Data Processing Terms

The following Data Processing Terms build a Data Processing Agreement ("**DPA**"), which, according to Section 6.2 of the Agreement, shall become an integral part of the ENGAGE Case Studies Data Provider Agreement ("**Agreement**") and is entered into by and between the Parties as defined in the Preamble of the Agreement, insofar as the Parties exchange personal data.

WHEREAS

a. The Parties have agreed on the following clauses in order to meet the requirements of the Regulation (EU) 2016/679 '*on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC*' (General Data Protection Regulation, hereinafter "**GDPR**") and to ensure the protection of the rights of the data subjects.

b. In the context of the contractual relationship between the Controller and the Processor, the latter performs the activities described in Section 2 of the Agreement (hereinafter, the "**Services**").

c. In order to carry out the Services on behalf of the Controller, the Processor processes the Data. This DPA applies and sets out the rights and obligations of the Controller and the Processor, to the extent personal data is processed by the Processor on behalf of the Controller in this context.

d. The clauses of this DPA shall take priority over any similar provisions contained in other agreements between the Parties regarding the processing of the personal data for the same purposes described herein.

e. Three appendices are attached to and form an integral part of the DPA. In more detail:

   i. *Appendix A* contains details about the processing of the personal data, including the purpose and nature of the processing, categories of personal data and categories of data subjects.

   ii. *Appendix B* contains a list of sub-processors used by the Processor and authorised by the Controller.

   iii. *Appendix C* contains a description of the technical and organizational measures which shall be implemented by the Processor.

f. The DPA along with the appendices shall be retained in writing, including electronically, by both Parties.

g. Where these clauses of this DPA use the terms defined in the GDPR, those terms shall have the same meaning as in the GDPR.

h. The clauses of this DPA shall be read and interpreted in the light of the provisions of the GDPR and shall not be interpreted in a way that conflicts with rights and obligations provided for in the GDPR or prejudices the fundamental rights or freedoms of the data subjects.

1. RIGHTS AND OBLIGATIONS OF THE CONTROLLER

a. The Controller is responsible for ensuring that the processing of the personal data takes place in compliance with the GDPR, applicable supplementing data protection law and this DPA.

b. The Controller has the right and obligation to make decisions about the purposes and essential means of the processing of personal data.

c. The Controller shall be responsible, among others, for ensuring that the processing of the personal data, which the Processor is instructed to perform on the Controller's behalf, relies on an appropriate legal basis in accordance with the GDPR or applicable supplementing data protection law.

2. THE PROCESSOR'S OBLIGATIONS

a. Processor shall process the personal data only in accordance with the documented instructions given by the Controller, including with regard to transfers of personal data to a third country or an international organisation, in this DPA, unless required to do so by European Union or European Union Member State law to which the Processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

b. Any further instructions that go beyond the instructions contained in this DPA must be within the subject matter of this DPA and the Agreement and shall always be given and kept in writing, including electronically, in connection with this DPA. If the implementation of such further instructions results in costs for the Processor, the latter shall inform the Controller about such costs with an explanation of the costs before implementing the instructions. Only after the Controller's confirmation to bear such costs for the implementation of the instructions, the Processor is required to implement such further instructions.

c. The Processor shall immediately inform the Controller if any of the instructions given by the latter, in the opinion of the Processor, contravene the GDPR or any other applicable European Union or European Union Member State data protection law. The Processor may suspend the implementation of the affected instruction until Controller confirms, amends or withdraws its instruction. If the Controller confirms the affected instruction upon the information provided by the Processor and acknowledges its liability for the challenged instruction, the Processor shall implement such instruction.

d. The Processor shall process the personal data on behalf of the Controller and only for the specific and explicit purpose(s) of the processing specified by the Controller, as set out in **Appendix A**.

e. The Processor shall make available to the Controller, upon request, all information necessary to demonstrate compliance with the Processor's obligations laid down in this DPA and Art. 28 GDPR.

3. CONFIDENTIALITY

The Processor shall only grant access to the personal data being processed on behalf of the Controller to persons under the Processor's authority who have committed themselves to

confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need-to-know basis.

