

EU Digital Laws: Mapping the Interplays with the GDPR

Data Act: EU General Data Protection Regulation

The Data Act, which seeks to reduce the legal and technical barriers to reusing privately held corporate data to the benefit of consumers and competition, naturally intersects with the EU General Data Protection Regulation requirements for protecting personal data. Namely, the Data Act's rules — designed to promote data sharing, data portability, interoperability and data subject access rights — require careful consideration of their interplays with the GDPR's existing protections for personal data.

Data Act

Article 1(5)

Insofar as any personal data or datasets containing both personal and non-personal data that are inextricably linked are processed in connection with the Data Act, the GDPR's rules and protections prevail. In the event of a conflict between the Data Act and GDPR, the latter prevails.

Article 4(12) and 5(8)

Personal data generated by the use of a connected product or related service may only be requested by a controller or a data subject. Data holders may set reasonable compensation to be met by third parties, but not by users, for costs incurred in providing direct access to the data generated by the user's connected product.

Recital 20

The Data Act does not impose an obligation to design connected products and related services in such a way as to store or process any personal data other than what is necessary in relation to the purpose limitation principle.

Recital 39

Third parties should erase personal data once it is no longer necessary for the purpose agreed upon with the user.

Recital 24

Data holders are not expected to indefinitely store data for users of connected products.

Recital 22

Controllers may task processors with making certain data available from on-device data storage or from a remote server to which data are communicated. Where the data holder and user qualify as joint controllers within the meaning of GDPR Article 26, they must transparently determine their respective responsibilities and agree on how these will be arranged under the GDPR. Such users may subsequently become a data holder under the Data Act and become subject to its obligations to make data available.

Article 6

Third parties shall only process data they receive under Article 5 of the Data Act for the purposes and under the conditions agreed upon with the user. Third parties are prohibited from using the data they receive for profiling except when it is necessary to provide a service requested by the user.

Article 17

Data requests from public sector bodies — e.g., the European Commission, European Central Bank or EU bodies — to data holders should be specific, transparent and proportionate in their scope of content and granularity.

Under the GDPR, the public sector body should notify the supervisory authority in the member state where the public sector body is established.

Article 37, 38 and 40

Insofar as personal data is concerned, the supervisory authorities responsible for monitoring the application of the GDPR are also responsible for monitoring the application of the Data Act.

GDPR

Article 2 and 4

Insofar as a Data Act user, i.e., a "natural or legal person that owns a connected product ... or that receives related services," is a GDPR data subject, the rights under the Data Act complement those of the GDPR.

Articles 6(1), 9, 15 and 79

Controllers who request personal data generated by the use of a connected product or related service must have a legal basis for processing the data under the GDPR.

If a data holder and a third party cannot agree on the terms of direct access, the data subject's rights under the GDPR, e.g., the right to data portability, must not be impeded, and the data subject may seek remedies in accordance with the GDPR.

Article 5(1)(c)

Under the GDPR, the processing of personal data should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed."

Article 17

Requirements under the Data Act for third parties to erase personal data once it is no longer required for the purpose agreed upon with the user complement the data subject's right to erasure under the GDPR.

Article 5(1)(e)

Data holders should implement a reasonable data retention policy in line with the GDPR's storage limitation principle.

Articles 4(7-8), 6(1)(a-b), 9(2)(a), 20 and 26

Processors are not considered to be data holders but may be tasked by controllers to make certain data available. Failure to agree on arrangements for transmitting data by a data holder and third party shall not hinder the right to data portability under the GDPR.

Article 22(2)(a-c)

The Data Act's prohibition on third-party use of data for profiling applies notwithstanding the GDPR's exceptions for profiling based on consent or the performance of a contract.

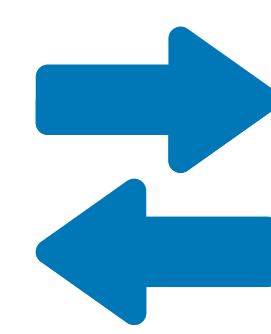
Articles 3, 6(1) and 51-59

Upon being notified of such a request, the competent authority under the GDPR may advise the public sector body to cooperate with the public sector bodies of the member state in which the data holder is established on the need to minimize the administrative burden on the data holder and/or may reject the request.

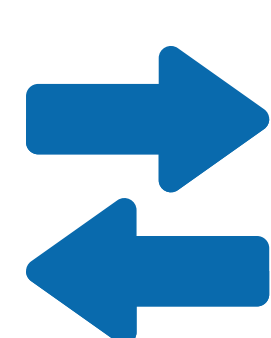
Articles 51-59 and 83

The GDPR's rules on the independence and cooperation of the supervisory authorities apply to the Data Act mutatis mutandis, i.e., "with things changed that should be changed."

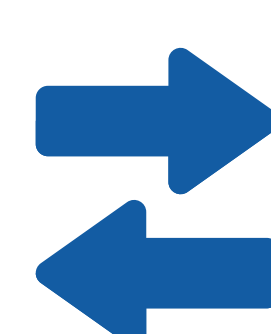
Precedence of the GDPR



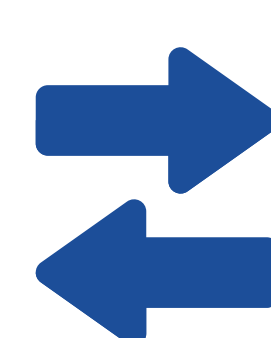
Access to personal data



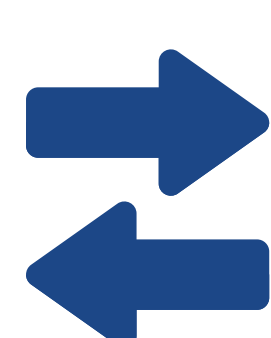
Data minimization



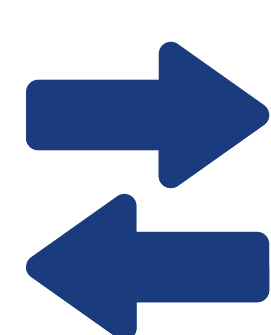
Right of erasure



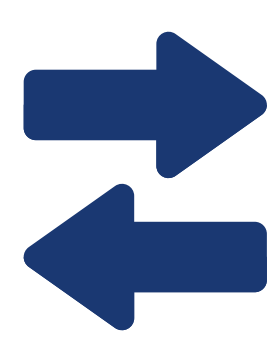
Data retention



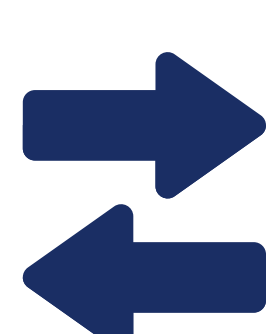
Responsibilities of controllers and processors



Prohibition on third parties' use of data for profiling



Data requests from public sector bodies/ notification of the GDPR supervisory authorities



Role of the GDPR supervisory authorities and penalties

