

# Data Portability

Information required by Regulation (EU) 2023/2854 of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act) concerning the data processing service of Netvisor KYC.

---

## Exportable and Non-exportable Data

Section (a) all categories of exportable data and digital assets that can be transferred during the switching process in accordance with Data Act and section (b) all categories of data specific to the functioning of the Service that are exempted from the previous list.

### a) Exportable data:

- **Basic customer register data:** Includes information from the customer list such as Business ID, customer name, company form, industry classification, account manager, creation date, and postal address.
- **Customer KYC / risk management data:** Includes customer-specific information such as basis for identifying beneficial owners, assessed risk level, risk indicators, next review date, approval date, approver, and current status.
- **Sanctions list screening data:** Includes details of conducted sanctions screenings, their dates, and summary results (e.g., number of matches).
- **Contact person data:** Includes the customer's contact persons' names, job titles or authorizations, contact information (phone/email), and information on the identification method, verified name, and sanctions screening status.
- **Continuous monitoring activities:** Includes a list of actions or activities performed as part of the customer's ongoing monitoring process.
- **Administrative data on data requests:** Includes information on submitted data requests, their submission dates, and current statuses.

### b) Non-exportable data:

- **Internal system log data:** Technical logs related to the operation, maintenance, and troubleshooting of the service.
- **Service settings and configurations:** General system-level settings that are not customer-specific.

- **Data request evaluation guidance questions:** Questions defined by the service provider to guide and support the customer in evaluating and responding to data requests, constituting the provider's intellectual property.
- **Customer responses to guidance questions:** Customer-provided answers forming part of the provider's internal evaluation process.
- Internal algorithms and risk calculation models: Methods and machine learning models used by the system to calculate or suggest risk levels.

## **Known restrictions and technical limitations for exports of data**

Basic customer register data can be exported in a machine-readable Excel format.

More detailed customer-specific data, such as contact person listings and continuous monitoring activities, can be exported as customer-specific PDF reports. The PDF format is not machine-readable, which may affect the portability and reusability of the data.

## **How Data is exported**

The customer can primarily and independently export the transferable data directly from the Netvisor KYC system.

The data will be provided in Excel and/or PDF format. Customer register data (such as the customer list) can be exported in a machine-readable Excel format. More detailed customer-specific information, such as contact person listings and event history, can be exported as customer-specific PDF reports.

Support can be contacted via the chat in the Netvisor KYC portal or by email at [tuki.kyc@visma.com](mailto:tuki.kyc@visma.com)

## **Subcontractors**

Up-to-date information on our subcontractors and their locations is available in the Visma Trust Centre.

## **Interfaces**

We provide [online documentation](#) for our service's APIs, which enables customers to use the service in conjunction with other cloud services they use

## **Disclosure of Data to Authorities**

The police and other authorities may request access to information from us. This can include both personal and non-personal data.

In all such cases, we follow strict internal policies and procedures for assessing the access request, and confer with legal counsels. We only share information that is strictly required by law, and we only share information on the basis of valid court orders or similar legal documents.

To prevent unauthorised access to any information we hold, we also implement technical measures such as encryption and access controls. The Visma Security Program ensures high security standards and confidentiality.

Furthermore, we ensure legal obligations in contracts with our subcontractors that ensure they too enact organisational and security measures similar to ours.

If we receive access requests from non-EEA authorities, we ensure our compliance with the Data Act article 32. Internal policies and routines are in compliance with this regulation.