DATA PROCESSING ADDENDUM

This Data Processing Addendum, including its Appendices, ("DPA") forms part of the Master Subscription Agreement, Livingroom Terms of Service (https://livingroomanalytics.com/terms), hereinafter defined as the "Agreement", reflecting the parties' agreement with regard to the Processing of Personal Data.

By signing the Agreement, Customer enters into this DPA on behalf of itself. The parties agree that this DPA sets forth their obligations with respect to the processing and security of Customer Data and Personal Data. Unless a separate Data Processing Agreement exists, this DPA governs the processing and security of the Livingroom Analytics' Services.

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR) between Customer (the data controller) and Livingroom Analytics, VAT/CVR DK38840606, Fruebjergvej 3, DK-2100 Copenhagen, Denmark (the data processor), each a 'party'; together 'the parties' HAVE AGREED on the following Contractual Clauses (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

1. Table of Contents

2. Preamble

1. These Contractual Clauses (the Clauses) set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.

2. The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 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).

3. In the context of the provision of the Livingroom Engagement Platform (the SaaS Software), the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

4. The Clauses shall take priority over any similar provisions contained in other agreements between the parties.

5. Four appendices are attached to the Clauses and form an integral part of the Clauses.

6. Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

7. Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorised by the data controller.

8. Appendix C contains the data controller's instructions with regards to the processing of personal data, the security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.

9. Appendix D contains the minimum level of security measures requirements agreed upon between the parties on the basis of the risk assessment that the Data Controller has performed.

10. The Clauses along with appendices shall be retained in writing, including electronically, by both parties.

11. The Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

3. The rights and obligations of the data controller

1. The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State[1] data protection provisions and the Clauses.

2. The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

[1] References to "Member States" made throughout the Clauses shall be understood as references to "EEA Member States".

3. The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

4. The data processor acts according to instructions

1. The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.

2. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

5. Confidentiality

1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data 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. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

2. The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

6. Security of processing

1. Article 32 GDPR stipulates that, 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 data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

   The data 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:

   a. Pseudonymisation and encryption of personal data;

   b. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;

   c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

   d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.

3. The Data Processor shall in ensuring the above – in all cases – at a minimum implement the level of security and the measures specified in Appendix D to this Data Processing Agreement.

4. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by *inter alia* providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

   If subsequently – in the assessment of the data controller – mitigation of the identified risks require further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

7. Use of sub-processors

1. The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

2. The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general written authorisation of the data controller.

3. The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least 3 months in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the data controller can be found in Appendix B.

4. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

   The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.

5. A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the

legal data protection content of the sub-processor agreement, shall not require submission to the data controller.

6. The data processor shall agree a third-party beneficiary clause with the sub-processor where – in the event of bankruptcy of the data processor – the data controller shall be a third-party beneficiary to the sub-processor agreement and shall have the right to enforce the agreement against the sub-processor engaged by the data processor, e.g. enabling the data controller to instruct the sub-processor to delete or return the personal data.

7. If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

8. Transfer of data to third countries or international organisations

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

2. In case transfers to third countries or international organisations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

3. Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:

    a. transfer personal data to a data controller or a data processor in a third country or in an international organization

    b. transfer the processing of personal data to a sub-processor in a third country

    c. have the personal data processed in by the data processor in a third country

4. The data controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.

5. The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

9. Assistance to the data controller

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

This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:

a. the right to be informed when collecting personal data from the data subject
b. the right to be informed when personal data have not been obtained from the data subject
c. the right of access by the data subject
d. the right to rectification
e. the right to erasure ('the right to be forgotten')
f. the right to restriction of processing
g. notification obligation regarding rectification or erasure of personal data or restriction of processing
h. the right to data portability
i. the right to object
j. the right not to be subject to a decision based solely on automated processing, including profiling

2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.3., the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

   a. The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

   b. the data controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

   c. the data controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);

   d. the data controller's obligation to consult the competent supervisory authority prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

3. The parties shall define in Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1. and 9.2.

10. Notification of personal data breach

1. In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.

2. The data processor's notification to the data controller shall, if possible, take place within 24 hours after the data processor has become aware of the personal data breach to enable the

data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

3. In accordance with Clause 9(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

   a. 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;

   b. the likely consequences of the personal data breach;

   c. 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.

