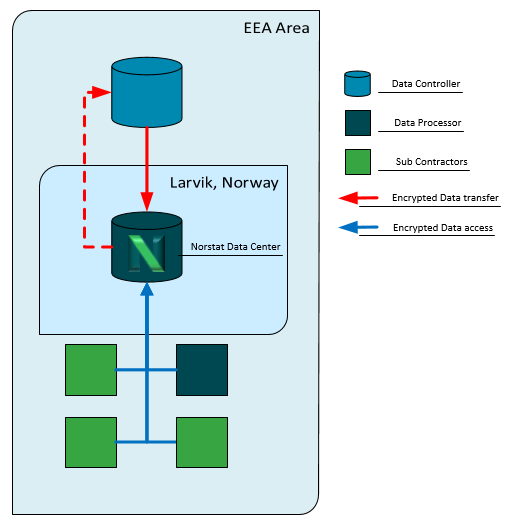
**Annex 1 –Data Flows and Data Security**

# Introduction

## This Annex 1 (Data Flows and Data Security) sets out the data flows entailed by the Data Processor’s provision of the Services and the minimum security requirements applicable to the Data Processor and its subcontractors' provision of the Services.’

# Overview



Data Controller transfer Personal Data to Data Processor’s Data Center facilities in Larvik, Norway. Norstat provide FTPS services for secure encrypted transfers. Data Processor and Sub Contractors can access data over encrypted VPN connections.

# Sub contractors

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Sub-contractor (Company name, registration no., address, contact details, including contact details of the data protection officer (if any) etc.) | Scope and purpose of processing | Categories of Personal Data | Processing (and storage) locations (eg country/state) | Transfer of or access to Personal Data by third parties | Legal basis for transfer of Personal Data (if applicable) (e.g. standard contractual clauses, safe harbour ect.) |
| Norstat Norge AS  NO982836018  MD Per Olav Ramstad | Market research data collection | Contact information, background variables | Processing:  Oslo, Larvik Storage: Larvik |  | Data processing agreement |
| Norstat Sverige AB  SE556604-6297  MD Henrik Åquist | Market research data collection | Contact information, background variables | Processing: Linkoping |  | Data processing agreement |
| Norstat Finland OY  FI15973876  MD Antti Suomela | Market research data collection | Contact information, background variables | Processing: Pori |  | Data processing agreement |
| Norstat Eesti AS  EE101186991  MD Evelin Pae | Market research data collection | Contact information, background variables | Processing:  Tallinn |  | Data processing agreement |
| Norstat Deutschland GmbH  DE245886432  MD Sebastian Sorger | Market research data collection | Contact information, background variables | Processing: Munich |  | Data processing agreement |
| Confirmit AS  NO976886240  COO Arnt Feruglio | Hosting and support for SaaS survey software. | Contact information, background variables | Storage:  Rackspace Ltd. (UK) |  | Data processing agreement |
| J&T Services, BG201007341  MD Todor Petev | Market research data collection | Contact information, background variables | Processing:  Sofia, BG |  | Data processing agreement |

# Minimum security requirements

The Data Processor shall by itself, and shall ensure that all of its subcontractors involved in the Processing of Personal Data (if any) under the Agreement at all times complies with the following minimum security requirements

## Availability

Implemented measures securing availability on critical systems:

* Hardware monitoring - enabling rapid repair.
* Performance monitoring - ensuring system efficiency and avoiding bottlenecks.
* Hardware redundancy and failover systems - reducing system downtime.
* Business Continuity Plans and systems - reducing impact of serious incidents and enabling rapid recovery.
* Firewalls or Intrusion Prevention Systems - guarding against downtime due to malicious actions such as denial-of-service (DoS) attacks and network intrusions.

## Integrity

All data is classified and handled according to Norstat’s Internal Control System. In the case of non-sensitive personal data, the following rules apply:

* Documents must only be copied for people who are authorized for that category.
* Any loss or compromise of protected documents must be reported to the security officer and the immediate line manager.
* Stored in a secure area on the file system that is only accessible to those who should have the information
* Prevent access to information from outsiders.
* Printouts must be collected from the printer immediately such that confidentiality (“need to know”) in processing the case is maintained.
* Documents/electronic media must be kept under supervision or locked away.
* Physical documents (paper) should be sent through the post in a sealed envelope
* Sent over an encrypted FTPS connection, or as an encrypted file/encrypted attachment to an email.
* The information must not be communicated in locations where conversations could be overheard by outsiders.
* Paper to be destroyed or placed in company shredders.
* Disks and equipment containing hard disks or other storage material (such as memory chips, backup tapes etc.) must be sent to the IT department to be destroyed securely.
* Data equipment should be sent to the IT department or repaired by external partners with the approval of the IT department.

## Confidentiality

Implemented measures securing confidentiality of Personal Data:

* Authentication – All users accessing Personal Data are authenticated persons.
* Access control – Physical access to data storage facilities is limited to approved personell and is logged.
* Encryption – transfer of Personal Data, and access to Personal Data is encrypted using VPN technology, FTPS services or file encryption.

## Transparency

Under the category of Personal Data, Norstat will receive and handle static exports of contact lists including data necessary for performing surveys. There is no real time information available for processing such lists.

## Isolation (purpose limitation)

Norstat is processing data for the purpose of Market Research, and will not re-use data for other purposes, or other partners. Personal Data (contact lists) for specific projects will not be re-used for other projects unless this is explicitly requested form Data Controller.

## Intervenability

Norstat will hold copies of Personal Data from Data Controller in form of respondent lists. All intervention on data must be performed in Data Controllers systems. If data is to be replaced or updated, this must be initiated from Data Controller. Updating, replacing or deleting data can only be performed manually by Norstat upon request from Data Controller.

## Portability

If an export of Personal Data is requested, Norstat will be able to export data from contact lists by a manual process performed by a Norstat employee with sufficient access.

Survey data is by default anonymized, and is thereby not retrievable for portability purposes.

## Accountability

Norstat has implemented an Internal Control system for handling Information Security and Personal Data to ensure compliance with current legislation.

## Data retention and deletion

Routines for data retention and deletion of Personal Data is established and described in the Internal Control system.

## Physical security

Physical security for all data processing and data storage facilities are controlled through the Internal Control system.