Standard Data Processor Agreement

Version January 2026

Prepared by

Date

Standard Contractual Clauses

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

between

[NAME]
CVR [CVR-NO]
[ADDRESS]
[POSTCODE AND CITY]
[COUNTRY]

(the data controller ("Partner"))

and

WorkPoint A/S
CVR 26082668
Esbjerg Brygge 28
6700 Esbjerg
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.

Table of Contents

1. Preamble

1.1   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.

1.2   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).

1.3   In the context of the provision of WorkPoint's end-user license agreement about software services (the "Service" or the "Services") the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

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

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

1.6   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.

1.7   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.

1.8   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.

1.9   Appendix D contains provisions for other activities which are not covered by the Clauses.

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

1.11   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.

2. The rights and obligations of the data controller

2.1   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 State1 data protection provisions and the Clauses.

2.2   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".

2.3   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.

3.   The data processor acts according to instructions

3.1   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.

3.2   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.

4.   Confidentiality

4.1   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.

4.2   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.

5.   Security of processing

5.1   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.

5.2   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:

5.3   Pseudonymisation and encryption of personal data;

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

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

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

5.4 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.

5.5 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.

5.6 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.

6. Use of sub-processors

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

6.2 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.

6.3 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 thirty (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.

6.4 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.

6.5 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.

6.6   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.

6.7   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.

6.8   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.

7.   Transfer of data to third countries or international organisations

7.1   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.

7.2   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.

7.3   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

7.4   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.

7.5   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.

8.   Assistance to the data controller

8.1   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

8.2   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.

8.3   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.

9.   Notification of personal data breach

9.1   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.

9.2   The data processor's notification to the data controller shall, if possible, take place within forty eight (48) 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.

9.3   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.
   c.   the likely consequences of the personal data breach;
   d.
   e.   the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

9.4   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.

10.   Erasure and return of data

10.1   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.

11.   Audit and inspection

11.1   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.

11.2   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.

11.3   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.

12.   The parties' agreement on other terms

12.1   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.

13.   Commencement and termination

13.1   The Clauses shall become effective on the date of both parties' signature.

13.2   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.

13.3   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.

13.4   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.

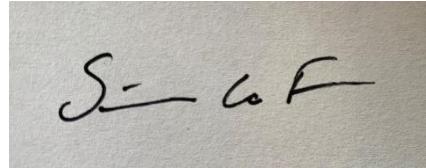## 14.   Signature

On behalf of the data controller

Name   [NAME]
Position   [POSITION]
Date   [DATE]
Signature   [SIGNATURE]

On behalf of the data processor

Name   Simone La Fontaine

Position	Data Protection Contact
Date	[DATE]
Signature	

15. Data controller and data processor contacts/contact points

15.1   The parties may contact each other using the following contacts/contact points:

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

Name	[NAME]
Position	[POSITION]
Telephone	[TELEPHONE]
E-mail	[E-MAIL]

Name	Simone La Fontaine
Position	Data Protection Contact
Telephone	+45 76 110 110
E-mail	dataprotection@workpoint.dk

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:
The parties have agreed that the data processor shall provide one or more of the following services as further described in the parties' agreement regarding the data processor's provision of Services to the data controller:

The purpose of the processing is to provide end-user license agreement about project document management software, developed by the data processor, to the data controller as Software-as-a-Service, hereafter referred to as "the Services", as further described in the parties' agreement regarding the data processor's provision of Services to the data controller. Including specific tasks ordered by the data controller.

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 provides services as further described in the parties' agreement regarding the data processor's provision of Services to the data controller, including end-user license agreement about project document management software, and ongoing operation, including monitoring and maintenance of the services to the end-user.

In specific situations, processing may include organisation, structuring, facilitation, temporary storage, filtration, troubleshooting, adaptation or alteration, retrieval, consultation, use, alignment, combination, restriction or erasure of personal data when so required in connection with the supply of the agreed Services, or if so required in order to comply with a request from the data controller.

A.3. The processing includes the following types of personal data about data subjects:
The data processor processes the types of personal data that the data controller directly or indirectly gives the data processor access to, which typically includes the following types of customer contact information:

General personal data (cf. Article 6 of the General Data Protection Regulation):
- Name of the contact person
- Company name
- Employment status (Employed or no longer employed)
- Position
- Department in the client company
- E-mail address
- Phone number
- Company address
- Company country
- IP-adress
- Email history

The data processor processes no types of personal data covered by Article 9 or Article 10 of the GDPR in regarding the data processor's provision of Services to the data controller.

