



LIGHTINGEUROPE
THE VOICE OF THE LIGHTING INDUSTRY

LightingEurope's Explicative Note on the Data Act

REGULATION (EU) 2023/2854

January 2026

INTERNAL DOCUMENT – Reserved for LightingEurope members

Table of Contents

1.	Introduction	1
1.1	In a nutshell	1
1.2	Background & timeline	1
2.	Chapter I – General Provisions	2
2.1	Scope (Article 1)	2
2.2	Definitions (Article 2)	2
3.	Chapter II – B2C and B2B Data Sharing	5
3.1	Obligation to make product data and related service data accessible to the user (Article 3)	5
3.2	Rights and obligations of users and data holders with regard to access, use and making available product data and related service data (Article 4)	6
3.3	Right of the user to share data with third parties (Article 5)	7
3.4	Scope of data sharing obligations (Article 7)	8
4.	Chapter III – Obligations of Data Holders Under Union Law	9
4.1	Conditions under which data holders make data available to data recipients (Article 8)	9
4.2	Compensation for making data available (Article 9)	9
4.3	Dispute settlement (Article 10)	9
4.4	Technical protection measures on the unauthorised use or disclosure of data (Article 11)	10
5.	Chapter IV: Unfair Contractual related to data access and use between enterprises	11
5.1	Unfair contractual terms unilaterally imposed on another enterprise (Article 13)	11
6.	Chapter V: Making Data Available to Public Sector and EU Bodies in Exceptional Cases	12
6.1	Obligation to make data available on the basis of an exceptional need (Article 14)	12
6.2	Exceptional need to use data (Article 15)	12
6.3	Obligations of data holders when complying with requests for data (Article 18)	13
6.4	Compensation in cases of an exceptional need (Article 20)	13
7.	Chapter VI: Switching Between Data Services	14
7.1	Removing obstacles to effective switching (Article 23)	14
7.2	Contractual terms concerning switching (Article 25)	14
7.3	Gradual withdrawal of switching charges (Article 29)	14

7.4	Technical aspects of switching (Article 30)	15
8.	Chapter IX: Implementation & Enforcement	16
8.1	Competent authorities and data coordinators (Article 37)	16
8.2	Penalties (Article 40)	16
8.3	Model contractual terms and standard contractual clauses (Article 41)	16
8.4	Role of the European Data Innovation Board (EDIB) (Article 42)	16

1. Introduction

1.1 In a nutshell

This explicative note, reserved for LightingEurope members, summarises the most important sections of the EU Data Act (Regulation (EU) 2023/2854) and provides some notes to help companies interpret key provisions and to guide attention to crucial aspects of the law.

The document brings attention to some obligations for producers of connected products and providers of related services within the lighting industry. The structure follows a breakdown of the Regulation's key chapters and selected articles.

1.2 Background & timeline

The regulation lays out harmonised rules on fair access to and use of data. More specifically, the Data Act clarifies who can use what data and under which conditions. The act itself is also a reaction to the increasing number of connected products being developed and entering the EU market.

The GDPR sets the legal basis for data privacy and data protection, while the Data Act allows users (businesses or individuals that own, lease, or rent such a product) to better control the data they generate. It specifies cases in which a business has a legal obligation to share data with another business

IMPORTANT NOTES

The Regulation entered into force on 11 January 2024 and **started applying from 12 September 2025**.

- ➔ The obligation resulting from Article 3(1) will apply to connected products and the services related to them placed on the market **after 12 September 2026**.
- ➔ Chapter IV will apply to contracts concluded after 12 September 2025.
- ➔ Chapter IV will apply from 12 September 2027 to contracts concluded on or before 12 September 2025, provided that they are:
 - of indefinite duration, or
 - due to expire at least 10 years from 11 January 2024.