4. SECURITY OF PROCESSING

a. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Controller and Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. Accordingly, the Controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

- pseudonymisation and encryption of personal data;
- the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

b. According to Article 32 of the GDPR, also the Processor shall in its turn – independently from the Controller – implement technical and organizational measures to ensure the security of personal data:

- to prevent unauthorised persons from gaining physical access to the data processing equipment where the personal data is processed;
- to ensure that the persons entitled to use its data processing system are only able to access the data within the scope and to the extent covered by their respective access permission (authorisation) and that personal data cannot be read, copied, modified, or removed without authorization;
- to make sure that data collected for different purposes can be processed separately;
- to ensure that if security measures are adopted through external entities, the Processor obtains written description of the activities performed that guarantees compliance of the measures adopted with this document, given that the Processor monitors such compliance;
- to use state of the art encryption technologies;
- to make sure that it can check and establish whether and by whom personal data has been inputted into data processing systems or removed;
- to prevent the personal data from being read, copied, altered or deleted by unauthorised parties during the transmission thereof or during the transport of the data media;
- to make sure that personal data is protected from accidental destruction or loss.

c. Further details are stipulated in **Appendix C.**

d. The Controller hereby confirms that the Processor has implemented appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subjects.

5. **USE OF SUB-PROCESSORS**

a. The Processor shall not engage any other processor (sub-processor) for the processing of the personal data under this DPA without the prior general written authorization of the Controller.

b. The Processor has the Controller's general authorisation for the engagement of sub-processors. The list of sub-processors authorised by the data Controller and currently used by the Processor can be found in **Appendix B**. The Processor shall specifically inform in writing (e.g., by email) the Controller of any intended changes concerning the addition or replacement of sub-processors at least 45 days in advance, thereby giving the Controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). In order to make the assessment and the decision whether to authorise sub-processors, the Processor shall provide the Controller with the information necessary to enable the controller to exercise its right to object. If the Controller does not object within thirty (30) calendar days after receipt of Processor's notice the further sub-processor(s) shall be deemed accepted and the Processor will inform the Controller about this when the aforementioned time period commences.

c. If the Controller has a legitimate reason to object to the use of the sub-processor and objects within the term set forth in Section 5(2), the Processor shall have the right to cure the objection through one of the following options (to be selected at the Processor's sole discretion): (a) the Processor cancels its plans to use the sub-processor with regard to the processing of personal data under this DPA; or (b) the Processor will take the corrective steps requested by the Controller in its objection (which remove the Controller's objection) and proceeds to use the sub-processor(s); or (c) Controller may agree not to use (temporarily or permanently) the particular aspect of the Service that would involve the use of such sub-processor(s). If none of the above options are reasonably available and the objection has not been cured within thirty (30) calendar days after the Processor's receipt of the Controller's objection, either Party may terminate the affected Service with sixty [60 days'] prior written notice.

d. Where the Processor engages a sub-processor for carrying out specific processing activities (on behalf of the Controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the Processor under this DPA.

e. At the Controller's request, the Processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the Controller. To the extent necessary to protect business secret or other confidential information, including personal data, the Processor may redact the text of the agreement prior to sharing the copy.

f. If the sub-processor does not fulfil its data protection obligations, the Processor shall remain fully liable to the Controller as regards the fulfilment of the obligations of the sub-processor.

6. **INTERNATIONAL TRANSFER OF THE PERSONAL DATA**

a. Any transfer of personal data to third countries or international organisations by the Processor shall only occur on the basis of documented instructions from the Controller and shall always take place in compliance with Chapter V of the GDPR.

b. This DPA shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR and cannot be relied upon by the Parties as a transfer tool under Chapter V of the GDPR.

7. **ASSISTANCE TO THE CONTROLLER**

a. The Processor shall promptly notify the Controller about any request received directly from the data subject. It shall not respond to that request itself, unless and until it has been authorised to do so by the Controller.

b. Taking into account the nature of the processing, the Processor shall assist the Controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the Controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR.

c. The Processor shall, furthermore, taking into account the nature of the processing and the information available to it, assist the Controller in ensuring compliance with its obligation pursuant to Art. 32 to 36 GDPR and, thus, to:

   i. notify without undue delay and, where feasible, not later than 72 hours after having become aware of it, any event which qualifies as personal data breach pursuant to the GDPR to the competent data protection authorities, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of the data subjects;

   ii. communicate without undue delay any personal data breach to the data subject involved, when such breach is likely to result in a high risk to the rights and freedoms of the data subjects;

   iii. carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment or "**DPIA**");

   iv. consult the competent data protection authority prior to processing where a DPIA indicates that the processing would result in a high risk in the absence of measures taken by the Controller to mitigate the risk.

