

#5 Decoding the Data Act

This is the fifth post in the Decoding the Data Act series.

In this edition, we discuss the content of the data sharing agreements.

Are there any guidelines regarding the Data Sharing Agreement?

Based on Article 41 of the Data Act, the Expert Group at the EC has developed [model contractual clauses for mandatory and voluntary access to Data](#). The model contractual clauses for mandatory data sharing cover the following scenarios:

- an agreement between the data holder and the user,
- an agreement between the data holder and the recipient,
- an agreement between the user and the recipient of the data.

Below, we present the provisions of the agreement between the **data holder and the user** to which particular attention should be paid:

- Provisions regarding the possibility of use of the Data by the data holder.

Details should be specified regarding the manner in which the data holder may use non-personal Data (see our second post in the series [\[link\]](#), where we have indicated in detail how to describe the possibility of use of the Data by the data holder). Without specifying such a possibility, the data holder will not be able to use the Data otherwise than on the basis of the agreement with the user.

- Provisions regarding the disclosure of Data to third parties.

It is important to address the possibility or lack thereof of disclosing Data to third parties (e.g. other companies within the group). Such possibility always requires the user's consent. Return to our second post [\[link\]](#), where we answered what such consent should look like and what conditions it must meet. If consent is not obtained, the data holder will not be able to disclose the Data to other entities for purposes other than the performance of the agreement with the user.

- Provisions regarding the grounds for sharing personal data.

It is necessary to verify whether personal data will also be shared within the Data. If so, it is necessary to verify whether there are valid legal grounds for such sharing under the GDPR. See our comments on the data holder's obligations in relation to the sharing of personal data in the second post [\[link\]](#) in the #Decoding the Data Act series.

- Provisions on the protection of trade secrets.

If the disclosure of the data holder's trade secrets is to occur in connection with the disclosure of Data, the data holder has the right to protect such secrets.

The holder should indicate which Data is confidential (this will be data that has economic value and that the data holder takes measures to keep it confidential) and require the user and third parties to keep it confidential by expressing their consent and implementing the necessary security measures. You can read more about trade secret protection in our next post in the #Decoding the Data Act series.

- Provisions concerning changes of user or multiple user scenarios.

The data holder should regulate in the agreement what happens if the users changes, including the obligation to notify the holder about such changes, liability, and rules of access to data in the event of a change of user (e.g., as a result of sale or destruction of a product) or access of several users to one product (e.g., in the case of rented cars). If this issue is omitted, a new / different user may have access to the previous user's data / different user's data.

- Provisions concerning technical means of data transfer.

The agreement should specify the technical means of data transfer. The Act indicates, among other things, that Data should be made available to the user in an easily accessible, secure, structured, commonly used and machine-readable format. Detailed provisions on technical issues related to Data transfer may be included in an annex.

- Provisions on liability.

The agreement should regulate the liability of the parties for non-performance or improper performance of the agreement, including the possibility of claiming damages, requesting the removal of Data used in breach of the agreement, and the possibility of suspending the provision of Data in the event of a serious breach of obligations by the user. It is also worth agreeing the rules on support if there are problems with the Data quality or transfer of Data.

- Provisions regarding termination.

It is necessary to regulate issues related to the possibility of terminating the agreement, including in the event of product destruction, loss of the user's status, or by mutual agreement of the parties. However, a change of user will not always lead to the termination of the agreement.

It is also worth regulating in the agreement the possibility of using the data after its expiry.



Optional: in the agreement between the data holder and the user, the parties may agree whether the user will be entitled to remuneration for the use and disclosure of the Data by the data holder, if this would be fair and justified from their perspective:

- such a situation could arise, for example, if the data holder used the Data to develop new products or services in a way beyond standard use, or if it created aggregated data for commercial exploitation, or if the user consented to the sale of the Data to third parties;
- we are unlikely to encounter such a situation where the Data is used solely for the purposes of an agreement concluded with the user or to ensure the functionality, security and protection of the product or related service.



Reverse engineering – permitted or prohibited?

Definitely prohibited by the provisions of the Act with respect to connected products. The user or a third party may not use the obtained Data to develop a product that competes with the connected product from which the data originates. Furthermore, it is prohibited to share this Data with a third party for these purposes. This restriction does not apply to related services.

It is also generally prohibited to use the Data to obtain information about the economic situation, assets and production methods of the manufacturer and, where applicable, the data holder.

In the next post in the [Decoding the Data Act](#) series, you will learn how you can protect your trade secrets. 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 Warszawa

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