4. The parties shall define in Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

11. Erasure and return of data

1. On termination of the provision of personal data processing services, the data processor shall be under obligation to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so unless Union or Member State law requires storage of the personal data.

12. Audit and inspection

1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.

2. Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.7.

3. The data processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the data controller's and data processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the data processor's physical facilities on presentation of appropriate identification.

13. The parties' agreement on other terms

1. The parties may agree other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

14. Commencement and termination

1. The Clauses shall become effective on the date when the Data Controller is signing up with the Livingroom Engagement Platform.

2. Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

3. The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

4. When the Data Controller renews or purchases a new subscription with Livingroom, the then-current Clauses will apply and will not change during Data Controller's subscription. However, if or when Livingroom Analytics introduces new features to the Livingroom Engagement Platform, Livingroom Analytics may alter and update the Clauses that apply to Data Controller's use of those new software features.

5. If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 11.1. and Appendix C.4., the Clauses may be terminated by written notice by either party.

6. Signature

   On behalf of the data processor

Name	Roar V. Bovim
Position	CEO
Date	April 12th, 2023
Signature	

15. Data controller and data processor contacts/contact points

1. The parties shall be under obligation continuously to inform each other of contacts/contact points and changes to contacts/contact points.

Appendix A Information about the processing

A.1. The purpose of the data processor's processing of personal data on behalf of the data controller is:

To enable the Data Controller to use the Livingroom Engagement Platform which is owned and managed by the Data Processor.

The Livingroom Engagement Platform consists of:

a) a secure online administrator and leadership application used to intelligently monitor, track and improve employee performance and engagement

b) an add-on employee app, which can be accessed via a browser or installed on mobile de-vices and used in conjunction with the administrator application. Among others, the employee app is used to perform engagement and performance surveys.

Collectively a) and b) shall be referred to as the "Service".

A.2. The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing):

The processing for the Data Controller of personal data will be related to collecting, registering, storing and analysing personal data in order to help the Data Controller improving engagement and performance of its employees.

A.3. The processing includes the following types of personal data about data subjects:

Data collected and presented in the administration application:
name, birth date, gender, nationality, e-mail address, telephone number, employee picture, employment data, employment status, employee number, work location, absence status, department, report manager, job title, position start date, job level, job description, employee work type, flexible hour status, shift work status, education level, education field, education school, data of education, education grade (optional), data from user interaction with the Service such as the numbers and frequency of using the Service.

Data collected through the employee app:
employee evaluation of the workplace such as sense of belonging, sense of appreciation, communication, work purpose, personal and organizational growth and development, leadership, work facilities, task satisfaction, task execution, influence and autonomy, data from user interaction with the Service such as the numbers and frequency of using the Service.

Special categories of data:
None.

A.4. Processing includes the following categories of data subject:

Employees or organizational members who are working full or part-time for the Data Controller.

A.5. The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration:

Processing shall not be time-limited and shall be performed until these Clauses are terminated or cancelled by one of the Parties.

Appendix B Authorised sub-processors

B.1. Approved sub-processors

On commencement of the Clauses, the data controller authorises the engagement of the following sub-processors which have undertaken, together with their respective sub-processors, to comply with the European Union SCC 2021 (2021 Standard Contractual Clauses):

