When a file contains both personal and non-personal data, it is referred to as a mixed dataset.

Regarding mixed datasets, Recital 7 of the Data Act notes that the GDPR [2] and the ePrivacy Directive (where applicable) provide the foundation for sustainable and responsible data processing.

A slightly different nuance is found in another EU regulation which mentions mixed datasets; the Regulation on a Framework for the Free Flow of Non-personal Data in the European Union. According to this law, and the Commission guidance on the Free Flow of Non-personal Data Regulation, the following applies:

1. the 'Free Flow of Non-Personal Data Regulation' applies to the non-personal data part of the set;
2. The GDPR applies to the personal data part of the set;
3. If the non-personal data and the personal data are "inextricably linked", GDPR will apply to the whole data set, even if the personal data represents a small part of the set.

The Commission's guidance goes on to explain that non-personal data and personal data are "inextricably linked" when it is impossible or technologically or economically not feasible to separate the two types of data.

The recommendation for handling mixed datasets is to ensure adequate protection and comply with obligations under the GDPR. However, when it is not possible to identify the data subject, the Data Controller is exempt from obligations under Articles 15 to 20 of the GDPR. These obligations include the rights to rectification, erasure, restriction of processing, the notification obligation for rectification or erasure or restriction of processing, and data portability, as outlined in Article 11 of the GDPR.

Question 7: When should my organisation use technical and organisational measures to protect the data?

When processing personal data, appropriate technical and organisational measures must be implemented to protect the data. One protective measure that is emphasised in both the GDPR

[2] And the 2018 *Regulation on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data*

and the Data Act is pseudonymisation. It is recommended to apply the same standard of pseudonymisation under the Data Act as is required by the GDPR.

The Data Act also addresses protective measures in situations where personal data must be shared with a public sector body, the Commission, the European Central Bank, or an EU institution due to an "exceptional need." In such cases, the requesting organisation is required to specify the technical and organisational measures necessary to protect the data. Additionally, the requesting organisation should assess whether the personal data can be anonymised.

On the other hand, the Data Holder must anonymise personal data unless the request to make data available to a public sector body, the Commission, the European Central Bank, or an EU institution necessitates the disclosure of personal data. In such instances, the Data Holder is required to pseudonymise the data.

National laws may eventually be established to govern the disclosure of other types of data in specific situations, such as medical or statistical data. When this data cannot be aggregated and must be shared as personal data, an appropriate level of technical and organisational measures should be implemented to protect it.

Question 8: what needs to be considered to minimise risks associated with the Data Act?

The EU Data Act establishes a single, coherent framework for sharing both personal and non-personal data within the European Single Market. Its goals are to ensure fairness in data-driven value chains, improve user access to data generated by connected products and related services, and stimulate innovation across sectors.

At the same time, making more data available inevitably heightens exposure to misuse, privacy breaches, loss of trade secrets, cybersecurity incidents, and discriminatory or unequal access. The Act therefore couples the new access rights with a set of layered safeguards that vary according to the relationship in which data are shared: business-to-consumer (B2C), business-to-business (B2B), and business-to-government (B2G).

Risk mitigation in B2C and B2B relationships

In B2C contexts (Articles 3 and 4), connected products and related services must be designed so that data is, by default, directly accessible to users in a structured, secure, and machine-readable format. Consumers must receive access free of charge and be protected from unfair or opaque contractual terms. They must retain meaningful control over their data, including options to grant or revoke access and manage reuse conditions.

In B2B relationships, where imbalances may exist, the Data Act allows parties to define contractual restrictions on the use or further sharing of data when such use could threaten safety, health or trade secrets (Articles 4(2) and 4(6)). Agreements must include confidentiality clauses and businesses can suspend data sharing if the agreed measures are not implemented

or if trade secrets are compromised (Article 4(7)). The Act requires that such terms be fair and avoid exploiting asymmetries in bargaining power, especially for SMEs (Article 5(3)).

Technical and organisational protections

The Data Act allows Data holders to implement technical protection measures such as encryption, access controls and smart contracts to prevent unauthorised access or use (Article 11(1)). These measures must not prevent legitimate user access, but they are crucial for ensuring compliance and protecting sensitive information. Data holders may also rely on pseudonymisation and secure data transfer protocols, particularly when data involves sensitive information or third-party access.