2. Chapter I – General Provisions

2.1 Scope (Article 1)

The regulation covers personal and non-personal data and **regulates the making available of product data and related service data to users** of the connected product or related services, and the making available of data, by data holders to data recipients (including public sector bodies). The Regulation will apply, inter alia, to:

- manufacturers of connected products placed on the market in the Union and providers of related services, irrespective of the place of establishment of those manufacturers and providers;
- users in the Union of connected products or related services;
- data holders, irrespective of their place of establishment, that make data available to data recipients in the Union;
- data recipients in the Union to whom data are made available;
- providers of data processing services, irrespective of their place of establishment, providing such services to customers in the Union;

2.2 Definitions (Article 2)

To identify the correct scope and area of interest, note the following definitions:

1) '**data**' means any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording

(5) '**connected product**' means an item that obtains, generates or collects data concerning its use or environment and that can communicate product data via an electronic communications service, physical connection or on-device access, and whose primary function is not the storing, processing or transmission of data on behalf of any party other than the user;

(6) '**related service**' means a digital service, other than an electronic communications service, including software, which is connected with the product at the time of the purchase, rent or lease in such a way that its absence would prevent the connected product from performing one or more of its functions, or which is subsequently connected to the product by the manufacturer or a third party to add to, update or adapt the functions of the connected product;

(7) '**processing**' means any operation or set of operations which is performed on data or sets of data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or other means of making them available, alignment or combination, restriction, erasure or destruction;

(8) **‘data processing service’** means a digital service that is provided to a customer and that enables ubiquitous and on-demand network access to a shared pool of configurable, scalable and elastic computing resources of a centralised, distributed or highly distributed nature that can be rapidly provisioned and released with minimal management effort or service provider interaction;

(13) **‘data holder’** means a natural or legal person that has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation adopted in accordance with Union law, to use and make available data, including, where contractually agreed, product data or related service data which it has retrieved or generated during the provision of a related service;

(14) **‘data recipient’** means a natural or legal person, acting for purposes which are related to that person’s trade, business, craft or profession, other than the user of a connected product or related service, to whom the data holder makes data available, including a third party following a request by the user to the data holder or in accordance with a legal obligation under Union law or national legislation adopted in accordance with Union law;

(15) **‘product data’** means data generated by the use of a connected product that the manufacturer designed to be retrievable, via an electronic communications service, physical connection or on-device access, by a user, data holder or a third party, including, where relevant, the manufacturer;

Merely descriptive data, such as information in user manuals, serial numbers, or model identification, is **not considered product data**.

(17) **‘readily available data’** means product data and related service data that a data holder lawfully obtains or can lawfully obtain from the connected product or related service, without disproportionate effort going beyond a simple operation;

(21) **‘making available on the market’** means any supply of a connected product for distribution, consumption or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge;

(22) **‘placing on the market’** means the first making available of a connected product on the Union market;

(25) **‘small enterprise’** means a small enterprise as defined in Article 2(2) of the Annex to Recommendation 2003/361/EC;

26) **‘microenterprise’** means a microenterprise as defined in Article 2(3) of the Annex to Recommendation 2003/361/EC;

(32) '**digital assets**' means elements in digital form, including applications, for which the customer has the right of use, independently from the contractual relationship with the data processing service it intends to switch from;

(33) '**on-premises ICT infrastructure**' means ICT infrastructure and computing resources owned, rented or leased by the customer, located in the data centre of the customer itself and operated by the customer or by a third-party;

3. Chapter II – B2C and B2B Data Sharing

A data holder is an entity that can use or make available data, including product data or related service data retrieved or generated during the provision of the related service. **Typically, the manufacturer is a data holder.** However, the manufacturer may outsource that role to another entity. Also, a company that provides a related service is typically a data holder.

If a company's role is limited to being a retailer or seller of a smart product, then the data holder obligations fall to the manufacturer or the related service provider. For example, the manufacturer of a control gear controllable via some protocol in a luminaire is typically not a data holder since the data created is usually provided to the dashboard of a service provider.