NAME & VAT REGISTRATION NUMBER	ADDRESS	DESCRIPTION OF PROCESSING	COMPLIANCE TO SCC 2021
Microsoft Corporation IE256796	Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park Leopardstown, Dublin 18 D18 P521, Ireland	The data is stored at the Sub-Processor's servers and processed, including statistical calculations, sorting, filtering and accessing, for the purpose of delivering the Livingroom Service for Data Controller's employees, managers and administrators.	**A.** "Microsoft implements and maintains the security measures set forth in Annex II of the 2021 Standard Contractual Clauses for the protection of Personal Data within the scope of the GDPR." ("Data Security, Security Practices and Policies", Microsoft DPA, p. 8) **B.** "All transfers of Customer Data, Professional Services Data, and Personal Data out of the European Union, European Economic Area, United Kingdom, and Switzerland to provide the Products and Services shall be governed by the 2021 Standard Contractual Clauses implemented by Microsoft." ("Data Transfers and Location, Data Transfers", Microsoft DPA, p. 10) **C.** "Microsoft is responsible for its Subprocessors' compliance with Microsoft's obligations in this DPA. Microsoft makes available information about Subprocessors on a Microsoft website. When engaging any Subprocessor, Microsoft will ensure via a written contract that the Subprocessor may access and use Customer Data, Professional Services Data, or Personal Data only to deliver the services Microsoft has retained them to provide and is prohibited from using Customer Data, Professional Services Data, or Personal Data for any other purpose. Microsoft will ensure that Subprocessors are bound by written agreements that require them to provide at least the level of data protection required of Microsoft by the DPA, including the limitations on disclosure of Processed Data. Microsoft agrees to oversee the Subprocessors to ensure that these contractual obligations are met." ("Notice and Controls on the use of Subprocessors", Microsoft DPA, p. 10)

The data controller shall on the commencement of the Clauses authorise the use of the abovementioned sub-processors for the processing described for that party. The data processor shall not be entitled – without the data controller's explicit written authorisation – to engage a sub-processor for a 'different' processing than the one which has been agreed upon or have another sub-processor perform the described processing.

B.2. Prior notice for the authorisation of sub-processors

The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least 3 months in advance.

Appendix C Instruction pertaining to the use of personal data

C.1. The subject of/instruction for the processing

The data processor's processing of personal data on behalf of the data controller shall be carried out by the data processor performing the following:

The data processor will be collecting, registering, storing and analysing employee data in order to help the Data Controller improving engagement and performance of its employees.

The Livingroom Terms & Conditions, https://livingroomanalytics.com/terms/ contains further descriptions of the processing.

C.2. Security of processing

The level of security shall reflect that the risk associated with the processing for the rights and freedoms of natural persons is assessed to be low.

The Data Processor shall hereafter be entitled and under obligation to make decisions about the technical and organisational security measures that are to be applied to create the nec-essary (and agreed) level of data security.

The Data Processor shall however – in any event and at a minimum – implement the measures following Appendix D, which have been agreed with the Data Controller (on the basis of the risk assessment that the Data Controller has performed).

C.3. Assistance to the data controller

The data processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the data controller in accordance with Clause 9.1. and 9.2. by implementing the following technical and organisational measures:

The data processor will assist the data controller in fulfilling Clause 9.1 and 9.2 by providing the necessary information and technical measures while the data controller will be responsible for responding to requests as well as communicating and reporting of breach to the government and data subjects. If the data processor receives requests from data subjects regarding any of its GDPR rights, the data processor will redirect the data subject to make its request directly to the data controller.

In order to assist the data controller, the data processor has developed data subject request procedures and a data subject request form to provide the necessary information and be prepared for actions in assisting the data controller. The Livingroom Customer Service personnel has also undergone training in responding to data subject requests. While many of the requests can be handled by the data controller using the functionality of the engagement platform, the data processor will assist with providing additional information and technical measures where this is necessary.

Furthermore, the data processor has developed an Information Security Incident Response Procedure, a Personal Data Breach Notification Procedure and an Incident Response Plan for data breach, in order to be able to assist the data controller in terms of a breach. The data processor has also carried out data protection impact assessments of the engagement platform's processing operations and are prepared to assist the data controller in similar assessments.

C.4. Storage period/erasure procedures

Personal data is stored with the Data Processor until the Data Controller requests that the data are erased or returned.

Upon termination of the provision of personal data processing services, the data processor shall either delete or return the personal data in accordance with Clause 11.1., unless the data controller – after the signature of the contract – has modified the data controller's original choice. Such modification shall be documented and kept in writing, including electronically, in connection with the Clauses.

C.5. Processing location

Processing of the personal data under the Clauses cannot be performed at other locations than the following without the data controller's prior written authorisation:

- Microsoft Azure Data Center, Ireland, North Europe
- Livingroom Analytics, Denmark

C.6. Instruction on the transfer of personal data to third countries

If the data controller does not in the Clauses or subsequently provide documented instructions pertaining to the transfer of personal data to a third country, the data processor shall not be entitled within the framework of the Clauses to perform such transfer.

