Standard Contractual Clauses

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)

Between

The Customer
(the "**data controller**")

and

SameSystem A/S
CVR no.: 31487927
Rentemestervej 2A
2400 København NV
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. These Clauses forms part of the license agreement between the parties.

These Clauses shall govern all processing of personal data conducted by the data processor (including its affiliates) on the data controller's (including its affiliates) behalf.

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. The data processor will deliver the services described in the licence agreement and the general license terms between the parties and will in order to fulfil the licence agreement, process personal data on behalf of the data controller in accordance with the Clauses.

4. This data processing agreement shall supersede all prior processing agreements between the data processor and the data controller.

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 minimum 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 provisions for other activities which are not covered by the Clauses.

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.

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.

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

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. Based on 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. 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 30 days 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. 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, The Danish Data Protection Agency (Datatilsynet), 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, The Danish Data Protection Agency (Datatilsynet), 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 and/or return all personal data processed on behalf of the data controller and verify 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. and C.8.

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 of both parties' signature.

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. 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.

15. Contact

The data controller may contact the data processor on: dataprivacy@samesystem.com for all general inquiries about these Clauses and in case of data breaches.

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:

That the data controller can apply SameSystem's online workforce management system (SameSystem), to collect and process information about its employees and manage its work-force.

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 data processor makes SameSystem available to the data controller and on behalf of the data controller stores personal data about the employees of the data controller on the data processors and approved sub-processor's servers.

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

- Name
- Date of birth
- Social security number/national insurance number
- E-mail address
- Telephone number
- Home address
- Salary/pension
- Payroll and employee no.
- Job function
- Working hours
- Department
- Correspondence between data subjects
- Absence and leave (incl. parental leave and absence due to holiday and illness, excluding medical certificates)
- Warnings/dismissals
- Benefits
- Other job functions/responsibilities

All personal data which the data processor is given access to, shall be treated confidentially.

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

- Employees of 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:

The Clauses remains in force until the termination of the licence agreement and shall terminate in accordance with clause 14 above.

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:

NAME	HOSTING COUNTRY	ADDRESS INCL. COUNTRY	DESCRIPTION OF PROCESSING
SameSystem UAB, LT100004691219	No data storage	Didžioji g. 25, LT-01130, Vilnius, Lithuania	Development and improvements of the IT system. Technical aid, if necessary.
Hetzner Online GmbH, DE812871812	Germany (mainsite) and Finland (backup-site)	Industrie str. 25, 91710 Gunzenhausen, Deutschland	The storing of all data in the system, including personal data.
Scaleway SAS	France	8 rue de la Ville l'Evêque, 75008 Paris, France	The storing of data in France is primarily concerns backup data.
Link Mobility Group	Norway	Langkaia 1 – Havnelageret, 0150, Oslo, Norway	Delivery of SMS. (No data is processed in USA)
SMTP.DK Aps	Denmark	Refshalevej 163A 1. Tv 1432 København K, Denmark	Delivery of e-mails.
E-Signatur Danmark A/S CVR. 38491687	Ireland	Lersø Park Alle 107, 2100 København Ø. Denmark	Digital signatures
Sendbird, Inc	Germany	400 1st Ave San Mateo, California 94401 United States	Internal chat and messaging functionality within the SameSystem solution (chat between the users). Only the user's 'display name' and the chat/messages are processed. **NB**: This is an **optiona**l service, which the customer can choose to have activated by SameSystem.

The data controller shall on the commencement of the Clauses authorise the use of the above-mentioned 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 the Data Controller of any changes to the list of sub-processors at least 30 days prior to such changes and allow the Data Controller to object to the change of the sub-processor list. In case the Data Controller has not objected to the change of a sub-processor or engagement of a new sub-processor within the deadline, the sub-processor is seen as accepted.

Should the change to the list of sub-processors include an addition of sub-processor in a third country, the Data Controller must be notified as agreed in appendix C, clause C.6.

