INFORMATION ON DATA EXPORT OPTIONS AND THE SWITCHING PROCESS (DATA ACT)

This page provides the information required under Regulation (EU) 2023/2854 of the European Parliament and of the Council on harmonised rules on fair access to and use of data (the "**Data Act**") regarding:

a) a detailed specification of all categories of data and digital assets transferable during the switching procedure, including at least all exportable data;

b) a comprehensive specification of categories of data specific to the internal functioning of the service, which are excluded from exportable data under letter (a) of this section,

c) information on available procedures for switching data processing service providers and data transfer, including available switching methods, transfer formats, and technical and other limitations known to Power Nodes;

d) the data structures and data formats, as well as the relevant standards and open interoperability specifications, in which the exportable data referred to in Article 25(2)(e) of the Data Act are available,

e) information on the jurisdiction governing the information and communication technology infrastructure used for data processing for the respective services,

f) a general description of technical, organisational and contractual measures adopted by Power Nodes to prevent international access by public authorities to non-personal data stored in the European Union or their transfer, where such access or transfer could conflict with European Union or national law of the relevant Member State.

The rights described on this page apply if and to the extent that the Service is provided as a data processing service within the meaning of the Data Act. To the extent that the provision of the Service does not meet the definition of a data processing service under the Data Act, these rights do not arise for the Customer.

1. AVAILABLE METHODS FOR SWITCHING TO ANOTHER PROVIDER OF DATA PROCESING SERVICES AND DATA TRANSFER

You may switch to another provider of data processing services or migrate to their own on-premises infrastructure. For this purpose, the following methods are available:

- **Self-service data export via the application**
  Customer may export selected data directly from the user interface using built-in export functions (export to Excel).

- **Export via API**
  Customers may use the API interface.

- **Assisted export and migration support**
  Upon request, Power Nodes may provide assistance with migration to the extent described in this document.

2. TECHNICAL AND OTHER KNOWN LIMITATIONS

Although Power Nodes seek to make switching and data portability as smooth as possible, the following limitations may apply:

- **Dependencies on third-party services**

If you use integrations with third-party tools, data in those tools may be subject to their own limitations regarding export, formats or API availability. Power Nodes cannot guarantee the portability of data processed exclusively within such third-party environments.

- **Performance and capacity limits**
  High-volume or frequent bulk exports may be subject to limitations (rate limits), scheduling or batch processing in order to maintain the stability and performance of the Service for all customers.

- **Your configuration and the target environment**
  Successful import into the target environment (another provider or an on-premises system) depends on the technical capabilities, configuration and data model of that environment. Power Nodes do not control and is not responsible for limitations on the side of the target system.

CATEGORIES OF EXPORTABLE DATA AND DIGITAL ASSETS, DATA STRUCTURES AND FORMATS

3.1 Categories of exportable data and digital assets

- **Customers**
  - Your details (incl. connections to users)
  - Assigned labels
  - Your custom data fields
  - Credit movements
  - GDPR consents granted
  - Communication history
- **Users**
  - User details (excluding password)
- **Analasys**
  - Analysis results
  - Analysis intermediate

3.2 Categories of data that cannot be exported

- **Configuration of payment gateways and terminals**

  Specific parameters posing a security risk and directly tied to the system integration at the technical level.

3.3 Categories of data for which switching is very complex, costly, or for which switching is not possible without significant changes to the architecture of data, digital assets or services

- **Cloud database services**

For the smoothest possible operation of the Service, Power Nodes uses a proprietary data model and table structure developed by Power Nodes, as well as specific database functions and procedures, including an internal data format, which in this configuration exist only with Power Nodes. A transfer may therefore require, in particular, a redesign of the database schema and conversion of data into another format.

4. ICT INFRASTRUCTURE AND RELEVANT JURISDICTIONS

- Data are stored in a database in the AWS the EU (AWS – EU Central 1 - Frankfurt), including ongoing backups. These backups are also automatically stored in a redundant data center in West Europe—Frankfurt
- the relevant jurisdiction in relation to the primary cloud infrastructure is the Germany.

5. MEASURES AGAINST UNAUTHORISED INTERNATIONAL ACCESS BY PUBLIC AUTHORITIES

Power Nodes is committed to ensuring that any international access by public authorities to non-personal data stored in the EU takes place in accordance with applicable EU and Member State law. Power Nodes have implemented a combination of technical, organisational and contractual measures designed to prevent access or to challenge access requests that would conflict with EU law or national law.

Technical measures include, inter alia:

• *Logical and physical separation of environments*

Data stored in the EU are hosted in data centers in the EU and are logically separated from other environments.

• *Access control and the principle of least privilege*

Access to production systems is strictly controlled, logged and restricted to authorised persons based on their role and need-to-know.

• *Encryption*

Data are protected in transit and at rest using industry-standard encryption mechanisms, to the extent enabled by the relevant infrastructure and services used.

These measures reduce the risk that foreign public authorities obtain direct access to data via infrastructure providers without using appropriate legal channels.

Organisational and contractual measures include:

• *Contractual commitments of providers*

Power Nodes require from its cloud and infrastructure providers to comply with applicable EU law and—where permitted by law—to inform Power Nodes of any legally binding requests by public authorities for access to data. Standard Contractual Clauses (SCCs) are also agreed between Power Nodes and the infrastructure provider where relevant.

• *Internal procedures for handling requests*

If Power Nodes receive a request from a public authority outside the EU/EEA for access to data stored in the EU, Power Nodes will:

- carefully assess the legal basis for such request,
- verify whether the request is compatible with EU law and the relevant national law, and

- challenge or oppose the request if Power Nodes reasonably believes it conflicts with such laws or exceeds the requesting authority’s powers.

• *Transparency towards customers*

Unless legally prohibited, Power Nodes will inform you (if you’re affected) without undue delay of such a request and the data concerned so that you can take appropriate steps to protect your interests.