

# TimeControlOnline

## Master Subscription Agreement Addendum

**Dated: December 7, 2018**



### **HMS Software**

189 Hymus, Suite 402  
Pointe-Claire, QC H9R 1E9, Canada  
+1 514 695 8122  
[www.TimeControl.com](http://www.TimeControl.com)  
[info@hms.ca](mailto:info@hms.ca)

**Table of Contents**

Addendum ..... 1

Definitions ..... 1

Scope of this Addendum ..... 2

Roles and Scope of Processing ..... 2

Details of Data Processing: ..... 2

Sensitive Personal Data ..... 2

Sub-Processing ..... 3

Security Measures and Security Incidence Response ..... 3

Audit Reports ..... 3

Transfers of Personal Data ..... 4

Return or Deletion of Data ..... 4

Cooperation ..... 4

General ..... 4

Language of Agreement ..... 5

Signed ..... 5

Annex A ..... 6

    TECHNICAL AND ORGANISATIONAL SECURITY MEASURES TO BE IMPLEMENTED BY HMS ..... 6

    Data Privacy objectives and measures ..... 7

    Data Privacy Structures at the Data Importer ..... 7

ANNEX B ..... 11

    MODEL CLAUSES ..... 11

        1. Definitions ..... 11

        2. Details of the transfer ..... 12

        3. Third-party beneficiary clause ..... 12

        4. Obligations of the data exporter ..... 12

        5. Obligations of the data importer ..... 13

        6. Liability ..... 14

        7. Mediation and jurisdiction ..... 14

        8. Cooperation with supervisory authorities ..... 14

        9. Governing Law ..... 14

        10. Variation of the contract ..... 14

        11. Subprocessing ..... 15

        12. Obligation after the termination of personal data processing services ..... 15

## Addendum

This Data Processing Addendum ("ADDENDUM") is effective as of the 7th of May, 2018, forms part of the TimeControl Online Master Subscription Agreement ("Agreement") between Client and Heuristic Management Software Inc. ("HMS Software", "HMS") and applies where, and to the extent that, HMS Software processes Personal Data on behalf of Client when providing the Service under the Agreement. All capitalized terms not defined in this ADDENDUM shall have the meanings set forth in the Agreement.

## Definitions

**"HMS Software"** shall mean Heuristic Management Software Inc., a Canadian federally incorporated company headquartered at 189 Hymus, Suite 402, Pointe Claire, Quebec H9R 1E9 Canada

**"HMS"** shall mean Heuristic Management Software Inc., a Canadian federally incorporated company headquartered at 189 Hymus, Suite 402, Pointe Claire, Quebec H9R 1E9 Canada

**"Affiliate"** means an entity that directly or indirectly Controls, is Controlled by or is under common Control with HMS Software.

**"Agreement"** means the TimeControl Online Master Subscription Agreement.

**"Control"** means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the entity in question. The term "Controlled" will be construed accordingly.

**"EU Data Protection Law"** means (i) prior to 25 May 2018, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of Personal Data and on the free movement of such data ("Directive"); and (ii) on and after 25 May 2018, Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation) ("GDPR").

**"Data Protection Laws"** means all data protection and privacy laws applicable to the processing of Personal Data under the Agreement, including, where applicable, EU Data Protection Law.

**"Model Clauses"** means the Standard Contractual Clauses for Data Processors as approved by the European Commission in Decision 2010/87/EU and in the form set out in Annex B.

**"Processing"** has the meaning given to it in the GDPR and "process", "processes" and "processed" will be interpreted accordingly.

**"Sub-processor"** means any Data Processor engaged by HMS Software or its Affiliates to assist in fulfilling its obligations with respect to providing the Service pursuant to the Agreement or this ADDENDUM. Sub-processors may include third parties or members of the HMS Software Group.

**"Data Controller"** means an entity that determines the purposes and means of the processing of Personal Data.

**"Data Processor"** means an entity that processes Personal Data on behalf of a Data Controller.

**"Group"** means any and all Affiliates that are part of an entity's corporate group.

**"Personal Data"** means any information relating to an identified or identifiable natural person.

**"Privacy Shield"** means the EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield Framework self-certification program operated by the U.S. Department of Commerce and approved by the European Commission pursuant to Decision C(2016)4176 of 12 July 2016 and by the Swiss Federal Council on January 11, 2017, respectively.

**"Security Incident"** means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Client Data.

## Scope of this Addendum

**Scope of ADDENDUM:** This ADDENDUM applies where and only to the extent that HMS Software processes Client Data on behalf of Client in the course of providing the Service to the Client pursuant to the Agreement.