3.1 Obligation to make product data and related service data accessible to the user (Article 3)

Manufacturers of connected products shall ensure that the products and related services provide product data and related service data and metadata securely, free of charge and structured in commonly used and machine-readable format. Before concluding a contract for purchase, lease or rent of a connected product, the seller/rentor/lessor/manufacturer must provide the following information:

the type, format and estimated volume of product data which the connected product is capable of generating;
whether the connected product is capable of generating data continuously and in real-time;
whether the connected product is capable of storing data on-device or on a remote server, including, where applicable, the intended duration of retention
how the user may access, retrieve or, where relevant, erase the data, including the technical means to do so, as well as their terms of use and quality of service

The article also lays out the information from the provider of a related service.¹ It is necessary to provide the following information before concluding a contract:

¹ Keep in mind the definition of a related service as a digital service for the connected product the absence of which “would prevent the connected product from performing one or more of its functions, or which is subsequently connected to the product by the manufacturer or a third party to add to, update or adapt the functions of the connected product”

the nature, estimated volume and collection frequency of product data that the future prospective data holder is expected to obtain and, where relevant, the arrangements for the user to access or retrieve such data, including the prospective data holder's data storage arrangements and the duration of retention;
the nature and estimated volume of related service data to be generated, as well as the arrangements for the user to access or retrieve such data, including the future data holder's data storage arrangements and the duration of retention;
whether the prospective data holder expects to use readily available data itself and the purposes for which those data are to be used, and whether it intends to allow one or more third parties to use the data for purposes agreed upon with the user;
the identity of the prospective data holder , such as its trading name and the geographical address at which it is established and, where applicable, of other data processing parties;
the means of communication which make it possible to contact the prospective data holder quickly and communicate with that data holder efficiently;
how the user can request that the data are shared with a third party and, where applicable, end the data sharing
the user's right to lodge a complaint alleging an infringement of any of the provisions of this Chapter with the competent authority designated pursuant to Article 37
whether a prospective data holder is the holder of trade secrets contained in the data that is accessible from the connected product or generated during the provision of a related service, and, where the future data holder is not the trade secret holder, the identity of the trade secret holder;
the duration of the contract between the user and the prospective data holder, as well as the arrangements for terminating such a contract

3.2 Rights and obligations of users and data holders with regard to access, use and making available product data and related service data (Article 4)

Obligations for data holders → [Key requirements for producers of connected products](#)

Data holders, **if the data is not directly accessible to the user**, must make the data available, upon request of the user, with the same characteristics as if it were directly available. Access limitations or restrictions to the data can be contractually agreed upon if the processing could undermine security requirements of the connected product, resulting in a serious adverse effect on the health, safety, or security of natural persons. If the data holder refuses to share the data, it shall notify the competent authority as per Article 37. For authentication purposes, data holders can ask only for the necessary information from users and are not allowed to register or log data beyond what is necessary for the execution of the user's access request and for the security and maintenance of the data infrastructure. The data holder (or the trade secret holder if different) shall identify the data protected as trade secrets, including in the relevant metadata.

The data holder (or the trade secret holder if different) shall also agree with the user on technical and organisational measures necessary to **preserve the confidentiality of the shared data**, in particular in relation to third parties, such as model contractual terms, confidentiality agreements, strict access protocols, technical standards, and the application of codes of conduct. Data holders can withhold or suspend the sharing of data identified as trade secrets if no agreement with the user on the necessary measures is reached or if the user fails to implement agreed-upon measures. If these cases were to happen, the data holder must substantiate the decision and inform the user. The data holder must also notify the competent authority designated as per Article 37 that such data was withheld or data sharing suspended and identify which measures have not been agreed or implemented, and when relevant, which trade secrets have had their confidentiality undermined.

If the user is not the data subject whose personal data is requested, any personal data generated by the use of a connected product or related service must be made available by the data holder to the user only where there is a valid legal basis for processing under Article 6 and 9 of the GDPR and of Article 5(3) of the ePrivacy Directive.² Data holders cannot use the generated data to derive insights about the economic situation, assets, and production methods of, or the use by, the user in any other manner that could undermine the commercial position of that user in the markets in which the user is active.

