Appendix: Switching and Exit documentation

This appendix forms part of the Order Agreement for 55 Degrees' products purchased outside of the Atlassian Marketplace, such as those for use in Microsoft's Azure DevOps or for our standalone SaaS products. For equivalent documentation pertaining to our Atlassian products, please consult the 55 Degrees website.

1. General notes on exportable data

Certain data elements may be stored by the Provider in a transformed or protected format (for example, hashed or encrypted values) as part of the Provider's security measures to protect Customer data.

Where such transformations are one-way (e.g. hashing with salting), the original values cannot be reconstructed by the Provider, and such will therefore be exported in their stored and protected form. The Customer acknowledges that such data therefore may not be directly human-readable or reusable in another system, which may affect the categories of exportable data described below.

2. Exportable data per product

2.1 ActionableAgile Analytics for Azure DevOps

Exportable data

The following inputs from the Customer are stored by the Product in JSON format:

- User preferences
- Dataset configurations
- Dataset view configurations

The following outputs are generated by the Customer's use of the Product and are stored in JSON format:

- No outputs are generated and stored at this time.

Excluded categories of data and digital assets

Categories of data and digital assets specific to the internal functioning of the Product where a risk of breach of the Provider's or a third party's trade secrets exists or data relating to the integrity and security of the Product, the export of which would expose the Provider to cybersecurity vulnerabilities:

- Internal functioning of the Product and trade secrets, including but not limited to

    - Internal algorithms and calculation logic
    - Infrastructure configuration and orchestration
    - Internal schema and processing metadata
- Provider / Third-Party Data, including but not limited to
    - Azure DevOps data stored by Microsoft
    - Monitoring or observability tooling data
- Data and digital assets protected for privacy and security reasons, including but not limited to
    - Authentication tokens
    - API tokens
    - Encryption keys

2.2 ActionableAgile Analytics (Standalone SaaS)

Exportable data

The following inputs from the Customer are stored by the Product in JSON format:

- User preferences

The following outputs are generated by the Customer's use of the Product and are stored in JSON format:

- No outputs are generated and stored at this time.

Excluded categories of data and digital assets

Categories of data and digital assets specific to the internal functioning of the Product where a risk of breach of the Provider's or a third party's trade secrets exists or data relating to the integrity and security of the Product, the export of which would expose the Provider to cybersecurity vulnerabilities:

- Internal functioning of the Product and trade secrets, including but not limited to
    - Internal algorithms and calculation logic
    - Infrastructure configuration and orchestration
    - Internal schema and processing metadata
- Provider / Third-Party Data, including but not limited to
    - External work management platform data stored by host platforms
    - Monitoring or observability tooling data
- Data and digital assets protected for privacy and security reasons, including but not limited to:
    - Authentication tokens
    - API tokens
    - Encryption keys

INFORMATION ON PROCEDURES FOR SWITCHING AND PORTING

Tools/Process for switching

1. The Customer shall request a data export by creating a request via the Provider's support portal at https://support.55degrees.se and providing sufficient information to identify their subscription.
2. The Provider will retrieve the Customer's exportable data and provide the data export in the format specified in the Exit Documentation via the support request.
3. The Customer shall confirm that the data export has been received and is accessible.
4. Upon such confirmation, or where the Provider has reasonable grounds to believe that the data has been made available to the Customer for export as set out in this Appendix via the support request, the Provider will close the support request.

Estimated time for export and transfer of exportable data

The time required to export and make available the Customer's exportable data will depend on factors such as data volume, system load, and technical constraints.
Based on typical usage, data exports are generally completed within **five (5) to ten (10) business days** from receipt of a complete request. In many cases, data exports are completed sooner; however, the above timeframe allows for processing, validation, and handling of concurrent requests.
The Customer acknowledges that:

- the above estimate assumes that the Customer uses the Provider's tools and follows the provided documentation and instructions; and
- the time required by the Customer or any third party to import and implement the data in the destination environment does not affect the Provider's obligation to make the exportable data available.

Known risks to continuity in the provision of functions or services

The Customer acknowledges that during the Switching Process, the following risks to continuity may arise:

- Temporary disruption to access to the Product during data export activities
- Differences in data models, configurations, or functionality between the Product and the New Provider's environment
- Delays caused by the Customer's or a third party's preparation, configuration, or implementation activities
- Limitations in the ability of the New Provider's system to process or interpret the exported data
- Data elements stored in protected or transformed formats (e.g. hashed values), which may not be directly usable in another system

The Provider shall not be responsible for risks or disruptions arising from factors outside the Provider's control, including those related to the Customer's or any third party's systems or implementation activities.

Securing of IT resources

During the Transitional Period, the Provider shall:

- allocate reasonable internal resources to perform data export in accordance with this Exit Plan;
- maintain appropriate system availability to enable access to the Product and exportable data; and
- ensure that appropriate technical and organizational security measures are applied to protect the Customer's exportable data during the Switching Process.

For the avoidance of doubt, the Provider is not required to allocate dedicated or additional resources beyond what is reasonably necessary to fulfill its obligations under this Exit Plan.

Jurisdiction of ICT infrastructure and measures to prevent international unlawful government access

The Provider stores Customer exportable data using cloud infrastructure hosted by Amazon Web Products (AWS).

The Customer may select the geographic region in which its data is stored. Currently, the Provider offers the following regions:

- United States (US East)
- European Union (Stockholm, Sweden)
- Australia (Sydney)

Customer exportable data is stored within the selected region.

Further information about AWS infrastructure and data center locations is available at: https://aws.amazon.com/about-aws/global-infrastructure/

The Provider also utilizes third-party platforms, including Atlassian Forge, to operate and deliver the Product. Such platforms may process data as part of the operation of the Product, but do not constitute the primary storage location of the Customer's exportable data.

The Provider implements appropriate technical, organizational, and contractual measures to protect Customer data against unlawful international government access, including:

- storing exportable data within the Customer-selected region
- restricting access to Customer data based on least-privilege principles
- using encryption in transit and at rest
- using secure authentication and access controls
- entering into appropriate contractual arrangements, including data processing agreements where applicable

The Provider relies on AWS and other platform providers that maintain industry-standard security certifications and publicly commit to handling government access requests in accordance with applicable laws and established transparency and accountability practices.

Complex switches

In most cases, switching can be completed by exporting the Customer's exportable data in accordance with this Exit Plan.
However, certain switching scenarios may involve complexity or result in limitations, including but not limited to:

- differences in data models, configurations, or functionality between the Product and the New Provider's system
- reliance on third-party platforms (such as Atlassian or Microsoft Azure DevOps), where data structures and access mechanisms are defined by those platforms
- Customer-specific configurations, datasets, views, or forecasting setups that are not directly transferable to another environment
- dependencies on calculations, analytics, or visualizations (such as probabilistic forecasts or process metrics) that are specific to the Product and not reproducible in another system
- data elements stored in protected or transformed formats (e.g. hashed values) for security reasons, which are not reversible and may not be directly usable in another system

In such cases, switching may require additional effort by the Customer or the New Provider, and certain functionality, outputs, or configurations may not be fully replicable in the destination environment.
The Provider does not guarantee functional equivalence or compatibility with any third-party system. Switching is generally feasible, but may result in differences in functionality, configuration, or performance in the destination environment.