

Information on the SmartDialog service under the EU Data Act

This guidance applies to the use of the SmartDialog platform to the extent that the obligations concerning data processing services under the Data Act apply to the SmartDialog service. It explains how to retrieve data from Arena Interactive's SmartDialog when transferring data to another data processing service or to your own ICT infrastructure. This page supplements the agreement, service descriptions and General Terms.

1. Transferable Data and digital assets

Transferable Data comprises contact details held in active group services (telephone numbers, email addresses and other contact details entered into the system), as well as sent and received messages for the retention period specified for the Customer's data (up to 365 days). Dedicated short codes owned by the Customer are transferable. Such dedicated numbers may be used in two-way messaging services.

Transferable Data does not include encrypted messages, messages whose retention period has expired, categories of data relating to the internal operation of the services, access logs, system or security logs, system configurations, settings or digital assets. These exclusions are based on service security, integrity, data protection and intellectual property rights.

2. Procedures for switching services and transferring data

The Customer may switch to another data processing service or transfer data to its own ICT infrastructure by contacting Arena Interactive's customer service at support@arenainteractive.fi and notifying Arena Interactive of the switch and its schedule. The Customer can retrieve data from SmartDialog or via the API.

3. Available support and assistance

Arena Interactive's customer service provides guidance on retrieving data where necessary. If separately agreed, Arena Interactive may provide the Customer with the required data.

4. Data transfer formats and technical interfaces

Message logs exported from the SmartDialog system are provided in a structured, commonly used and machine-readable format (CSV or Excel export). Where APIs can be used for the Data Transfer, the data format is generally JSON. The Customer can retrieve message log data and contact details directly from SmartDialog.

The APIs for retrieving contacts and message logs are described in the Group Management and Message Traffic sections of Arena Interactive's OpenAPI documentation. The current documentation is available at <https://openapi.arena.fi/>.

5. Transition and retrieval periods and data deletion after the transition

The Notice Period, Transition Period and Retrieval Period applicable to switching services, as well as the terms governing the deletion of Transferable Data, are set out in

Arena Interactive's General Terms. The Customer may contact Arena Interactive at support@arenainteractive.fi with any questions concerning the Transition Period.

6. Limitations and exceptions

Message log data cannot be transferred if the Customer uses encrypted message content. Operator-provided long codes ordered for the Customer and shared short codes are not transferable. These may be used in two-way messaging services.

Some data (for example, data that is not available through self-service export) may require a request to our customer service at support@arenainteractive.fi.

7. Jurisdiction applicable to the ICT infrastructure

The SmartDialog service is provided in the Microsoft Azure environment. The ICT infrastructure used for data processing in the service is located in the Microsoft Azure North Europe region in Ireland and is subject to Irish jurisdiction.

8. Access to data by third-country authorities

Arena Interactive uses technical, organisational and contractual safeguards to prevent access by third-country authorities to non-personal data held in the EU, or transfers of such data, where such access or transfer would conflict with EU law or applicable national legislation.

The technical safeguards for the SmartDialog service include, for example, storing data within the EU/EEA, encryption in transit and at rest, controlled management of keys and secrets, segregation of customers and environments, multi-factor authentication, role-based access control, logging and technical monitoring. Organisational governance is based on identifying data assets, data classification, risk management, prior assessment of suppliers, and assessment of the impacts of changes and international service chains. Contractual requirements ensure that personnel and parties in the service and subcontracting chains are subject to confidentiality, information security and notification obligations, that access is restricted, that audit and reporting rights are in place, and that data is returned, transferred and deleted when the service relationship ends.

The SmartDialog service is provided in the Microsoft Azure environment. Under the applicable contractual terms, Microsoft does not disclose processed data to law enforcement authorities or provide access to such data unless required by law. If a law enforcement authority requests processed data from Microsoft, Microsoft directs the authority to request the data directly from the customer. If Microsoft is compelled to disclose processed data to a law enforcement authority or provide access to such data, Microsoft promptly notifies the customer and provides the customer with a copy of the request for disclosure, unless prohibited by law. Microsoft does not provide any third party with direct, indirect, unrestricted or unsupervised access to processed data or with the platform encryption keys used to encrypt processed data.