Data sharing is also subject to purpose limitation. Third parties must only process the data for the purposes agreed with the user and must delete it once no longer necessary (Article 6(1)). For personal data, full compliance with the GDPR is mandatory. If these obligations are breached, data holders may require the deletion of data and the cessation of derived services or products (Articles 11(2) to 11(4)). In B2B contexts, technical measures can also include audit trails to monitor compliance.

Managing trade secrets across sharing scenarios

Whether data is shared with users or third parties, the Act provides strong protections for trade secrets. These can only be disclosed if strictly necessary and if appropriate technical and contractual safeguards are in place (Articles 4(6) and 5(9)). If such protections are not respected, data holders may suspend sharing and must inform the competent authority (Article 5(10)). Contracts must define how trade secrets are protected and specify confidentiality obligations.

Public sector access and the B2G dimension

In exceptional cases, public authorities may request data when there is a clear public interest (Article 17). These requests must be specific, proportionate and justified. The authority must use the data only for the stated purpose, apply strict security measures and delete the data when no longer needed (Articles 18 and 19). Where possible, anonymisation or pseudonymisation must be applied to personal data. Public bodies must also implement technical and organisational measures similar to private actors and comply with confidentiality requirements when handling sensitive data.

Context matters

The obligations and protections laid out in the Data Act are context sensitive. B2C sharing focuses on user empowerment and consumer protection. B2B relationships emphasise fair contracting and confidentiality. B2G access is limited to exceptional needs and is strictly regulated. This layered approach allows for effective risk mitigation without imposing a one size fits all model.

In conclusion, by defining tailored rules for different data sharing contexts and promoting the use of contractual, technical and organisational safeguards, the Data Act provides a strong legal foundation for minimising risks. However, operationalising these safeguards requires more than

legal compliance. Technical solutions including APIs and standardised access mechanisms play a key role in ensuring secure, auditable and trustworthy data sharing across all actors.

Question 9: What is a commonly used method for sharing data per the Data Act, and what are ways to reduce data protection risks?

There are several ways to reduce risks associated with the Data Act; implementing data-sharing governance policies is the first step. As with GDPR compliance, robust management of data sharing can be formalised through contracts and documentations defining each party's roles and responsibilities; this is particularly useful between data holders and third parties. Contracts could include procedures for managing access and, if necessary, assigning access control rights, setting security requirements, as well as ensuring accountability and traceability.

The data recipient is generally a data processor within the sharing process. However, the contract with the third party could provide for joint processing responsibility if the third party, in law or practice, exercises a determining influence over the processing objectives and conditions. This could apply, for instance, when the third party provides a sharing API that the data holder connects to for data sharing.

Measures to prevent unauthorised access, recommended by various national regulators: As with the GDPR, a risk-based approach should be taken, where the level of protection required is commensurate with the severity of the possible consequences for the Data Subject or User. For instance, the recommendation of the French data protection authority, CNIL, includes the following:

- Partition the data to be share through either physical or logical data segmentation, or both. Availability of data may become important in certain situations, where user may be seriously impacted without it. In such situations, keeping data in separate 'compartments' may reduce potential data breach.
- Use of additional technical measure, such as a digital safe, to protect passwords and authentication protocols.
- Maintain a comprehensive log of access and actions performed on the database to identify any data misuse and errors, as well as ensure Data Holder / Data Recipient (or its agent) has provided necessary data updates within continuous sharing.
- Create a "sandbox" environment for data sharing in which Users can safely experiment with the data.

Because of the specific type of data covered by Data Act, data transfer via Application Programming Interfaces (APIs) may be the most commonly used method. APIs support the secure exchange of personal and non-personal data between data holders and authorised third parties. APIs generally offer a higher level of security than data-sharing platforms or email services, through which risk of data breaches can be reduced during sharing.

APIs are a preferred tool for data sharing, particularly when:

- Large volumes of data are updated frequently,
- Third parties need to regularly access the data to meet user access requests, especially when there is a high number of such requests, and
- The third party directly transfers data to the user without permanent data storage.

Question 10: What are the obligations of the Data Holder?

The EU Data Act establishes several key obligations for Data Holders.

Data Access by Design and by Default

Data Holders must design, and manufacture connected products or related services (such as smart devices) so that the data generated by the device is accessible by default and free of charge to the User. This includes relevant metadata necessary for interpreting and using the data. Access must be easy, secure, comprehensive, structured, and provided in a common and machine-readable format.

