

#7 Decoding the Data Act

This is the seventh entry in the #Decoding the Data Act series. This time, we present the rights and obligations of data users under the Act.

For clarity, a user within the meaning of the Act is a natural or legal person who owns a connected product, or who has been granted a temporary right to use it based on a contract (e.g. based on a hire or lease agreement), or who uses a related service.

USER RIGHTS

Right of access to Data and the right to share it with third parties

Under the Act, a user has the right to direct, **free**, and secure access to Data generated by the connected product and related services. This Data should be made available in a structured, commonly used, and machine-readable format, together with the metadata necessary for its interpretation (Article 4(1) of the Act).

Thus, the Act does not allow charging for the Data generated by the connected product itself, but the Act also **does not prevent charging for additional services provided by the data holder**. Such additional services may include: additional technical support in making the Data available, preparing the Data in non-standard formats that go beyond the requirements of a structured, commonly used, and machine-readable format; providing detailed analyses or reports based on the Data, or providing increased frequency of access to the Data beyond standard requirements and integration services with the user's systems.

In the case of historical data, i.e. data generated by a communicated product before the entry into force of the Data Act, the data holder is NOT obliged to make it available. The Act applies the principle of prospective effect and explicitly limits its application to communicated products placed on the market after 12 September 2025.

In addition, the user may designate a third party (e.g. a service provider or leasing company) to whom the data holder is obliged to disclose the Data at the user's request (Article 5(1) of the Act). In this case, the disclosure of the Data may involve a fee payable by the third party to the data holder (while remaining free of charge for the user). The Data should be made available to the third party where appropriate and, if technically possible, on a continuous and real-time basis.



PLEASE NOTE! The third party cannot be an undertaking designated as a gatekeeper within the meaning of the Digital Markets Regulation (Article 5(3) of the Act).

Detailed information on the sharing of Data under the Act can be found in [#4 in the series](#), [Decoding the Data Act](#).

Right to information

Before purchasing a product or service, the seller should provide the user with clear and understandable information about the type of Data, the manner in which it is shared, the format, the frequency of access and the conditions of use (Article 3 of the Act).

Details regarding the data holder's information obligation towards the user are discussed in [#2 in the series](#).



Right to decide on the manner of the use of Data by the data holder

The user has the right to decide whether the data holder will be able to use the Data, and if so, to what extent. Without the user's consent, the data holder will not be able to use the Data for other purposes. For more information on consent and examples of how the Data may be used by the data holder, see [#2 in the series](#).

The right to decide to whom the data holder may transfer the Data

The user has the right to decide whether the data holder will be able to share the Data with other entities, and if so, which ones. Without the user's consent, the data holder will only be able to share the Data with third parties for purposes related to the performance of the contract with the user (e.g. when using a cloud service provider where the Data is stored, or an application is made available as part of a related service). We discussed the issue of consent to share Data with third parties in detail in [#2 of the series](#).

Right to lodge a complaint and dispute resolution

In the event of a refusal to grant access to Data, or a breach of the provisions, the user may lodge a complaint with the competent authority or use the dispute resolution procedure (Articles 10 and 38 of the Act). The complaint should be lodged with the competent authority or the data coordinator, if one has been appointed. That authority is required to examine the complaint, conduct an investigation, and inform the complainant of the progress and outcome of the case (Article 38 of the Act). The user also has the right to an effective judicial remedy in the event of a decision by the authority or a failure to act (Article 39 of the Act).

Breaches of the obligations laid down in the Act are subject to penalties – Member States are required to establish effective, proportionate, and dissuasive penalties, which may include fines, warnings, reprimands, or orders to adjust business practices. When determining the amount of the penalty, factors such as the nature, gravity, and duration of the breach, corrective measures and previous breaches are taken into account (Article 40 of the Act).

In August, a draft bill implementing the Data Act appeared on the Council of Ministers' list of legislative and programme work – the draft bill on Fair Access to and Use of Data. The planned date for the adoption of the draft by the Council of Ministers is the fourth quarter of 2025. The function of the competent national authority is to be performed by the President of the Office of Electronic Communications, but at this stage, there is no information about penalties.

The right to personal data protection of personal data contained in Data

Personal data generated as a result of using a connected product or related service is only made available if there is a legal basis for its disclosure under Articles 6 and 9 of the GDPR. We wrote more about the disclosure of personal data in [#2 in the series](#).

The right to choose optional clauses resulting from model Data sharing agreements

The user may, among other things,:

- (i) choose the method of accessing the Data, e.g. through Data transmission or through access to Data at the place where it is stored;
- (ii) agree to restrict their right to use or share the Data, e.g. in exchange for additional remuneration and if this is not disadvantageous to them;
- (iii) choose the option regarding the entry into force of the agreement (immediately or from a specified date) and the duration of the agreement (an undefined or defined term); or
- (iv) the applicable law.

USER OBLIGATIONS

Prohibition on the use of Data for competitive purposes

The Act introduces:

- a prohibition on the use of the obtained Data to develop a competitive product related to the product from which the Data originates, and
- a prohibition on making this Data available to third parties for this purpose and on using the Data to obtain information about the economic situation, assets, and production methods of the manufacturer or data holder (Article 4(10) and Article 6(2)(e) of the Act).

However, this prohibition does not apply to the creation of competing related services.

Prohibition on the abuse of technical infrastructure

Another restriction is the prohibition on the use of coercive measures and the abuse of loopholes in the data holder's technical infrastructure, which are designed to protect the Data, to gain access to it (Article 4(11) of the Act).

Obligation to protect trade secrets

The user is obliged to implement agreed technical and organisational measures to protect the data holder's trade secrets. If these measures are not implemented, the data holder may suspend or terminate the provision of Data (Article 4(6)-(8) and Article 5(9)-(11) of the Act).

Details regarding the protection of trade secrets are discussed in [#6 of this series](#).



Obligation to protect personal data

If the user is not the data subject, the data holder may disclose data containing personal data only based on a valid legal basis under Articles 6 or 9 of the GDPR and, where applicable, under Article 5(3) of Directive 2002/58/EC. This means that the data holder must verify the legal basis each time when disclosing the personal data of a person other than the user.

You already know who the user is and what their rights and obligations are. In the next post in the [Decoding the Data Act](#) series, you will learn more about the data recipient. Stay tuned!

Feel free to contact us!



Agata Szeliga

Partner, attorney-at-law

☎ +48 698 660 648

✉ agata.szeliga@skslegal.pl



Agnieszka Jurcewicz-Androsz

Associate, attorney-at-law

☎ +48 600 782 823

✉ agnieszka.jurcewicz-androsz@skslegal.pl



Warsaw

Jasna 26, 00-054 Warsaw

T +48 22 608 70 00

F +48 22 608 70 70

E office@skslegal.pl

Katowice

Korfantego 138a, 40-156 Katowice

T +48 32 731 59 86

F +48 32 731 59 90

E office.katowice@skslegal.pl

Poznań

Mickiewicza 35, 60-837 Poznań

T +48 61 856 04 20

F +48 61 856 05 67

E office.poznan@skslegal.pl