8. **NOTIFICATION OF PERSONAL DATA BREACH**

a. In case of any personal data breach within the meaning of Clause 7.c.i. above, the Processor shall, without undue delay after having become aware of it, notify the Controller of such personal data breach. The Processor's notification shall, if possible, take place within 72 hours after it has become aware of the personal data breach, so to enable the Controller to timely comply with its obligation to notify the event to the competent supervisory authority.

b. In accordance with Clause 7.c.i. above, the Processor shall assist the Controller in notifying any personal data breach affecting the personal data processed under this DPA to the competent supervisory authority, meaning that the Processor is required to assist the Controller in obtaining, where reasonably feasible, the information listed below:

- the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- the likely consequences of the personal data breach;
- the measures taken or proposed to be taken by the Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

9. **LIMITATION OF LIABILITY AND INDEMNIFICATION**

a. Any liability arising out of or in connection with a violation of the obligations of this DPA or under applicable data protection law, shall follow, and be governed by, the liability provisions set forth in, or otherwise applicable to, the Agreement, unless otherwise provided within this DPA.

b. The Controller shall defend, indemnify, and hold harmless Processor and the officers, directors, employees, successors, and agents of the Processor from all claims, damages, liabilities, assessments, losses, costs, administrative fines and other expenses (including, without limitation, reasonable attorneys' fees and legal expenses) arising out of or resulting from any claim, allegation, demand, suit, action, order or any other proceeding by a third party (including supervisory authorities) that arises out of or relates to the violation of Controller's obligations under this DPA and/or any applicable data protection law.

10. **ERASURE AND RETURN OF PERSONAL DATA**

a. On termination of the Services, the Processor shall be under an obligation to return to the Controller all the non-anonymised personal data and to delete any existing copies of the non-anonymised personal data, unless a provision of law or an order of a competent authority exists which requires the Processor to further retain all or some of the personal for predetermined and legally admitted purposes.

b. Processor may retain Controller personal data to the extent required by applicable laws and only to the extent and for such period as required by them. For the avoidance of doubt and

with effect from the cessation date, Processor shall become the Controller in respect of Controller personal data retained in accordance with this section.

11. **AUDIT AND INSPECTION**

a. The Parties shall be able to demonstrate compliance with this DPA.

b. The Processor shall deal without undue delay and properly with all inquiries from the Controller that relate to the processing under this DPA.

c. The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations set out in Art. 28 GDPR and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller. The information obligation is generally met by providing the Controller, upon the Controller's request, with an annual audit report based on [ISO 27001 or ISAE3402 or SSAE16-SOC 1 Type 2 or ISAE3000 or SSAE16-SOC 2 Type 2 or similar] or similar audit reports created by a third party ("**Audit Report**").The Controller may request inspections conducted by the Controller or another auditor mandated by the Controller ("**On-Site Audit**"). Such On-Site Audit is subject to the following conditions: (i) On-Site Audits are limited to processing facilities and personnel of the Processor involved in the processing activities covered by this DPA; and (ii) On-Site Audits occur not more than once annually or as required by applicable data protection law or by a competent supervisory authority or if there are indications of non-compliance or subsequent to a material personal data breach that affected the personal data processed by the Processor under this DPA; and (iii) may be performed during regular business hours, solely insubstantially disrupting the Processor's business operations and in accordance with the Processor's security policies; and (iv) the Controller will inform Processor of its intention to conduct an audit at least 45 days prior to the envisaged date by written notice, unless a shorter notification period is legally required or the Controller provides compelling grounds that a shorter notification period is appropriate in the individual case.; and (v) the Controller shall bear any costs arising out of or in connection with the On-Site Audit. The Controller is obliged to create an audit report summarizing the findings and observations of the On-Site Audit ("**On-Site Audit Report**"). On-Site Audit Reports as well as Audit Reports are confidential information of the Processor and shall not be disclosed to third parties unless required by applicable data protection law or subject to Processor's consent.

d. The Processor and Controller shall make the information referred to in this Section 11, including the results of any audits, available to the competent supervisory authority on request.

12. **PARTIES' AGREEMENT ON OTHER TERMS**

The Parties may agree other clauses concerning the processing of personal data by the Processor on behalf of the Controller, as long as they do not contradict directly or indirectly this DPA or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

13. **COMMENCEMENT AND TERMINATION**

a. This DPA shall become effective on the date the Agreement becomes effective.

b. Both Parties shall be entitled to require this DPA to be renegotiated if changes to the applicable law, or inexpediency of the DPA, should give rise to such need.

c. This DPA shall apply for the duration of the Services. For such duration this DPA cannot be terminated unless other equivalent clauses governing the provision of personal data processing services have been agreed between the Parties.