Data Access Requests

If Users cannot directly access the data via the smart device, the Data Holder must share the data upon request. These requests must be fulfilled without undue delay, in a common and machine-readable format, free of charge, and, where relevant and feasible, continuously and in real-time. Additionally, Users can request that the Data Holder share the data generated by the device with a third party. When fulfilling such a request, the Data Holder must provide the data under the same conditions described above. Unlike sharing data with the User, however, the Data Holder in such a scenario may charge reasonable compensation from the third party for sharing the data. The Data Holder must ensure that access requests can be processed in a straightforward manner and not burdened by unnecessary procedures or information requests from the User.

Transparency

Before entering into a contract for purchasing, renting, or leasing a connected product, the Data Holder must provide the User with clear and comprehensible information. This includes details on the type and volume of data, data retention periods, whether the product generates data continuously and in real-time, and whether the data is stored remotely or on the device. The User must also be informed about how to exercise their rights to access, retrieve, or delete data.

Similarly, before entering into a contract for services related to a connected product, the Data Holder must inform the User about the type and volume of data, data retention periods, third parties who may use the data, and the purposes for which the data is used. The Data Holder must also explain how the User can request data sharing with a third party, end data sharing, and lodge a complaint in case of non-compliance with the Data Act.

Data Portability

The Data Act empowers Users to transfer their data to a third party, facilitating switching between service providers or using data with different applications. The Data Holder must make this process seamless and ensure the data is provided in a commonly used and machine-readable format.

Question 11: How do I formalise data sharing in a Business-to-Business context?

The terms and conditions for data sharing must be formalised in a contract between the parties involved. The agreement must be fair, reasonable, non-discriminatory, and transparent, which is especially important when the contracting party is a small or medium-sized business, a non-profit organisation, or a research institution.

When a Data Holder shares data with another business (the Data Recipient) under the Data Act, they may request a reasonable fee from the Data Recipient for the data provided.

Question 12: My organisation is a Data Holder. Can I refuse to make data available?

The User and Data Holder may restrict data access if such access could compromise the product's security requirements as mandated by law. They may also agree to limit or prohibit the access, use, or further sharing of data.

In cases involving trade secrets, the Data Holder is authorised to establish arrangements for maintaining data confidentiality and protecting trade secrets. This includes agreeing on technical and organisational measures to ensure confidentiality.

Additionally, there is no obligation for the Data Holder to share data with a third party located outside the EU.

Question 13: What is the impact of the Data Act on the management of data subject rights in cases where the data is personal data?

The Data Act does not alter the rights and obligations established under the GDPR. Conversely, it reinforces and facilitates the right to data portability. Specifically, the Data Act requires Data Holders to enable customers to switch their data within 30 days.

When dealing with personal data, the Data Holder in many cases will act as the data controller and must handle data access requests in accordance with the GDPR. In cases where User is an organisation, the User becomes the data controller. The data controller must verify whether personal data is involved and ensure there is a legal basis for making such data available, especially if the User is not the data subject.

Question 14: What are the legal bases that can be used for the processing of personal data, to which Data Act applies?

The Data Act operates without prejudice to the GDPR, meaning that the GDPR takes precedence over the Data Act (Art. 1(5), Rec. 7 Data Act). Consequently, every processing of personal data must have a valid legal ground.

Data Holders have legal grounds under Articles 6 of the GDPR. If the data subject is also the sole User, the situation is straightforward, as the Data Holder can rely on the legal ground of compliance with a legal obligation (see Art. 6(1)(c) of the GDPR, Art. 4 Data Act). However, if the User is an organisation with multiple individuals using the connected device, the situation can become more complex. For instance, if a company uses a shared vehicle, the company must select a legal ground that considers employee data. In such cases, processing personal data generated by employees using a pool vehicle may need to be based on consent (Art. 6(1)(a) and Art. 9(2) of the GDPR) or performance of a contract (Art. 6(1)(b) of the GDPR). It is important to note that the Data Act heavily relies on contractual agreements, thus complementing Art. 6(1)(b) of the GDPR for processing personal data under contract. For example, under a contract, a User may share personal data with a third party to provide a service, using Art. 6(1)(b) as the legal basis.

Finally, in most cases, the Data Recipient will process the data on behalf of the Data Holder or User.

Question 15: My organisation is a User and would like to process the data made available by the Data Holder on the basis of Legitimate Interest. Will that work?