C.7. Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor

The Data Processor (and any sub-processor) shall once a year at the Data Processor's expense submit a statement regarding the Data Processor's and the Data Processor's possible sub-processors' compliance with the security measures requirements stipulated in this Data Pro-cessing Agreement. The statement shall be provided at the end of each year so that it reach-es the Data Controller not later than 1st of February.

If the Data Controller assess, that the statement submitted by the Data Processor does not sufficiently validate the Data Processor's and the Data Processor's possible sub-processors' compliance with the security measures requirements stipulated in this Data Processing Agreement, the Data Processor must, at the request of the Data Controller and at the Data Controller's expense, obtain an auditor's statement from an independent auditor regarding the Data Processor's and the Data Processor's possible sub-processors' compliance with the security measures requirements stipulated in this Data Processing Agreement. The statement shall be prepared on the basis of a ISAE 3000 or any equivalent standard.

The Data Controller is entitled on request to disclose to the Danish Data Protection Agency any data received under the provisions of clause C7.

Appendix D Security requirements for low risk data processing

D.1. SECURITY POLICY

Requirement ID	Requirements	ISO27001 reference	ENISA reference
K1	The Supplier shall establish a set of policies for information security in relation to the performance of the Contract.	A.5.1.1	A.1
K2	The Supplier's information security policies in relation to the performance of the Contract shall be reviewed at planned intervals and, if necessary, on an *annual* basis.	A.5.1.2	A.2

D.2. ORGANISATION OF INFORMATION SECURITY

Requirement ID	Requirements	ISO27001 reference	ENISA reference
K3	The Supplier shall define and allocate all responsibilities for information security in relation to the performance of the Contract to the employees of the Supplier.	A.6.1.1	B.1
K4	The Suppliers shall ensure that all rights and responsibilities are adapted and/or revoked in accordance with clearly defined procedures during internal re-organizations, change of employment and terminations.	A.6.1.1	B.2

D.3. ACCESS CONTROL POLICY

Requirement ID	Requirements	ISO27001-reference	ENISA reference
K5	The Supplier shall ensure that the employees of the Supplier only have access to the personal data, which they specifically are authorised to process in relation to the performance of the Contract.	A.9.1.2	C.1

D.4. ASSET MANAGEMENT

Requirement ID	Requirements	ISO27001-reference	ENISA reference
K6	The Supplier shall identify the IT resources (hardware, software, and network) used for the performance of the Contract and prepare and maintain a register of the IT resources. The Supplier shall further appoint an employee to be responsible for the task of maintaining and updating the register.	A.8.1.1	D.1
K7	The Supplier shall, in relation to the performance of the Contract ensure that the register of the IT resources is reviewed and updated *on a regular basis*.	A.8.1.1	D.2

D.5. OPERATIONAL PROCEDURES AND RESPONSIBILITIES

Requirement ID	Requirements	ISO27001-reference	ENISA reference
K8	The Supplier shall apply documented operating procedures, including change procedures, in the IT systems used in the performance of the Contract. The Supplier shall further monitor these procedures on a regular basis.	A.12.1.1	E.1
K9	The Supplier shall separate the development, test and operating environments in relation to the performance of the Contract to reduce the risk of unauthorised access to or change of the operational environment in which the personal data is processed. No tests are to be performed on personal data without a prior, specific agreement with the Customer.	A.12.1.3	E.2

D.6. SUPPLIER RELATIONSHIPS

Requirement ID	Requirements	ISO27001-reference	ENISA reference
K10	The Supplier shall ensure that guidelines and similar directions regarding data security related to the access to personal data of subcontractors used for the performance of the Contract, are agreed with subcontractors and are documented. The Supplier shall ensure that such agreements reflect the security requirements for the Supplier and are appropriate considering the risk assessment in force.	A.15.1.1	F.1
K11	The Supplier shall establish and agree on all relevant data security requirements with each subcontractor who may be granted access to, processes, stores, communicates or supplies IT infrastructure components for data covered by the Contract. The Supplier shall in this respect ensure that subcontractors notify the Supplier of any personal data breach without undue delay and otherwise in accordance with the data processing agreement.	A.15.1.2	F.2
K12	The Supplier shall ensure that written security agreements are entered into with subcontractors, and subcontractors are to document compliance with of such agreements.	A.15.1.2	F.3