A.4. Processing includes the following categories of data subject:
The data processor processes the categories of personal data that the data controller directly or indirectly gives the data processor access to, which typically includes the following categories of customer contact information:

- Partner contact persons (current, former, future)
- Customer contact persons (current, former, future)

- Partner users (current, former, future)
- Customer users (current, former, future)

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 data processor's processing of personal data on behalf of the data controller is performed when the parties' agreement regarding the data processor's provision of Services to the data controller comes into force and runs until terminated.

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. See list of sub-processors at Data Sub-Processors (workpoint365.com)

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. Notice for approval of sub-processors
The data processor's notice of any planned changes in terms of addition or replacement of sub-processors must be received by the data controller no later than thirty (30) days before the addition or replacement is to take effect, in so far this is possible.

Regardless of the above, the data controller accepts that there may be situations with a specific need for such change in terms of addition or replacement of sub-processors with a shorter notice or immediately. In such situations, the data processor will notify the data controller of such change as soon as possible.

If the data controller has any objections to such changes, the data controller shall notify the data processor thereof before such change is to take effect. The data controller shall only object to such changes if the data controller has reasonable and specific grounds for such refusal.

In case of the data controller's objection, the data controller furthermore accepts that the data processor may be prevented from providing all or parts of the agreed Services. Such non-performance cannot be ascribed to the data processor's breach. The data processor will maintain its claim for payment for such services, regardless if they cannot be provided to the data controller.

If it has been specifically agreed that the data processor cannot use sub-processors without the data controller's prior approval, the data controller accepts that this may mean that the data processor may be prevented from providing the Services. If the data controller has refused any changes in terms of addition or replacement sub-processors, non-provision of Services will not be considered a breach of the agreement regarding the data processor's provision of Services to the data controller that can be ascribed to the data processor in situations where non-performance may be ascribed to matters relating to a sub-processor.

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 takes place in accordance with the parties' agreement regarding the data processor's provision of Services to the data controller.

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:

Provision of IT services in accordance with the parties' agreement regarding the data processor's provision of Services to the data controller entered into between the parties.

C.2. Security of processing
The level of security shall reflect a generally high level of security reflecting the types of data being processed. The data processor has aligned its information security management system with the ISO 27001:2022 standard and have implemented and complies with technical and organisational controls in accordance with this standard.

In addition, the level of security shall take into account the specific agreed services in the parties' agreement regarding the data processor's provision of Services to the data controller:
The data processor shall initiate and implement appropriate security measures to protect the personal data provided against accidental or unlawful destruction, loss, alteration, unavailability, unauthorized disclosure of or access to the personal data. The data processor may change the implemented security measures on an ongoing basis, however, changes in security measures must never lead to a deterioration of the agreed security level.

In order to ensure an appropriate level of security, the data controller shall make the data protection impact assessment carried out by the data controller for the agreed processing available to the data processor, and the data controller shall regularly update this to the data processor.

The data processor is entitled and obliged to make decisions about the technical and organizational security measures to be implemented to establish the necessary (and agreed) security level.

The data processor shall however – in any event and at a minimum – implement the following measures that have been agreed with the data controller:

Organizational security
The data processor has a documented information security management system that addresses and describes how information security is implemented across the organization.

The data processor maintains and enforces policies for secure management and processing of information, including personal information, with the objective of ensuring that personal information is processed in accordance with applicable laws and regulations. The data processor has implemented appropriate measures to ensure that all employees are familiar with these policies and the guidelines and controls described within them. The data processor enforces regular mandatory training for all employees in both the GDPR and its practical implications along with training in information security.

The data processor has established an audit programme which includes annual audit and review of its policies relation to the implemented organizational and technical controls relating to access to data, including personal data.

With respect to the current technical level, implementation costs and the type, extend, context and purpose of the data processing of personal data, the data processor has implemented and enforces the principles of data protection throughout all phases of the lifecycle of the information and the systems processing it.

The data processor ensures that third party suppliers in scope of its information security management system conform to a set of minimum requirements, confidentiality agreements and controls as defined by the data processor.