According to Article 6 (1) f of the first subparagraph of Article 6(1) of the GDPR processing can be regarded as necessary for legitimate interests pursued by the controller or by a third party, only on condition that:

- the data controller has informed the Users of a legitimate interest that is pursued by the data processing;

- such data processing is carried out only in so far as is strictly necessary for the purposes of that legitimate interest; and
- that it is apparent from a balancing of the opposing interests, having regard to all the relevant circumstances, that the interests or fundamental freedoms and rights of the Users do not override that legitimate interest of the controller or of a third party.

The balancing test essentially weighs the competing interests of the data controller against the interests or fundamental rights and freedoms of the data subjects.

Evaluating the limitations and restrictions?

The use of personal data generated by connected devices can be restricted or limited in accordance with applicable EU and national laws. For example, national employment laws may regulate the monitoring of employees using connected devices in the workplace.

Additionally, legitimate interest cannot be used as a legal basis when data received from the Data Holder falls under the special categories of personal data as defined in Article 9 of the GDPR. This includes biometric data and health-related data generated by connected medical devices.

Moreover, when the data received from the Data Holder is processed for automated decisions that produce legal effects concerning the data subject or similarly significantly affect them (such as automated credit scoring), legitimate interest cannot be used as a valid legal ground.

In these cases, a different legal basis will be required.

Examples of interests or fundamental rights and freedoms of data subject

The rights and freedoms at stake depend, in principle, on the specific circumstances of the particular case3.

By way of example, the sharing or the use – not agreed with the User - of the personal data generated by a connected car or by a home assistant may represent a threat:

- for the private and family life of the data subjects, protected by Article 7 of the Charter of Fundamental Rights of the EU (the "Charter"); and
- for the right to security, protected by Article 6 of the Charter.

How the DPO can assist in this process

The balancing test must be conducted on a case-by-case basis, taking into account all possible risks to the data subjects. According to Opinion 06/2014 of the WP29 on the notion of legitimate interests of the data controller, the data controller should:

- Identify the fundamental rights and interests of the data subject that could be impacted.
- Consider the reasonable expectations of the data subjects.
- Evaluate the impacts on the data subject and compare them with the benefits expected from the processing by the data controller.

[3] See judgment of 4 May 2017, *Rīgas satiksme*, C-13/16, EU:C:2017:336, paragraph 31

It is important to note that children deserve specific protection concerning their personal data, as they may be less aware of the potential risks.

While the role of the DPO in legitimate interest assessment is not specifically regulated by the GDPR, it is analogous to the DPO's role in a Data Protection Impact Assessment. Therefore, the DPO should provide advice, when requested by the data controller, regarding the balancing test and monitor its execution.

Question 16: My organisation is a public body. In what situations can my organisation request data based on "exceptional need"?

The concept of "exceptional need" is introduced early in the Data Act, where Article 1(1) outlines that part of the Act's purpose is to harmonise rules on the availability of data held by the Data Holder to public bodies when there is an "exceptional need" for the data to perform a specific task carried out in the public interest. This sets a high standard, limiting the provision to public-type bodies and requiring an "exceptional need," specifically for a task in the public interest. The data made available is restricted to fulfilling this exceptional need.

If there are alternative means to accomplish the task, some may argue that this provision does not apply. The term "exceptional" is likely to exclude normal, regular usage, implying that only truly extraordinary circumstances qualify. Additionally, there must be a predetermined, identified task that is both exceptional that triggers this need. If a public body cannot clearly identify and document such an "exceptional need" and "specific task" in advance, it may not be able to invoke this provision.

Moreover, the scoping provision should be read in conjunction with the specific details of what constitutes an exceptional need and when it applies, as further elaborated later in the Data Act. Article 1(3) reinforces these potential limitations, stating that data can only be made available "where there is an exceptional need." This raises a cautionary note that the scoping provision might inadvertently limit the application of later provisions, possibly in ways not intended by the legislation.

The main definitions within the Data Act do not explicitly define "exceptional need." However, Article 2(29) groups "public emergency" and "exceptional situations" together, which might lead some to interpret exceptional need as being limited to public emergencies. The term "exceptional circumstances" is also mentioned in various contexts, such as in Articles 4(7) and 5(11), including those related to intellectual property.