Data holders must not make available non-personal product data to third parties for commercial or non-commercial purposes other than the fulfilment of their contract with the user.

Obligations for users

Users are prohibited from using the data from the data holder to develop a connected product competing with the product the data is originating from, nor are they allowed to coercively access the data by exploiting gaps in the technical infrastructure.

3.3 Right of the user to share data with third parties (Article 5)

² Regulation (EU) 2016/679 and Directive 2002/58/EC

Data holders must make readily available data and relevant metadata accessible to third parties upon a user's request, or a party acting on their behalf. This data must be provided without undue delay, in the same quality as available to the data holder, easily, securely, free of charge to the user, and in a comprehensive, structured, commonly used, machine-readable format. Where technically feasible, it should also be continuous and real-time.

3.4 Scope of data sharing obligations (Article 7)

The data sharing obligations outlined in Chapter II generally do not apply to data generated from connected products manufactured and designed or related services provided by a microenterprise or a small enterprise, under the conditions specified in the legislation. This also applies for a limited time to newly medium-sized enterprises.

4. Chapter III – Obligations of Data Holders Under Union Law

4.1 Conditions under which data holders make data available to data recipients (Article 8)

When a data holder has an obligation to share data under the Data Act or other relevant Union or national law, they must agree on the arrangements for making the data available to the data recipient. This agreement must adhere to principles of fairness, reasonableness, and non-discrimination. The data holder is explicitly prohibited from discriminating between comparable categories of data recipients regarding these arrangements. If a data recipient believes the conditions are discriminatory, the data holder must, upon a reasoned request, provide information demonstrating that no discrimination occurred.

A data holder cannot make data available to a data recipient on an exclusive basis unless the user of the connected product or related service specifically requests it. The scope of information provided for compliance verification is limited to what is strictly necessary for fulfilling contractual terms or obligations under the Data Act or other applicable law. Unless otherwise provided by Union or national law, the obligation to make data available does not extend to the disclosure of trade secrets, although specific measures can be agreed upon to preserve their confidentiality.

4.2 Compensation for making data available (Article 9)

Compensation for B2B data sharing shall be non-discriminatory and reasonable, potentially including a margin. Compensation must account for the data holder's costs in making the data available, investments in data collection/production, and potentially the data's volume, format, and nature. For SMEs and not-for-profit research organisations, compensation is limited to direct costs (formatting, dissemination, storage). The European Commission will issue compensation calculation guidelines. The article permits other laws to waive or lower compensation and requires data holders to provide transparent compensation breakdowns. However, compensation may not be claimed if it is the result of an unreasonable product limitation in functionality.

4.3 Dispute settlement (Article 10)

Article 10 grants users, data holders, and data recipients access to certified dispute settlement bodies to resolve disagreements related to data access, fair and non-discriminatory terms, and compensation. Fees for dispute resolution must be transparent. If the dispute body rules in favour of the user or data recipient in certain cases, the data holder bears all fees and reimburses the claimant. However, if the data holder wins, the user or recipient is not required to reimburse fees unless the body finds the claim to be abusive.

Member States must notify the Commission of certified bodies, which the Commission will then publish. A dispute body will refuse to handle cases already before another body or court. Parties must have a reasonable opportunity to present their views, receive submissions from the other party, and comment. Decisions, which are binding only with explicit prior consent, must be made within 90 days, in writing with reasons. Annual activity reports detailing dispute outcomes, resolution times, and common reasons for disputes are also required.

4.4 Technical protection measures on the unauthorised use or disclosure of data (Article 11)

Data holders are permitted to use appropriate Technical Protection Measures (TPMs), including smart contracts and encryption, to prevent unauthorised data access and ensure compliance with the Data Act's sharing obligations (Articles 4, 5, 6, 8, and 9) and contractual terms. However, these TPMs must not discriminate between data recipients or hinder a user's right to access, retrieve, use, or share their data with third parties as per Article 5 or other Union or national law. Users, third parties, and data recipients are generally prohibited from altering or removing these TPMs without the data holder's agreement.