The data processor supervises data sub-processors in accordance with the methodology developed by the Danish Data Agency as described in the "Guide on supervision of data processors" ("Vejledning om tilsyn med databehandlere") which includes a general assessment of the data sub-processors based on their processing activities, data categories, results from past inspections, and public information.

Physical security

All premises of the data processor are guarded by access restrictions; only employees of the data processor have access to the premises and all guests are logged and are not allowed to access the premise areas where personal data is processed or stored without supervision of an employee.

The data processor generally minimizes the amount of data, including personal data, which is kept in physical format at its premises. Any sensitive information – including personal data – is stored in locked areas only accessible to select and approved personnel. All physical copies of sensitive information, including personal data, is securely disposed of in accordance with industry practices once no longer required.

The data processor strives to only keep back-up information offsite of its physical premises. For back-up stored at any of the data processor's physical premises, the data is kept in secure areas only accessible to select and approved staff, and access to these areas are logged.

Access management

The data processor ensures that the personal information provided by the data controller is only accessible by approved personnel in accordance with the data processor's policies for access control. These policies follow the principle of least privilege regarding access to all data, including data stored online, and the policies and their implementation are reviewed frequently and audited annually. These policies also ensures that access is revoked once no longer necessary.

The data processor has implemented a process for changes to permission levels (including permission to accessing and working with data, including personal data) which includes requirements of management approval. This process is audited annually.

Systems which are used by the data processor to process personal information are secured through multifactor authentication. Multifactor authentication is also enforced for all remote access to data and infrastructure.

The data processor enforces the same requirements and principles regarding access to data, including personal data, to its employees regardless of whether the employee is working on premise or remotely.

The data processor has implemented encryption of all its online connections to ensure the protection of data during transmission.

Logging

The data processor enforces security logging on all network equipment, servers and applications including databases and IT-administration systems.

Back-up

The data processor (partly through third party back-up providers) carries out frequent back-up of its data (including personal data). The data processor has described procedures for how to restore data from its back-up providers, and this is reviewed frequently.

Access to back-up data is restricted to only authorized personnel.

Availability

The data processor strives to utilize cloud-based solutions as far as reasonably possible to manage personal data in order to ensure that physical or onsite technical issues will have a minimum of impact on the data processor's ability to access personal data.

The data processor has implemented procedures for efficient detection, analysis, and management of security incidents in order to ensure availability of data, including personal information.

The data processor has implemented a strategy for business continuity and processes for data recovery in the event of an incident, which covers systems used for processing personal information. The data processor regularly tests its security incident response plan to ensure effectiveness and that involved personnel are trained and ware of necessary actions to take.

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:

At the specific request of the data controller, the data processor shall, taking into account the nature of the processing, assist the data controller as far as possible, by appropriate technical and organizational measures, in fulfilling the data controller's obligation to respond to requests to exercise the rights of the data subjects as laid down in the GDPR.

If a data subject makes a request to the data processor to exercise his or her rights, the data processor shall notify the data controller thereof without undue delay.

Taking into account the nature of the processing and the information available to the data processor, the data processor shall make reasonable efforts, upon specific request, also assist the data controller in ensuring compliance with the data controller's obligations in relation to

- Implementation of appropriate technical and organizational measures
- Security breaches
- Notification of personal data breaches to the data subject
- Conducting impact assessments
- Prior consultations with supervisory authorities.

C.4. Storage period/erasure procedures

The data controller holds personal data processed by the data processor on behalf of the data controller. Thus, personal data made available for the data processor's processing will be stored until erased by the data controller or until termination of the Services relating to processing of personal data.
Upon termination of the personal data processing service, the data processor shall either delete or return the personal data in accordance with clause 11.1. Information about the data controller's contact persons shall be deleted in accordance with the same deletion deadlines that data processor has established for its customers.

Personal data about potential customers and partners shall be stored for as long as necessary and deleted no later than 6 months after the potential customer has expressed that the customer is not interested or after the last interaction with the customer.

Personal data about existing customers is stored for as long as necessary and until the customer relationship ends and deleted in accordance with the time limits for former customers.

Personal data about former customers is stored for as long as necessary and deleted no later than 3 years after the end of the customer relationship. However, information for bookkeeping purposes is stored for up to 5 years from the end of the financial year to which the invoice relates in accordance with the Danish Bookkeeping Act.