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 makes SameSystem available to the data controller as described in the license agreement, and the general license terms and will in order to fulfil the license agreement store personal data on behalf of the data controller, about the employees of the data controller and on the data processor's servers and relevant sub-processor servers as listed, described and approved by the data controller in Appendix B, B1.

The Data processor is instructed to process the personal data only for this purpose and is not entitled to process or use the data controller's personal data for any other purpose.

C.2. Security of processing

This section outlines the minimal security requirements to the data processor's internal security level and controls.

C.2.1.1 Organisation of Information Security (A.5 Security Policy & A.6 Roles and responsibility)

The data processor must have a documented security policy that addresses information security for all personnel employed by the data processor. The security policy must be reviewed and updated at least annually. There must be a policy on the processing of personal data – it can be included in the information security policy. An inventory of policies and procedures must be available at all times and maintained at a defined frequency determined by the data processor reflecting the obligations agreed in the Clauses.

An information security function must be responsible for security initiatives within the data processor's organisation. A named individual must be responsible for information security services delivered to the data controller.

The data processor must have relevant updated information security risk assessments available, which, upon request, must be made available to the data controller before services are delivered or changed.

Risk assessments of other external parties' access to data, systems and networks must be maintained by the data processor.

Roles and responsibilities related to the information security policy including the processing of personal data must be clearly defined and described.

C.2.1.2 Security Awareness (A.7 Human resource security)

The data processor must implement an information security and data protection awareness program to train all employees, who can access or handle the data controller's data.

C.2.1.3 Asset Management and Devices (A.8 Asset management)

The organisation must have a register of the IT resources used for the processing of personal data on behalf of the data controller. This must be maintained by a specific resource, who also reviews and updates the list regularly, at least annually.

All devices that are relevant in the handling and/or processing of the data controller's data, including USB-keys and other mobile devices, must be protected, including hard disk encryption, strong passwords used to protect against unauthorized access to personal data and access limitation to solely include employees with specific work-related purposes. Passwords must be stored in a hashed form. Login must automatically be blocked after 5 failed login attempts to protect against unauthorized access to personal data.

If personal information can be processed on data processor's employee-owned devices (BYOD) the devices must be adequately secured including encryption, forced adequate passwords and access limitation to employees with specific work-related purposes, e.g., through sandboxing technologies. BYOD policies, guidelines and data protection policies must, upon request, be provided to the data controller – this also includes adopting a Mobile Device Management (MDM) tool to enforce the above.

The data processor must ensure control with all assets used to deliver services to the data controller which ensures that all data controller data are securely overwritten using specialised software before hardware decommissioning or reuse for other purposes.

External media in use, including USB-keys, tablets, smartphones, etc. must be encrypted and securely erased or destroyed when decommissioned to protect against unauthorised access to personal data.

Disks and removable media must be stored and protected against unauthorised access during repair, service and when transported, and must be handled in line with all security requirements.

C.2.1.4 Access Management (A.9 Access Control)
The data processor must have clearly defined roles and responsibilities for the employees. Relevant screening, which may include evaluation of the following: background check, criminal records, previous employer etc. must be implemented before employment with terms and conditions of employment applied appropriately.

The data processor must implement user administration procedures, which define user roles and their privileges and how access is granted, changed, and terminated; which address appropriate segregation of duties; and which define the logging/monitoring requirements and mechanisms.

Privileged access to data, applications and infrastructure must be limited to persons with a specific, documented business purpose. Access rights and the allowed use of personal data must be described in writing for relevant job functions.

The data processor must ensure documented, efficient periodic control of the assigned rights on all types of user accounts across all systems that support the data controller's services. The control review must be updated at a minimum once every twelve months for end-user accounts and minimum once every six months for privileged accounts. Resigning or terminated users must have their credentials disabled immediately after their last working day.

The data processor must support the data controller in performing a review of the data controller's own accounts. On request from the data controller, the data processor must provide an overview of each employee's access rights to the data controller's data and systems.

All employees must be assigned unique User-IDs and re-issue of de-activated or expired user ID are prohibited.