## Roles and Scope of Processing

**Role of the Parties:** As between HMS Software and Client, Client is the Data Controller of Client Data and HMS Software shall process Client Data only as a Data Processor acting on behalf of Client.

**Client Processing of Client Data:** Client agrees that (i) it will comply with its obligations as a Data Controller under Data Protection Laws in respect of its processing of Client Data and any processing instructions it issues to HMS Software; and (ii) it has provided notice and obtained (or will obtain) all consents and rights necessary for HMS Software to process Client Data pursuant to the Agreement and this ADDENDUM.

**HMS Software Processing of Client Data:** As a Data Processor, HMS Software will process Client Data only for the purpose of providing the Service and in accordance with Client's documented lawful instructions, as set forth in the Agreement and this ADDENDUM. The parties agree that the Client's complete and final instructions with regard to the nature and purposes of the processing are set out in this ADDENDUM. Processing outside the scope of these instructions (if any) will require prior written agreement between Client and HMS Software with additional instructions for processing.

**Third Party Platform:** Client may utilize optional features or functionality, in Client's sole discretion, provided by third party service providers ("Third Party Platform") in the course of using the Service. Client acknowledges that Third Party Platform will be Data Processor in respect of any Personal Data provided to the Third Party Platform by the Client. For clarity, such Third Party Platform is not a Sub-processor of HMS Software and not subject to the provisions of this ADDENDUM. In the case of Third Party Platform, once the Personal Data has left HMS Software systems and is under the processing responsibility of such Third Party Platform, HMS Software has no further responsibility for such Personal Data under this ADDENDUM.

## Details of Data Processing:

**Subject matter:** The subject matter of the data processing under this ADDENDUM is the Client Data.

**Duration:** As between HMS Software and Client, the duration of the data processing under this ADDENDUM is the term of the Agreement.

**Purpose:** The purpose of the data processing under this ADDENDUM is the provision of the Service to the Client.

**Nature of the processing:** HMS Software provides a cloud-based timesheet system called "TimeControl Online" ("Platform") which enables its Clients to collect and harness time data, and other such professional services as described in the Agreement. HMS Software processes Client Data upon the instruction of Client in accordance with the terms of the Agreement.

**Categories of data subjects:** Employees, contractors, agents, advisors, freelancers (past, potential, present and future) of Client (who are natural persons); prospects, Clients, business partners, and vendors of Client (who are natural persons).

**Types of Client Data:** First and Last name, email, job title, time spent on work related tasks, time spent on personal time

## Sensitive Personal Data

**Prohibited Data:** Client shall not disclose (and shall not permit any data subject to disclose) any Sensitive Personal Data to HMS Software, including but not limited to information submitted through custom field extensions within the Platform, for processing that are not expressly disclosed in Details of Processing Section above. Where Sensitive Personal Data is nevertheless submitted within Client Data, Client acknowledges that in such cases it shall be in breach of the Agreement (including this ADDENDUM) and accepts full responsibility for any subsequent liability arising from unauthorized or unlawful processing of the Sensitive Personal Data.

## Sub-Processing

**Authorized Sub-processors:** Client agrees that in order to provide the Service, HMS Software may engage Sub-processors to process Client Data. HMS has engaged Amazon and its EC2 Platform as a storage and processing infrastructure for TimeControl Online.

**Sub-processor Obligations:** Where HMS Software authorizes any Sub-processor as described below

- HMS Software will restrict the Sub-processors access to Client Data only to what is necessary to assist HMS Software in providing or maintaining the Service, and will prohibit the Sub-processor from accessing Client Data for any other purpose;
- HMS Software will enter into an agreement with the Sub-processor imposing data protection terms that require the Sub-processor to protect the Client Data to the standard required by Data Protection Laws and;
- HMS Software will remain responsible for its compliance with the obligations of this ADDENDUM and for any acts or omissions of the Sub-processor that cause HMS Software to breach any of its obligations under this ADDENDUM.

HMS Software will provide Client with at least 30 days' notice to clients if it intends to make any changes to its Sub-processors. Client may object in writing to HMS Software's appointment of a new, or replacement of an old, Sub-processor within ten (10) calendar days of such notice, provided that such objection is based on reasonable grounds relating to data protection. In such event, the parties will discuss such concerns in good faith with a view to achieving resolution. If this is not possible, Client may suspend or terminate the Agreement (without prejudice to any fees incurred by Client prior to suspension or termination).