D.7. INFORMATION SECURITY INCIDENT MANAGEMENT

Requirement ID	Requirements	ISO27001-reference	ENISA reference
K13	The Supplier shall define managerial responsibility and procedures to ensure quick, efficient and orderly handling of data security breaches related to the performance of the Contract.	A.16.1.1	G.1
K14	The Supplier shall ensure that data security breaches related to the performance of the Contract are reported through the appropriate management channels without undue delay and in accordance with the data processing agreement and Articles 33 and 34 of the General Data Protection Regulation.	A.16.1.2	G.2

D.8. INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT

Requirement ID	Requirements	ISO27001-reference	ENISA reference
K15	The Supplier shall, in relation to the performance of the Contract, establish requirements to data security and data security continuity in critical situations, e.g., in case of a crisis or catastrophe.	A.17.1.1	H.1

D.9. HUMAN RESOURCE SECURITY

Requirement ID	Requirements	ISO27001-reference	ENISA reference
K16	The Supplier shall ensure that all employees and contractors maintain data security in accordance with the established policies and procedures of the organisation in relation to the performance of the Contract.	A.7.2.1	I.1

D.10. INFORMATION SECURITY AWARENESS, EDUCATION AND TRAINING

Requirement ID	Requirements	ISO27001-reference	ENISA reference
K17	The Supplier shall ensure that the employees of the Supplier are adequately informed about the security controls of the IT system relevant to their job function. Employees involved in the processing of personal data should also be properly informed about relevant data protection requirements and legal obligations through regular awareness campaigns.	A.7.2.2	J.1

D.11. ACCESS CONTROL

Requirement ID	Requirements	ISO27001-reference	ENISA reference
K18	The Supplier shall establish, document and maintain a policy for access control in relation to the performance of the Contract in accordance with the risk assessment in force at any time.	A.9.1.1	K.1
K19	The Supplier shall minimise the use of common user accounts in relation to the performance of the Contract. If the use of common accounts is necessary, the Supplier shall ensure that all users of a common account are authorised to use the information accessible to the common account holders.	A.9.4.4	K.2
K20	The Supplier shall ensure that an authentication mechanism is implemented, allowing access to the IT system (based on the access control policy and system). As a minimum a username/password combination should be used. Passwords should respect a certain (configurable) level of complexity.	A.9.4.3	K.3
K21	The Supplier shall ensure that the access control system applied in relation to the performance of the Contract has the ability to detect and not allow the usage of passwords that does not respect a certain (configurable) level of complexity.	A.9.4.3	K.4

D.12. LOGGING AND MONITORING

Requirement ID	Requirements	ISO27001 reference	ENISA reference
K22	The Supplier shall ensure that log files are activated, kept and reviewed on a regular basis. Logging is to include registration of user activity, access to data (view, modification, and deletion), exceptions, errors and data security events in relation to the performance of the Contract.	A.4.12.1	L.1
K23	The Supplier shall protect log facilities and log information in relation to the performance of the Contract against tampering and unauthorised access.	A.4.12.2	L.2
K24	The Supplier shall ensure that the clocks in all relevant data processing systems used for the performance of the Contract are synchronised to a single reference time source.	A.12.4.4	L.2

D.13. OPERATIONS SECURITY

Requirement ID	Requirements	ISO27001-reference	ENISA reference
K25	The Supplier shall, in relation to the performance of the Contract, ensure that database and applications servers are configured to run using a separate account, with minimum OS privileges to function correctly.	A.12.5.1	M.1
K26	The Supplier shall, in relation to the performance of the Contract, ensure that database and applications servers only process the personal data that is actually needed in order to achieve its processing purposes.	A.12.5.1	M.2