Access rights must be implemented adhering to the "least privilege" approach.

Two-factor authentication must be required for privileged access to data, applications, and infrastructure.

Remote access to data, applications and infrastructure must require two-factor authentication.

C.2.1.5 Physical Security (A.11 Physical and environmental security)
Server rooms, data centres and office areas from where the data controller's data can potentially be accessed must be protected against unauthorised access.

Physical access control must be implemented for all such locations. Unauthorised access must be prohibited through 24x7 monitoring and access limitation with an electronic access audit log. Clear identification, through appropriate means e.g. ID badges for all personnel and visitors accessing the premises should be established, as appropriate.

Facilities must be equipped with relevant technical installations to ensure the availability of services.

C.2.1.6 Security on Location (A.11 Physical and environmental security)
Physical documents must be handled securely and protected throughout printing, secure storage to physical destruction for instance through the use of "follow me printing" and printers located in a secure limited access location. Filing cabinets must be placed in a secured location with limited access or in a secure storage. Cabinets must be secured according to the classification of what is stored within them.

Physical access control must be in place to protect all types of personal data on all media within each location, from offices and server rooms to printers and faxes that could produce prints containing the controller's personal data.

This includes protection against risks of unauthorised persons looking at computer screens, persons reading documents left on desks, cleaning staff with access outside business hours e.g., sensitive personal data being locked-up in cupboards, etc. A 'clean desk policy' should be used to prevent the above.

C.2.1.7 Updating, Patching and Change Control (A.12 Operation)
The data processor must ensure that system and software patches are deployed according to vendor recommendations on all systems and infrastructures that can provide services to the data controller, including internal workstations, applications and servers.

The data processor must perform rollout of security updates. Critical and Important security patches must be reviewed and installed as soon as possible.

C.2.1.8 Supplier Relationships (A.15 sub-processor relationships)

In case the data processor uses or plan to use a sub-processor:

Formal guidelines and procedures including relevant contractual measures covering the present criteria for the processing of personal data by a sub-processor should be in place before the processing takes place. If requested by the data controller, the documentation showing the sub-processor's compliance with these Clauses and/or the GDPR and/or relevant Member State legislation is made available to the data controller within a reasonable timeframe and without undue delay. These guidelines, procedures and contractual measures shall establish at least the same level of personal data protection and security as mandated in these Clauses.

C.2.1.9 Malware Protection (A.12 Operations security)
Updated malware protection must be installed and maintained on all the data processor's systems and hardware that are used in the processing of personal data on behalf of the data controller or are connected to systems or hardware administered by the data processor.

C.2.1.10 Backup (A.12 Operations security)
The data processor must have a documented backup policy and perform a backup of the data controller's systems and data. Data retention and data deletion requirements must be defined and handled in accordance with policies and procedures.

The data processor must implement procedures to verify backups by successfully re-establishing backed-up data, software, and systems at least every 6 months. Documentation must be available on request and included in KPI/reporting.

Backups must be protected from unauthorised access.

Backups must be encrypted and must be stored securely.

C.2.1.11 Logging and Monitoring (A.12 Operations security)
Logging of all access to personal data must take place. The access log must include the date and time of access, the UserID and the type of access (read, edit, delete, on sensitive data also view and search off data etc.).

Security logging must be enabled on all network equipment, servers and on all applications including databases and on IT system administrators – log files are to be timestamped and adequately protected against tampering and unauthorised access. Clocks should be synchronised to a single time source. Logs must be monitored – e.g. by setting up rules for alarms if logs show abnormalities that the data processor should react to.

A centralised system for collecting and reviewing security logs must as such be in place.

Logs of access to personal data and the use of personal data must be monitored and available for review in order to detect unauthorised access to personal data. It must be documented when and how often log files are reviewed and who has performed the control. Documentation must be available on request.

Failed login attempts must be logged and kept for 6 months in order to detect unauthorised access to personal data.

C.2.1.12 Network Security (A.13 Communications security)
The data processor must maintain network security using commercially available equipment and industry-standard techniques, including firewalls and intrusion detection systems.