## Security Measures and Security Incidence Response

**Security Measures:** HMS Software has implemented and will maintain appropriate technical and organizational security measures to protect Client Data from Security Incidents and to preserve the security and confidentiality of the Client Data ("Security Measures"). The Security Measures applicable to the Service are set forth in Annex A, as updated or replaced from time to time in accordance with Section below entitled "Updates to Security Measures".

**Updates to Security Measures:** Client acknowledges that the Security Measures are subject to technical progress and development and that HMS Software may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Service purchased by the Client.

**Personnel:** HMS Software restricts its personnel from processing Client Data without authorization by HMS Software as set forth in the Security Measures and shall ensure that any person who is authorized by HMS Software to process Client Data is under an appropriate statutory or contractual obligation of confidentiality.

**Client Responsibilities:** Notwithstanding the above, Client agrees that except as provided by this ADDENDUM, Client is responsible for its secure use of the Service, including securing its account authentication credentials, protecting the security of Client Data when in transit to and from the Service and taking any appropriate steps to securely encrypt or backup any Client Data uploaded to the Service.

**Security Incident Response:** Upon becoming aware of a Security Incident, HMS Software will notify Client without undue delay and will provide information relating to the Security Incident as it becomes known or as is reasonably requested by Client. HMS Software will also take reasonable steps to mitigate and, where possible, to remedy the effects of, any Security Incident.

## Audit Reports

**Audit Reports:** HMS Software audits its compliance against data protection and information security standards on a regular basis. Such audits are conducted internally using the standards set by OWASP (<https://www.owasp.org>) Upon Client's request, HMS Software will provide Client with details of the audits it conducts relevant to the Service it is providing to Client.

**Confidentiality of Audit Reports:** The Client acknowledges that each Report will constitute HMS Software's Confidential Information and will protect the Report in accordance with the confidentiality provisions of the Agreement.

In addition to HMS Software's audits, additional information about HMS Software's sub-processor, Amazon EC2 including their certificates from 3rd party audits can be found at <https://aws.amazon.com/security>. Amazon, has successfully completed multiple SAS70 Type II audits, and now publishes a Service Organization Controls 1 (SOC 1), Type 2 report, published under both the SSAE 16 and the ISAE 3402 professional standards as well as a Service Organization Controls 2 (SOC 2) report. In addition, AWS has achieved ISO 27001 certification, and has been successfully validated as a Level 1 service provider under the Payment Card Industry (PCI) Data Security Standard (DSS). In the realm of public sector certifications, AWS has received authorization from the U.S. General Services Administration to operate at the FISMA Moderate level, and is also the platform for applications with Authorities to Operate (ATOs) under the Defense Information Assurance Certification and Accreditation Program (DIACAP).

## Transfers of Personal Data

**Data center locations:** Unless by mutual agreement between Client and HMS Software, HMS Software will maintain all Client data in its Sub-Processor Data Center in the United States which is subject to Privacy Shield regulations. Client may elect to have all data hosted in a client center in one of several data centers in other countries for a fee. HMS will provide a list of potential Data Center Locations at the request of Client. Under no circumstance will Personal Data be moved by HMS to any other country without the express consent of Client.

## Return or Deletion of Data

Following expiration of the Agreement, HMS Software shall delete or return to Client at Client's choice all Client Personal Data in its possession in accordance with the terms of the Agreement save to the extent HMS Software is required by applicable law to retain some or all of the Client Personal Data (in which case, HMS Software shall implement reasonable measures to isolate the Client Data from any further processing).

## Cooperation

The Service provides Client with a number of controls that Client may use to retrieve, correct, delete, or restrict Client Data, which Client may use to assist it in connection with its obligations under the GDPR, including its obligations relating to responding to requests from data subjects or applicable data protection authorities. To the extent that Client is unable to independently access the relevant Client Data within the Service, HMS Software shall (at Client's expense) provide reasonable cooperation to assist Client to respond to any requests from individuals or applicable data protection authorities relating to the processing of Personal Data under the Agreement. In the event that any such request is made directly to HMS Software, HMS Software shall not respond to such communication directly without Client's prior authorization, unless legally compelled to do so. If HMS Software is required to respond to such a request, HMS Software will promptly notify Client and provide it with a copy of the request unless legally prohibited from doing so.

If a law enforcement agency sends HMS Software a demand for Client Data (for example, through a subpoena or court order), HMS Software will attempt to redirect the law enforcement agency to request that data directly from Client. As part of this effort, HMS Software may provide Client's basic contact information to the law enforcement agency. If compelled to disclose Client Data to a law enforcement agency, then HMS Software will give Client reasonable notice of the demand to allow Client to seek a protective order or other appropriate remedy unless HMS Software is legally prohibited from doing so.