The primary provisions regarding exceptional need are detailed in Chapter V. Article 14, titled "Obligation to Make Data Available on the Basis of Exceptional Need," states that when a public sector body, the Commission, the European Central Bank, or a Union body demonstrates an exceptional need, as defined in Article 15, to use certain data—including the relevant metadata necessary to interpret and use those data—these bodies must make a duly reasoned request.

Legal entities, other than public sector bodies, that hold the relevant data are then required to make it available.

Article 15 specifies that the "exceptional need" must be limited in both time and scope and can only exist under certain circumstances, which are clearly enumerated in a fixed list. For example, Article 15(1)a addresses responding to a public emergency, while Article 15(12)b covers other circumstances that must not involve personal data. Notably, there is an exclusion for micro and small enterprises under Article 15(2), although even small enterprises with a modest turnover may manage significant amounts of data.

Article 17 emphasises that the public body must "demonstrate" the exceptional need, which implies a higher standard of proof than simply labelling a need as exceptional. This requirement could exclude situations that are not genuinely exceptional. Article 17(1)c specifically mentions the need to explain how personal data will be handled, potentially raising contentious issues regarding interpretation and application. Additionally, Article 17(2)e mentions the requirement for pseudonymisation, and Article 17(2)c stresses the importance of proportionality in assessing exceptional need, further limiting its application.

Article 18(2) addresses the process for responding to data requests, including timelines, modifications, and distinctions between public emergency exceptional need and other types of exceptional need. Compensation for the provision of data may also be considered, as outlined in Article 20. Furthermore, data sharing for research and statistical organisations in the context of exceptional need is discussed in Article 21.

References to exceptional need appear throughout the Data Act, particularly in Recitals 5, 31, 63, 65, 66, 69, 70-73, 75, 77, 103, and 107, among others. These references and the specific articles together provide the framework for understanding and applying the concept of exceptional need within the Data Act.

Question 17: How is profiling defined under the Data Act?

The same definition for profiling is used in both the GDPR and the Data Act, namely Article 4(4) of the GDPR, which defines profiling as *"any form of automated processing of personal data consisting of using personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."*

Question 18: Is profiling prohibited under the Data Act?

Profiling is generally not prohibited under the Data Act. However, profiling is not permitted in a very specific context, namely, when *User* (often the data subject) shares the data with organisations. Article 6(2)b of the Data Act strengthens User rights and provides another avenue for Users to better protect themselves from unwanted profiling practices.

This situation is stated in Article 6(2)b of the Data Act:

6.2 The Third Party shall not:

…(b) notwithstanding Article 22(2), points (a) and (c), of Regulation (EU) 2016/679, *use the data it receives for the profiling, unless it is necessary to provide the service requested by the User;*

To provide clarity of interpretation, we outline below the relevant parts of Article 22 of the GDPR. Article 22(1) states:

1. The data subject shall have the right ***not to be*** *subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.*

Then, **Article 22(2) points (a) and (c)** of the GDPR states:

(a) Paragraph 1 shall not apply if the decision: is necessary for entering into, or performance of, a contract between the data subject and a data controller;
(b) …
(c) is based on the data subject's explicit consent.

There may be some confusion when interpreting both texts together, especially given the number of negative statements involved. The clause "notwithstanding Article 22(2), points (a) and (c), of Regulation (EU) 2016/679" should be understood as "in spite of Article 22(2) points (a) and (c)." Under normal circumstances, Article 22(2) outlines two exceptions to Article 22(1). However, these two exceptions do not apply in the context of Article 6.2(b) of the Data Act.

For further clarification, Article 6(2)b should be interpreted in conjunction with Article 5 of the Data Act. When done so, it becomes clear that profiling is prohibited in situations where the following three cumulative criteria apply, where:

- Personal data in question is part of a product (say an automatic espresso machine) or service data created through the use of connected products, and,
- Personal data is shared by the User of the espresso machine with your company, and your company is not the Data Holder, and,
- Profiling is not necessary for providing the data subject with the service requested.

Once this interpretation has been clarified, the next key question lies in determining what constitutes "*necessary to provide the service requested by the User.*" This will likely be interpreted on a case-by-case basis. For example, a *User* of a music streaming service shares his/her usage data to another media entertainment company, so that he/she can enjoy the same personalised recommendations. This requires the media entertainment company (*Data Recipient*) to carry out profiling. Since the request comes from the *User*, and profiling is necessary to deliver the requested service, this type of profiling by the *Data Recipient* will most likely be permissible. However, the media entertainment company cannot carry out profiling to find out the time of the day podcasts are listened to, for the media entertainment company to improve their operational processes. This would likely violate Article 6(2)b.