D.14. SECURITY REQUIREMENTS OF INFORMATION SYSTEMS

Requirement ID	Requirements	ISO27001-reference	ENISA reference
K27	The Supplier shall ensure that users will not be able to deactivate security settings in relation to the performance of the Contract.	A.12.2.1	N.1
K28	The Supplier shall ensure that anti-virus applications and detection signatures are configured on a weekly basis in relation to the performance of the Contract.	A.12.2.1	N.2
K29	The Supplier shall ensure that users do not have privileges to install or deactivate unauthorized software applications in relation to the performance of the Contract.	A.12.6.2	N.3
K30	The Supplier shall, in relation to the performance of the Contract ensure that the system has session time-outs when the user has not been active for a certain time period.	N/A	N.4
K31	The Supplier shall ensure that critical security updates released by the operating system developer are regularly installed.	A.12.5.1	N.5

D.15. COMMUNICATIONS SECURITY

Requirement ID	Requirements	ISO27001 reference	ENISA reference
K32	The Supplier shall, in relation to the performance of the Contract ensure that whenever access is performed through the Internet, communication is encrypted through cryptographic protocols (TLS/SSL or similar protocols).	A.13.1.1	O.1

D.16. BACK-UP

Requirement ID	Requirements	ISO27001-reference	ENISA reference
K33	The Supplier shall ensure that backup is carried out of information, software and system images in accordance with documented procedures applied for the performance of the Contract. Backup procedures is to be related to the documented roles and responsibilities of the Supplier.	A12.3.1	P.1
K34	The Supplier shall, in relation to the performance of the Contract ensure that backups are given an appropriate level of physical and environmental protection consistent with the standards applied to the originating data.	N/A	P.2
K35	The Supplier shall, in relation to the performance of the Contract ensure that the execution of backups is monitored to ensure completeness.	N/A	P.3
K36	The Supplier shall, in relation to the performance of the Contract ensure that full backups are carried out regularly.	A12.3.1	P.4

D.17. MOBILE DEVICES AND TELEWORKING

Requirement ID	Requirements	ISO27001-reference	ENISA reference
K37	The Supplier shall implement a policy and supporting security measures to control the risks arising by using mobile devices in connection with the performance of the Contract.	A.6.2.1	Q.1
K38	The Supplier shall, in relation to the performance of the Contract ensure that mobile devices that are allowed to access the information system should be pre-registered and pre-authorized.	A.6.2.1	Q.2
K39	The Supplier shall ensure that mobile devices used in relation to the performance of the Contract are subject to the same levels of access control procedures (to the data processing system) as other terminal equipment and the like used in relation to the performance of the Contract.	A.6.2.1	Q.3

D.18. TECHNICAL VULNERABILITY MANAGEMENT AND SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES

Requirement ID	Requirements	ISO27001-reference	ENISA reference
K40	The Supplier shall establish and apply rules in accordance with best practice for development of software used by the Supplier to the performance of the Contract.	A.14.2.1	R.1
K41	The Supplier shall ensure that specific security requirements are included in the requirements to the new information systems or improvements of existing information systems used by the Supplier in relation to the performance of the Contract.	A.14.1.1	R.2
K42	The Supplier shall implement specific technologies and techniques designed for supporting privacy and data protection (Privacy Enhancing Technologies (PETs)) for protection of personal data in relation to the performance of the Contract.	N/A	R.3
K43	The Supplier shall ensure that secure coding standards and practises are followed in relation to the performance of the Contract.	A.14.2.1	R.4
K44	The Supplier shall establish approval test programmes and related criteria for new information systems, upgrades and new versions of software used by the Supplier in relation to the performance of the Contract.	A.14.2.9	R.5

D.19. DISPOSAL OF MEDIA AND EQUIPMENT

Requirement ID	Requirements	ISO27001-reference	ENISA reference
K45	The Supplier shall dispose of media used for the performance of the Contract, when they are no longer needed, securely and in accordance with formal procedures.	A.8.3.2	S.1
K46	The Supplier shall, in relation to the performance of the Contract, ensure that documents with personal data are shredded before the documents are disposed of.	A.8.3.2	S.2

D.20. PHYSICAL AND ENVIRONMENTAL SECURITY

Requirement ID	Requirements	ISO27001 reference	ENISA reference
K47	The Supplier shall protect physical areas in relation to the performance of the Contract against access by non-authorised personnel.	A.11.1.2	T.1