APPENDIX A

INFORMATION ABOUT THE PROCESSING (EDW and HYP)

1. The purpose of the Processor's processing of the personal data on behalf of the Controller is:

   The development of case studies under the ENGAGE for ESG initiative based on the Data provided by the Data Provider.

2. The nature of the Processor's processing of the personal data on behalf of the Controller is:

   Collection, recording, organization, structuring, storage, use, disclosure by transmission, dissemination or otherwise making available, alignment, combination, erasure and destruction of personal data.

3. The processing includes the following categories of personal data:

   Cadastral and energy efficiency data of real estate properties.

4. Processing includes the following categories of data subjects:

   Customers of the Controller.

5. Processor's processing of personal data on behalf of the Controller may be performed when this DPA commences. Processing has the following duration:

   The duration of the Agreement.

APPENDIX B

AUTHORISED SUB-PROCESSORS.- EDW

On commencement of this DPA, the Controller expressly authorises the engagement of the following sub-processors by the Processor:

NAME	COMPANY'S ID NUMBER	ADDRESS	DESCRIPTION OF PROCESSING
Microsoft Ireland Operations Limited	256796	70 Sir Rogerson's Quay Dublin 2 Ireland	Microsoft (Office 365) and Microsoft Azure: data hosting service

AUTHORISED SUB-PROCESSORS.- Hypoport

On commencement of this DPA, the Controller expressly authorises the engagement of the following sub-processors by the Processor:

NAME	COMPANY'S ID NUMBER	ADDRESS	DESCRIPTION OF PROCESSING
Microsoft B.V.		Evert van de Beekstraat 354 1118 CZ Amsterdam Nederland	Storage of data
Quaere B.V.		Symfonielaan 24 3438 EV Nieuwegein 030-6361800 Nederland	IT infra support

APPENDIX C

TECHNICAL AND ORGANISATIONAL MEASURES.- EDW

1. ***Measures of pseudonymisation and encryption of personal data***

   The data for processing is already provided pseudonymised.

2. ***Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services***

   a. **Measures to ensure confidentiality**

   - End devices

     Processor provides all employees with suitable end devices. They are set up, managed and controlled by IT administrators.

     The use of the devices is regulated in the Processor's Acceptable Use Policy.

   - Authorisations

     Access to the Processor's infrastructure is only granted to those persons who have been authorized for this purpose.

     Permissions are usually controlled by roles and groups, which are differentiated according to permissions with the characteristics read, write, execute, delete.

   - Active Directory

     A central logon service manages and controls all system logons.

     All Processor internal PCs are connected to the existing Active Directory. External PCs, if necessary, have access only to Internet resources.

   - Network security Office

     The networks are strongly segmented according to functional areas. This is achieved by a complex VLAN structure, which can be controlled from each other via various routers and firewalls. There are physical firewalls to the outside.

   - Network security infrastructure

     The applications are cloud hosted. The underlying network structure is divided into different areas and secured via firewalls. Access to the applications is encrypted via a dedicated MPLS network connection.

   - Separation requirement

     Data collected for different purposes is processed separately and is segregated from other data and systems in such a way that unplanned use of this data for other purposes is excluded.

   b. **Measures to ensure integrity**

   Measures to ensure that stored personal data is not corrupted by system malfunctions:

- Change Control

  Changes are handled through the formal software development life cycle will be included within the company's change management program.

- Transmission Control

  Access and data transfer are implemented via protocols such as https, SFTP or with VPN connections. This ensures that data is not read or changed by unauthorized persons during transmission.

- Logging

  Accesses to the system environment and applications are logged in different systems and can be checked:

  ✓ System logon.
  ✓ All Active Directory logins are recorded in the Event Log.
  ✓ All VPN accesses are recorded in the VPN log.

- Applications

  The log levels of the applications are defined in such a way that user logins can be traced.

c. Measures to ensure availability and resilience

Measures to ensure that personal data is protected against accidental destruction or loss:

- Backup

  Appropriate backup plans exist and are routinely reviewed. The integrity and completeness of backups is checked regularly.

- Disaster environment

  Data is synchronized and systems are activated as needed in the DR environment. Tests are performed annually.

- Technical measures

  All measures such as access protection, physical security such as power loss, air conditioning failure or protection against fire are basic services provided by the suppliers. Corresponding proofs and certifications are available.