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:

The processing of personal data takes place at the data processor's addresses as well as the listed data processors and the addresses of their sub-processors. In addition, remote work may be carried out in accordance with the data processor's remote work policy as well as the current and future locations of the data processor and the sub-processor. Sub-processor means current sub-processors and any additions or replacements, taking into account the conditions for the data controller's approval of the sub-processor as set out in Clause 7 and Appendix B of the Clauses.

C.6. Instruction on the transfer of personal data to third countries
The data controller has authorised and thereby instructed the data processor to transfer personal data to a third country as further specified below. In addition, by subsequent written notification or agreement the data controller can provide instructions or specific consent pertaining to the transfer of personal data to a third country.

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.6.1 General approval of transfer of personal data to secure third countries
With the Clauses, the data controller provides a general and prior approval (instructions) for the data processor to transfer personal data to third countries if the European Commission has laid down that the third country/the relevant area/the relevant sector has a sufficient level of protection.

For transfers to organisations in the United States, certified under the EU-U.S. Data Privacy Framework ("DPF"), the data processor has an obligation to ensure that sub-processors used under the Clauses meets the requirements under the DPF-framework and have the necessary certification.

C.6.2 Approval of transfer to specific recipients of personal data in third countries subject to appropriate safeguards
The data controller has by signing the Clauses approved the use of the above-mentioned sub-processor(s) as indicated in the table in Appendix B.1 and instructed the data processor to transfer personal data to third countries for the delivery of the Services. Furthermore, the data processor shall be authorized to transfer personal data to third countries when this is required by the actions of the data controller.

The legal basis for transferring personal data to third countries is the EU Commission's Standard Contractual Clauses in force (SCC), which are concluded between the data processor and the above-mentioned sub-processor(s) in Appendix B.1. The data processer will be considered as the data exporter and the sub-

processor as the data importer. When personal data is transferred to the above-mentioned sub-processor(s), both parties agree to be obligated by the obligations in accordance with the SCC. The data processor and/or any sub-processor(s) are entitled to enter into SCC with the relevant sub-processor(s).

In case the EU Commission completes new SCC's subsequent to the formation of the SCC, the data processor and/or any sub-processor(s) is authorized to renew, update and/or use the SCC's in force from time to time.

The content of this instruction and/or the Clauses will not be considered as a change of the content of the SCC.

C.7. Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor
Pursuant to Articles 24 and 28 of the General Data Protection Regulation, the data controller is entitled and obliged to monitor the data processor's processing of personal data on behalf of the data controller. The data controller's monitoring of the data processor may consist in one of the following actions from the data controller:
- Self-checking based on documents provided to the data controller by the data processor,
- written inspection, or
- physical inspections.

C.7.1 Self-checks
The data controller may ask control questions to the data processor and, upon request, gain access to a number of documents for use in conducting self-monitoring, including
- A description of physical and organisational security measures with the data processor.
- IT-security policy

C.7.2 Written inspection and physical inspection
The data controller may choose to carry out inspections either as a written inspection or as a physical inspection. The inspection may be carried out by the data controller itself and/or in cooperation with a third party. An inspection must be based on the security measures agreed between the parties and may be performed subject only subject to a reasonable prior notice.

Procedure and reporting of written inspection or physical inspection:

- The controller shall contact the data processor by e-mail to dataprotection@workpoint-dk with a request to carry out an audit and/or inspection.
- In the case of written audits, the data controller must inform the data processor of this without undue delay.
- In the case of physical audits and/or inspections, the data controller shall agree the date of the audit and/or inspection in advance with the data processor.
- The data processor shall confirm receipt and provide the final date for conducting the audit and/or inspection.
- The performance of the audit and/or inspection takes place.
- The data controller prepares a report, which is subsequently forwarded to the data processor.
- The data processor will review the draft report and provide any comments to the data controller's observations (can be repeated several times).
- The final report is concluded by the data controller.
- The inspection is ended.

C.8. Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors
Based on the methodology developed by the Danish Data Agency as described in the "Guide on supervision of data processors" ("Vejledning om tilsyn med databehandlere"), the data processor will carry out audits,

including inspections, of sub-processors' processing of personal data either by self-monitoring audit statements and similar statements (if possible), written or physical inspection, or a combination hereof.

Appendix D   The parties' terms of agreement on other subjects

D.1 In general
In relation to the data processor's processing of personal data on behalf of the data controller, the parties have agreed on the regulation of other matters and special regulation as specified in this Appendix D.