The infrastructure must be segmented to at least separate production systems from test and development environments.

All personal data transmitted by the data processor must be encrypted while in transit and at rest.

C.2.1.13 Security Incident Management (A.16 Incident Management)
The data processor must implement procedures for quick and effective detection, analysis and handling of security events.

All security incidents and breaches related to services delivered to the data controller must be reported to the data controller without undue delay.

The data processor must implement the notification requirements outlined in the GDPR and provide the necessary information to the data controller within 24 hours.

C.2.1.14 Disaster Recovery and Business Continuity (A. 17 Information security aspects of business continuity management)
The data processor must implement a documented and tested disaster recovery plan and business continuity strategy covering the data controller's systems following an agreed service level.

Disaster recovery plans and business continuity strategies must be tested and updated regularly, and at least annually, to ensure that they are up-to-date and effective. Documentation must be available on request.

C.2.1.15 Data processing (C.7.3.8)

The data processor must be able to provide the data controller with a copy of all information processed by the data processor on a given data subject upon request in a structured, commonly used and machine-readable way

C.2.2 Solution Specific Security Requirements

C.2.2.1 Cloud Services
The processor shall perform a risk analysis of relevant cloud-based suppressors. The data processor's sub-processor agreements with eventual cloud providers, that form part of the solution, must be provided to the data controller upon request.

C.2.2.2 Application Lifecycle Security (A.14 Systems acquisition, development, and maintenance)
During the development lifecycle best practices, state of the art and well-acknowledged secure development practices, frameworks or standards should be followed meaning that the data processor must implement Data Protection by Design- and by Default principles in all phases of the data processing and system life-cycle. This includes that only relevant, proportional, and necessary information including use, disclosure, retention, transmission and disposal on individuals are collected for the application processing the data.

Personal data must not be used in the development or test environments without being anonymised, pseudonymised, scrambled or masked before use.

System development must take place in specialised development environments isolated from production and test systems and must be protected from unauthorised access.

Source code must be protected against unauthorised access and use.

The data processor must perform security reviews, vulnerability checks and penetration tests of all code and applications developed for the data controller before release. Periodic PEN tests should be performed and documented on web-facing applications.

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 is obliged to assist the data controller with its obligations set forth in this agreement without undue delay.

C.4. Storage period/erasure procedures
The data processors' authorisation to process personal data on behalf of the data controller is terminated when the Clauses or the license agreement is terminated, regardless.

Upon termination of the Clauses, the data processor and its sub-processors shall return and/or delete all personal data that the data processor has processed under the Clauses in accordance with Clause 14 above. The data controller may require documentation.

The data processor is however allowed to continue the processing of personal data up to one month after the termination of the Clauses, if the extent of data require a larger amount of work for the data processor. The data processor is in the same period entitled to let the personal data be part of the normal backup procedure. The data processors' treatment of personal data in this period is to be continued under the same instruction as described in the Clauses.

C.5. Processing location
The data processor's locations and the location of the data processor's sub-processors, are listed in Appendix B, B.1

Processing of the personal data under the Clauses cannot be performed at other locations than listed in Appendix B, B.1. Other/new processing locations will require prior notification by the data processor in accordance with Appendix B, B2 in the Clauses stating that the application of eventual new sub-processors (thereby eventually new processing locations) should be notified to the data controller at least 60 days before planned use.

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

C.6.1 The data processor may transfer data to a sub-processor approved in accordance with this agreement's clause 7.3.

C.6.2 The data processor shall secure a legal basis for transfer in accordance with the GDPR chapter V, without needing the data controller's signature. In these cases, the data processor is liable to secure the legality of the transfer basis.

C.6.3 In case of transfer of data to a third country, the data controller must be informed of this at least 30 days prior to the transfer occurring. Should the data controller not object to the transfer within this timeframe, the transfer will be approved in accordance with this agreement's clause 7.3.