- Network protection

  The networks are secured by zones, routers and firewalls. Only a limited number can be accessed directly from outside (via MFA). All other systems are located in protected network segments. Routers with firewall functionality are located between the networks.

  All network components are monitored and escalated in case of corresponding messages.

  A central console for virus threats and alerts is implemented.

- Penetration tests

  Defined applications are subjected to regular penetration tests. The tests are performed by external service providers.

- Hardware and Software Lifecycle

The lifecycle of hardware and software is monitored so that Processor ensures that support, firmware updates or security paths are provided by the manufacturers.

- Patching

  All endpoints are patched on a regular basis. The application of patches to operational systems is evaluated in advance to ensure that software updates do not have any negative consequences for the application.

d. Measures *for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident*

Please, see the measures listed above under section "Measures to ensure availability and resilience".

e. *Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational* measures *in order to ensure the security of the processing*

The processing of the personal data is performed in a secure site. Please, see above the measures listed under sections "Measures to ensure confidentiality, integrity and availability".

3. Measures for user identification and authorisation

Only authorised internal and external users through user identification and authorisation get access to the dedicated private area where the data is made available from Controller to Processor and vice versa.

Users or resources will be granted access only to permissioned systems that are necessary to fulfil their roles and responsibilities. Furthermore, users or resources will be provided with the minimum privileges on their accounts which are necessary to fulfil their specific roles and responsibilities.

4. Measures for the protection of data during transmission and storage

Data is uploaded, downloaded through and saved in a secure web-based system.

5. Measures for ensuring physical security of locations at which personal data are processed

- Physical Access control

  Measures that physically deny unauthorised persons access to IT systems and data processing equipment used to process personal data, as well as to confidential files and data carriers.

- Buildings and physical protection measures

  The building and the premises are secured with a key card locking system. Only authorised persons are granted access to the building. The issuance of the necessary key cards is managed centrally in the Central Services department.

- Data Center

  The environment where the data is made available from Controller to Processor and vice versa is operated by Microsoft. The environment is hosted in the European Union under the provisions of GDPR and is subject to applicable regulations regarding access protection.

  Physical access to the facilities is only possible by the service provider and is subject to strict access controls (access control, video, logging, secure zones).

- Security zones

There are no server rooms on the Processor premises and only one switchboard area. Access is only permitted to specially authorised employees.

- External persons

  A separation must be made here between visitors and external service providers.

  ✓ Visitors

  There are visitor regulations for visitors. All visitors are logged. The hosts have the responsibility to keep the logs.

  ✓ External service providers

  Cleaning personnel have access to the premises except for security zones. They are contractually obligated to maintain confidentiality.

  External service providers who provide support or project assignments are contractually obligated to maintain confidentiality, contract data processing, data protection and information security. They are not classified as visitors.

6. Measures for ensuring events logging

- User Accounts

  Logging of user accounts helps us to ensure that they are only performing the activities they are authorised to perform. This includes the following:

  ✓ Login to our systems.
  ✓ Read, write, modify or delete database records, folders or files.
  ✓ Upload and download of documents to and from our system.

- Date and time of log on and off

  Along with the person's user account, the date and time of log on and off are also recorded.

- Date and time of updating critical database records

  Within Processor, our tools involve addition and modification of critical database records (e.g. data quality rule builder). With this, the date and time along with the user account are stored in our database tables.

- Application and system exceptions

  Exception logging and analysis is the only way to investigate what is wrong with an application or system. At Processor, tools are equipped with this kind of logging and email alerts are sent to the IT Department to resolve any issue at the shortest possible time.

  ✓ Application – exceptions are logged, and email alerts are triggered.
  ✓ System – email alerts are triggered if the threshold of server's CPU, memory and disk consumptions are reached.

7. Measures for internal IT and IT security governance and management

An IT Security framework has been developed. In compliance with this framework:

a. Processor assesses IT security risks on a regular basis.

b. All IT assets are formally inventoried, updated or patched regularly to mitigate security vulnerabilities and protected against attacks through appropriate anti-virus / anti-malware software and other threat detection tools.

c. All user accounts, access rights and permissions are formally controlled.

d. User activities and critical IT system operations are logged in order to enable investigation as and when required.

e. Appropriate capabilities are in place to support business activities in the situation of a disaster or a major disruption of IT systems.

f. Backup systems and processes to restore backups are in place in order to ensure retrieval of information in case of accidental data loss.

g. All network related traffic between Processor's systems and the internet is controlled.

h. An IT Security Incident Management Procedure is in place and is taught to all employees to ensure staff knows how to react in such an event.

i. Processor counts on a dedicated IT Security Officer reporting to the Compliance Officer for the management of the IT Security framework.

j. Processor staff is bound by strict confidentiality obligations and prevented from sharing any business-related information (including personal data) with unauthorised recipients. The need-to-know principle governs the exchange of information within the company to ensure that confidential information is restrictedly disseminated.