5. Chapter IV: Unfair Contractual related to data access and use between enterprises

5.1 Unfair contractual terms unilaterally imposed on another enterprise (Article 13)

Contractual terms related to data access, use, liability, or remedies that are unfairly and unilaterally imposed by one enterprise on another are prohibited. A term is unfair if it significantly deviates from good commercial practice and good faith, especially if it limits liability for gross negligence, grants exclusive determination rights, inappropriately restricts remedies, unduly limits data use, allows termination on unreasonably short notice, or enables substantial price/condition changes without justification. The party imposing the term bears the burden of proving it was not unilateral.

Presumed unfair term	Description
Inappropriate limitation or extension of liability	Limits remedies for non-performance or extends liability of the party upon whom the term is imposed.
Detrimental data access and use	Allows the imposing party to use the other party's data in a way that harms their legitimate interests (e.g., trade secrets).
Restriction on data use	Prevents the imposed party from using, accessing, or exploiting their own data during the contract.
Restriction on contract termination	Prevents the imposed party from terminating the agreement within a reasonable period.
Restriction on obtaining a data copy	Prevents the imposed party from obtaining a copy of their data during or after the contract.
Unreasonably short notice for termination	Allows the imposing party to terminate the contract at unreasonably short notice, except for serious grounds.
Unilateral change of contract terms	Allows the imposing party to substantially change the price or other key terms without a valid reason or termination right for the other party.

6. Chapter V: Making Data Available to Public Sector and EU Bodies in Exceptional Cases

6.1 Obligation to make data available on the basis of an exceptional need (Article 14)

Data holders must make data available to public sector bodies, the European Commission, the European Central Bank, or other Union bodies when an "exceptional need" is demonstrated to carry out their statutory duties in the public interest. This obligation is activated only when specific conditions of exceptional need, as defined in Article 15, are met.

6.2 Exceptional need to use data (Article 15)

Article 15 details what constitutes an "exceptional need" for data, which must be limited in time and scope. It includes two primary scenarios:

Public emergency	Data is necessary to respond to a public emergency, and the public body cannot obtain it in a timely and effective manner by alternative means.
Other public interest tasks (non-personal data only)	For non-personal data, if a public body, acting under union or national law, identifies specific data whose absence prevents it from fulfilling a specific public interest task, and it has exhausted all other means to obtain the data (including market purchase or existing obligations), or if new legislation cannot ensure timely availability, or if obtaining data via this procedure substantially reduces administrative burden. This second scenario does not apply to microenterprises and small enterprises , under the conditions specified in the legislation.

6.3 Obligations of data holders when complying with requests for data (Article 18)

Under Chapter V, data holders must ensure data is made available without undue delay, in a secure manner, of the required quality, and in a format that allows for interoperability, with metadata for interpretation. They must implement measures to protect trade secrets and specify those in the request. If the data holder is a micro or small enterprise, their data sharing obligations are limited to direct costs for data processing services.

Data holders are obligated to make data readily available and accessible, and they must respond within specific timeframes (5 working days for emergencies, 15 working days for others), with a reasoned refusal if the data is unavailable or the request does not meet conditions.

6.4 Compensation in cases of an exceptional need (Article 20)

Data holders are generally entitled to compensation for making data available under an exceptional need. However, for requests related to responding to a public emergency, the data is to be made available free of charge. For other exceptional needs, compensation should cover the costs incurred in making the data available and may include a reasonable margin. The public sector body must explain the compensation basis.