If the data controller does not provide documented instructions pertaining to the transfer of personal data to a third country as instructed in these Clauses, 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 shall once a year at the data processor's own expense obtain an audit or certification report from an independent third party concerning the data processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The parties have agreed that the following type of audit and certification may be used in compliance with the Clauses:

ISAE3000

The approved report or certification shall, upon request, be submitted to the data controller, without undue delay, to prove compliance with the criteria stated in these Clauses.
The approved report or certification will also be available on www.samesystem.com.
The data controller may contest the scope and/or methodology of the report and may in such cases request a new audit/inspection under a revised scope and/or different methodology. The data processor is entitled to charge a reasonable hourly rate for the service regulated in Appendix D of these Clauses if the data controller demands other audits or/and certifications than stated in the above.

Based on the results of such an audit/inspection, the data controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The data controller or the data controller's representative shall in addition have access to inspect, including physically inspect, the places, where the processing of personal data is carried out by the data processor, including physical facilities as well as systems used for and related to the processing on behalf of the data controller. Such an inspection shall be performed when the data controller deems it required and where it has a concrete and relevant purpose.

C.8. Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors

The audit or certification as agreed in this appendix clause C.7 shall include the sub-processors used in the provided service in the scope of the audit or certification.

If the sub-processors are not part of the scope of the agreed audit or certification in C.7, the data processor shall once a year at the data processor's own expense obtain an audit or certification from an independent third party concerning the sub-processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses or perform a corresponding inspection of the sub-processor in accordance with the above standards or similar, as mentioned in clause C.7.

The approved report or certification shall, upon request, be submitted to the data controller, without undue delay, to prove compliance with the criteria stated in these Clauses. The data controller may contest the scope and/or methodology of the report and may in such cases request a new audit/inspection under a revised scope and/or different methodology. The data processor is entitled to charge a reasonable hourly rate for the service if the data controller demands other audits or/and certifications than stated in the above.

Based on the results of such an audit/inspection, the data controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The data processor or the data processor's representative shall in addition have access to inspect, including physically inspect, the places, where the processing of personal data is carried out by the sub-processor, including physical facilities as well as systems used for and related to the processing. Such an inspection shall be performed when the data processor (or the data controller) deems it required and where it has a concrete and relevant purpose.

Documentation for such inspections shall without delay be submitted to the data controller for information. The data controller may contest the scope and/or methodology of the report and may in such cases request a new inspection under a revised scope and/or different methodology where it has a concrete and relevant purpose.

The data controller may – if required – elect to initiate and participate in a physical inspection of the sub-processor. This may apply if the data controller deems that the data processor's supervision of the sub-processor has not provided the data controller with sufficient documentation to determine that the processing by the sub-processor is being performed according to the Clauses.

The data controller's participation in an inspection of the sub-processor shall not alter the fact that the data processor hereafter continues to bear the full responsibility for the sub-processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The data processor's and the sub-processor's costs related to physical supervision/inspection at the sub-processor's facilities shall not concern the data controller – irrespective of whether the data controller has initiated and participated in such inspection where it has a concrete and relevant purpose.

Appendix D) The parties' terms of agreement on other subjects

Regarding 9.2 and C.7

To the extent that the data controller requests the data processor's assistance with the services described in clause 9.2 (c) and (d), and in case the data controller demands other audits or/and certifications than stated above in Appendix C, clause C.7, the data controller is obliged to remunerate the data processor for the time used herewith at the hourly rates used by the data processor at any time.

Changes to the Data processing agreement

It is always the latest version of the data processing agreement that applies between the parties.

The data processor reserves the right to continuously make changes to, including clarifications of the agreement. These changes will typically be a result of new recommendations from e.g. The Data Protection Authority or the EU Commission as well as changes in practice and legislation in the area.

The Data Controller is therefore encouraged to sign up to receive notifications when there are changes to the agreement.

The Data Controller has, after receiving a notification about a change, 14 working days to object if the change cannot reasonably be accepted.

This provision does not apply to changes in the use of sub-data processors, which are regulated in section 7 of the agreement.