8. Measures for certification/assurance of processes and products

In the context of Processor's registration as a securitisation repository with the European Securities and Markets Authority, all policies and procedures have been reviewed and approved for content and completeness. This includes compliance and governance as well as IT security.

An external audit firm conforms the 3rd Line of Defence of Processor internal controls system framework and regularly review the processes and regulatory requirements.

9. Measures for ensuring data minimization

a. Processor shall only process the adequate, relevant and limited data to what is necessary and legally justified in relation to the purposes of the Agreement.

b. The Agreement defines the limited purpose of the data processing.

c. The Agreement specifies how the personal data will be used.

d. The data that Processor is going to process is pseudonymized.

e. Processor will delete the personal data that is no longer required.

10. Measures for ensuring limited data retention

Processor shall only keep personal data for the purpose for which it was obtained. This means that personal data is anonymised or erased from Processor´s systems when it is no longer required and the legal or contractual obligations have been met.

11. Measures for ensuring accountability

a. Processor has documented procedures for the Processing of Personal Data.

b. In the event that Processor is subject to an audit or investigation by a regulator, Processor is able to provide evidence of how Processor complies with the data protection requirements explained in this General Data Protection Policy.

c. When developing or considering a new Processing activity, in particular implementing a new technology or IT system, or changing any existing Processing activities, the owner of the Processing activity shall inform the Data Protection Officer and shall provide the Data Protection Officer with all necessary information in order to keep the related documentation (such as notices, records of Processing activities, data Processing and data transfer agreements) up-to-date.

12. Measures for allowing data portability and ensuring erasure

As part of the ordered processing, personal data is processed. The generated information after processing does not involve personal data and will be aggregated.

Once aggregation is complete, the detailed, underlying data is anonymised or erased. Thus, data portability is not applicable.

TECHNICAL AND ORGANISATIONAL MEASURES.- Hypoport

1. ***Measures of pseudonymisation and encryption of personal data***

The data for processing is already provided pseudonymised.

2. ***Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services***
   - Our processes as described in our ISAE 3402 type II.
   - Our processes as described in our business continuity plan.

3. **Measures *for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident***

Our processes as described in our business continuity plan.

4. ***Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational* measures *in order to ensure the security of the processing***
   - Our processes as described in our ISAE 3402 type II.
   - Our processes as described in our business continuity plan.

5. ***Measures for user identification and authorisation***
   - Role separation
   - User management privilege to administrator
   - MFA available

6. ***Measures for the protection of data during transmission***
   All connections are encrypted using TLS.

7. ***Measures for the protection of data during storage***

Data is encrypted at rest using Transparent Data Encryption (TDE).

8. ***Measures for ensuring physical security of locations at which personal data are processed***
   - Reception / security
   - Access with key for personnel only

9. ***Measures for ensuring events logging***

Logging is simultaneously done to both a file based and a database based logging store.

10. ***Measures for ensuring system configuration, including default configuration***

All systems are configured using bastion-host like templates. To reduce the attack surface all services/ports are disabled unless they are explicitly needed by/for the application to function.

11. Measures for internal IT and IT security governance and management

This is covered by Hypoport's ISAE 3402 Type II, particularly by sections I, II, VI & VII, which pertain to Logical access management, Change Management, Security Management and Hosting management respectively.

12. Measures for certification/assurance of processes and products

See answer to section 11.

13. Measures for ensuring data minimization

The systems allows for data to be removed at set intervals depending on the (GDPR) rules that apply. Additionally data minimization in the context of the ENGAGE project is incorporated *by design* in the creation process of the templates.

14. Measures for ensuring limited data retention

The systems allows for data to be removed at set intervals depending on the (GDPR) rules that apply.

15. Measures for ensuring accountability

Our processes as described in our ISAE 3402 type II.

16. Measures for allowing data portability and ensuring erasure

Microsoft's SOC2 applies here. When a data store/base is (re)moved, the cloud provider ensures that the source is properly disposed of.