7. Chapter VI: Switching Between Data Services

This Chapter details requirements for “providers of data processing services” to make it easier and faster for customers to switch services, promoting competition and user control over their data. Manufacturers in the lighting industry, if they produce smart or connected lamps, luminaires, and components, might fall under the categories of “manufacturers of connected products” and “data holders”. They might be subject to obligations regarding the access, use, and sharing of the data generated by their products.,

In line with the [EU Commission FAQ](#), we interpret data processing services as cloud providers’ services. Except in exceptional circumstances, lighting companies are not providers of data processing services, only providers of related services, and are thus not subject to enabling switching or interoperability between data processing services.

7.1 Removing obstacles to effective switching (Article 23)

Providers of data processing services must take measures (Articles 25, 26, 27, 29 and 30) to remove commercial, technical, contractual, and organisational obstacles that hinder customers from:

7.2 Contractual terms concerning switching (Article 25)

Providers of data processing services must include specific contractual terms related to switching in their contracts with customers. These terms should clearly outline:

The process for switching	The maximum notice period for termination (e.g., maximum 30 days)
Any charges for switching (which are being phased out; see article 29)	A minimum transition period after termination (e.g., at least 30 days) during which customers can access, retrieve, and transfer their data
Any charges for switching (which are being phased out; see article 29)	

7.3 Gradual withdrawal of switching charges (Article 29)

From 12 January 2027, providers of data processing services shall not impose any charges on the customer for the operations necessary to facilitate switching or to charge for data transit.

As a transitional measure until 12 January 2027, providers may only charge for costs directly incurred in relation to the switching process and data egress, and these charges must be reasonable and cost-based.

Requirements: Providers must clearly inform customers about their switching capabilities and any associated charges (during the transitional period) in an accessible format (e.g., on their website or in their terms of service) before a contract is concluded.

7.4 Technical aspects of switching (Article 30)

This article delves into technical specifics, requiring data service providers to:

- Provide open interfaces and tools to facilitate data export in commonly used and machine-readable formats.
- Ensure the continued functionality and performance of services during and after switching to compare functionalities.
- Cooperate to ensure effective and timely data migration.

[**Chapter VII** establishes safeguards against unlawful governmental access to and transfer of non-personal data held within the European Union by third-country (non-EU) governments. These Articles are mostly **for providers of data processing services** (e.g. cloud and edge computing providers).]

[**Chapter VIII** focuses on interoperability, aiming to ensure that data can flow within and between different data environments, particularly within common European data spaces, and to facilitate the development and reliable use of smart contracts.]

8. Chapter IX: Implementation & Enforcement

8.1 Competent authorities and data coordinators (Article 37)

Each Member State is required to designate one or more competent authorities responsible for monitoring and enforcing the Data Act. If more than one authority is designated, a "data coordinator" must be appointed to act as a single point of contact at the national level, facilitating communication and coordination.

8.2 Penalties (Article 40)

Member States are obliged to establish rules on penalties for infringements of the Data Act, ensuring they are effective, proportionate, and dissuasive. They must notify the Commission of these rules. The article also provides a non-exhaustive list of criteria for imposing penalties, such as the nature and gravity of the infringement, mitigating actions, previous infringements, and financial benefits gained. For certain infringements (Chapters II, III, and V), supervisory authorities (like data protection authorities) can impose administrative fines.

8.3 Model contractual terms and standard contractual clauses (Article 41)

The European Commission is tasked with developing and recommending non-binding model contractual terms for data access and use, including provisions on reasonable compensation and the protection of trade secrets. Additionally, it will develop non-binding standard contractual clauses specifically for cloud computing contracts to assist parties in drafting fair and balanced agreements. These aim to promote good practice and facilitate agreement, especially for SMEs.

8.4 Role of the European Data Innovation Board (EDIB) (Article 42)

This article establishes the European Data Innovation Board (EDIB). The EDIB's role is to advise and assist the Commission in the consistent application of the Data Act. This includes providing expertise on matters such as the calculation of reasonable compensation for data sharing (as referred to in Article 9) and generally supporting the development of a coherent approach to data governance and innovation across the EU.