The underlining assumption may be that *Data Recipients* are not the original Data Holders, they would most likely have limited control or understanding over how the data was collected or how the User intended it to be used. Profiling for services unrelated to the product or service

the User signed up for would be seen as an intrusion on their data protection rights under the GDPR and for good reason.

Consider the following scenario: a utility company could potentially use thermostat data of residential homes around energy consumption for their own financial benefit. The company could analyse energy consumption patterns and identify peak usage times, i.e. evenings and weekends, and make this available to the homeowners. They may even be able to compare energy usage patterns across similar households or building types for homeowners as benchmarks. Imagine a situation where a client of the utility company chooses to move to another utility company. A request can be raised to share the thermostat data so that the new utility company can provide energy saving advice, and the client can make use of it from day one of moving over to a new utility company. Where profiling is necessary for this purpose, it is permitted to do so in this scenario.

The new utility company may then consider creating loyalty profile that can be used to choose incentivise energy plans that can bind the person to a longer contractual term with a discounted rate. If the homeowner switches over to the new plan, the new utility company will benefit from financial stability, and the homeowner will have reduced costs. However, since the creation of a profile is strictly speaking not necessary to provide the service for the homeowner, the Data Act prohibits this profiling by the new utility company.

Question 19: Why is transparency crucial under the Data Act?

When we traditionally consider data and transparency, we focus on transparency rules related to providing upfront details about how personal data will be used and obtaining clear and fair consent for its collection. Transparency also plays a role in ensuring that individuals are aware of their data rights and can exercise them. Additionally, transparency is crucial in data contracts, policies, and terms and conditions between entities, as well as between entities and individuals.

In the context of the Data Act, however, the purpose of transparency shifts slightly. While traditional data protection rules remain in place, the Data Act emphasises transparency in the context of data sharing between entities. For instance, Article 5 highlights the need for transparency and fair, non-discriminatory conditions when Data Holders make data available to Data Recipients, particularly in data transfers between entities. Here, transparency may align more with competition rules than with traditional data protection rules.

Disagreements may arise regarding this interpretation, but these issues will more than likely become clearer as dispute bodies established under Article 10 begin to adjudicate on such matters as transparency. It will be important to see whether these procedural rules only consider the Data Act or if they will also consider data protection rules.

Article 28 of the Data Act refers to the traditional model of providing prior information, particularly concerning contractual obligations related to international data access and transfer. Although the section does not explicitly mention "transparency," the obligations for prior

information via websites are clear, and practitioners will need to fully address these requirements to avoid potential issues.

Transparency is also addressed in Article 19, which introduces "transparency obligations" that may mandate the retention of data in certain circumstances, potentially overriding requirements to delete or erase data. This particularly applies to public sector bodies.

Moreover, even where explicit transparency requirements are absent, such requirements may be necessary or implied for other provisions to function effectively. For instance, it may be challenging to justify an action if certain aspects occurred in a less than transparent manner. This is closely tied to the concept of understanding and respecting the reasonable expectations of individuals. A practical example is considering whether the historical use of data can be extended to a new AI application without violating these expectations.

Finally, transparency is also mentioned in several Recitals of the Data Act, including Recitals 5, 24, 25, 34, 42, 51, 65, 69, and 73, which readers may wish to review for further context.

Useful Links

- Data Act text https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng
- Information on European Data Strategy https://digital-strategy.ec.europa.eu/en/policies/strategy-data
- European Commission's website on Data Act https://digital-strategy.ec.europa.eu/en/policies/data-act, including a FAQ about the Data Act at https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act
- Regulation on Framework for the free flow of non-personal data in the European Union https://eur-lex.europa.eu/eli/reg/2018/1807/oj
- Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2019:250:FIN
- GDPR https://eur-lex.europa.eu/eli/reg/2016/679/oj
- CNIL guidance: Recommendation on the use of application programming interfaes (API) for the secure sharing of personal data (in French) https://www.cnil.fr/sites/cnil/files/2023-07/recommandation_api.pdf

Disclaimer

The information provided in this FAQ is for general insight and educational purposes only. It should not be interpreted as legal advice. For guidance specific to your situation, please consult a qualified legal professional.