In the event of any discrepancy between the Clauses and Appendix D, Appendix D shall prevail.

The Clauses take precedence over any corresponding regulation in service agreements between the parties regarding the part of the data processor's activities and responsibilities relating to the data processing in the Clauses, while the performance of all other activities relating to the provision of agreed services is subject to the other parts of the agreement relating to the provision of the services.

D.2 Consequences of the data controller's illegal instructions
The data controller is aware that the data processor depends on the data controller's instructions to which extent the data processor is entitled to use and process personal data on behalf of the data controller. Consequently, the data processor is not liable for any claims arising from the data processor's acts or omissions to the extent such acts or omissions is a direct data processing activity exercised in accordance with the data controller's instructions.

D.3 Implementation of other security measures
The data processor is entitled to implement and maintain other security measures than what has been specified in the parties' agreement regarding the data processor's provision of Services to the data controller and Appendix C.2, however, provided that such other security measures as a minimum provide the same level of security as the prescribed security measures.

D.4 - Provisions on third party beneficiaries in relation to sub-processors
The parties have agreed that clause 7.6 of the Clauses (as listed below) shall not apply between the parties.

The following text is therefore deleted from the Clauses:
"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."

D.5 Use of sub-processors supplying on standard terms
Regardless of clause 7 it is emphasized that if the data processor uses a sub-processor, who provides services on its own terms, which the data processor cannot deviate from, the sub-processor's terms for such processing performed by such sub-processor will apply. With the Clauses, the data controller accepts and instructs that such specific processing activities are based on the sub-processor's terms.

D.6 Remuneration

D.6.1 Assistance
The data processor is entitled to payment for assistance provided pursuant to clause 9 of the Clauses. Such payment is calculated on the basis of the time spent and the agreed hourly rates in the agreement regarding the data processor's provision of Services to the data controller, and if no hourly rates have been agreed, the

data processor's current hourly rates will be applied, with the addition of any cost paid, including also cost to be paid by the data processor for the assistance of sub-processors.

If the data processor's assistance leads to claims for increased security measures to be observed in relation to agreement regarding the data processor's provision of Services to the data controller and Appendix C, the data processor will, as far as reasonably possible, implement such additional security measures pursuant to further agreement with the data controller, provided that the data processor receives payment for such work.

D.6.2 Implementation of other security measures
If the data controller's claim or the data processor's ongoing evaluations lead to increased requirements for such security measures compared to the agreement regarding the data processor's provision of Services to the data controller, the data processor will introduce and implement such additional security measures pursuant to further agreement with the data controller, provided that the data processor receives payment for such work.

The data controller may request the data processor's assistance in connection with erasure of personal data.

D.6.3 Inspection and audit
The data processor is entitled to payment for the data controller's inspection and audit. Such payment is calculated on the basis of the time spent and the agreed hourly rates in the agreement regarding supply of Services, and if no hourly rates have been agreed, the data processor's current hourly rates will be applied, with the addition of any cost paid, including also cost to be paid by the data processor for the assistance of sub-processors.

D.7 Liability and breach
Any breach of the Clauses will be regulated and processed in accordance with the parties' agreement regarding the data processor's provision of Services to the data controller.

If the data processor has paid compensation and/or other amounts to a data subject based on Article 82 of the General Data Protection Regulation or section 26 of the Danish Liability for Damages Act (in Danish *"Erstatningsansvarsloven"*) the data controller must remedy the data processor for the paid amount, which exceeds the agreed limitation of liability in the parties' agreement regarding the provision of Services. The parties have thus contractually agreed to deviate from the Article 82(5) of the General data Protection Regulation and section 26 in the Danish Liability for Damages Act.

The parties agrees that according to Article 82(5) of the General Data Protection Regulation, a party who has paid damages to an injured party may have a claim for recourse pursuant to the principle in Article 82(5), regardless of whether the paid amount is corresponding to full damages,

For any compensation related to other non-financial loss to data subjects, the principle in Article 82 shall also apply in regard to the internal allocation of responsibility between the data processor and the data controller.

A party cannot make a claim for recourse or damages towards the other party for fines or other penalties awarded pursuant to Section 41 of the Danish Data Protection Act (in Danish *"databeskyttelsesloven"*) and for penalties accepted pursuant to Section 42 of the Danish Data Protection Act.