To the extent HMS Software is required under EU Data Protection Law, HMS Software will (at Client's expense) provide reasonably requested information regarding the Service to enable the Client to carry out data protection impact assessments and prior consultations with data protection authorities as required by law.

## General

The parties agree that this ADDENDUM shall replace and supersede any existing ADDENDUM (including the Model Clauses (as applicable)) the parties may have previously entered into in connection with the Service.

Except for the changes made by this ADDENDUM, the Agreement remains unchanged and in full force and effect, including, but not limited to, the mutual indemnities provided by the parties. If there is any conflict between this ADDENDUM and the Agreement, this ADDENDUM shall prevail to the extent of that conflict.

For the avoidance of doubt, any claim or remedies the Client may have against HMS Software, any of its Affiliates and their respective employees, agents and sub-processors arising under or in connection with this ADDENDUM, including: (i) for breach of this ADDENDUM; (ii) as a result of fines (administrative, regulatory or otherwise) imposed upon Client; (iii) under EU Data Protection Law, including any claims relating to damages paid to a data subject; and

(iv) breach of its obligations under the Model Clauses, will be subject to any limitation of liability provisions (including any agreed aggregate financial cap) that apply under the Agreement. Client further agrees that any regulatory penalties incurred by HMS Software in relation to the Client Data that arise as a result of, or in connection with, Client's failure to comply with its obligations under this ADDENDUM or any applicable Data Protection Laws shall count toward and reduce HMS Software's liability under the Agreement as if it were liability of the Client under the Agreement.

No one other than a party to this ADDENDUM, their successors and permitted assignees shall have any right to enforce any of its terms.

Any claims against HMS Software or its Affiliates under this ADDENDUM shall be brought solely against the entity that is a party to the Agreement. In no event shall any party limit its liability with respect to any individual's data protection rights under this ADDENDUM or otherwise.

This ADDENDUM and the Model Clauses will terminate simultaneously and automatically with the termination or expiry of the Agreement.

The provisions of this ADDENDUM are severable. If any phrase, clause, or provision is invalid or unenforceable in whole or in part, such invalidity or unenforceability shall affect only such phrase, clause or provision, and the rest of this ADDENDUM shall remain in full force and effect.

This ADDENDUM will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.

## Language of Agreement


The parties have expressly requested that this agreement be written in the English language. Les parties ont expressément demandé que ce contrat soit rédigé en langue anglaise.

## Signed

IN WITNESS WHEREOF, the parties have caused this ADDENDUM to be executed by their authorized representative effective as of the 7<sup>th</sup> of May 2018.

Heuristic Management Systems Inc.

Client: \_\_\_\_\_

By:  \_\_\_\_\_

By: \_\_\_\_\_

Name: Chris Vandersluis

Name: \_\_\_\_\_

Title: President

Title: \_\_\_\_\_

## Annex A

These Annexes ("ANNEXES") form a part of the TimeControl Online Service Agreement Addendum ("Addendum") between Client and Heuristic Management Software Inc. ("HMS Software", "HMS") and applies where, and to the extent that, HMS Software processes Personal Data on behalf of Client when providing the Service under the Agreement. All capitalized terms not defined in this ANNEX shall have the meanings set forth in the Agreement.

### TECHNICAL AND ORGANISATIONAL SECURITY MEASURES TO BE IMPLEMENTED BY HMS

#### **Entry control:**

Refusing permission to unauthorized personal to access the data processing systems used to process or use personal data.

#### **Admission control:**

Preventing data processing systems from being used by unauthorized persons.

#### **Access control:**

Ensuring that the data can only be accessed by persons who are authorized to do so.

#### **Input control:**

Ensuring that the data have been input correctly, to the extent the data importer inputs such data.

#### **Order control:**

Ensuring that data required for an order are processed in accordance with the relevant instructions.

#### **Disclosure control:**

Ensuring the security of personal data against loss or unauthorized access if they are disclosed or transferred.

#### **Availability control:**

Ensuring that the data are protected from destruction and loss.

#### **Separation control:**

Ensuring that data collected for different purposes are processed separately.

#### **Entry control:**

Refusing permission to unauthorized personal to access the data processing systems used to process or use personal data.

#### **Admission control:**

Preventing data processing systems from being used by unauthorized persons authorized to do so.



**Input control:**

Ensuring that the data have been input correctly, to the extent the data importer inputs such data.

**Order control:**

Ensuring that data required for an order are processed in accordance with the relevant instructions.

**Disclosure control:**

Ensuring the security of personal data against loss or unauthorized access if they are disclosed or transferred.

**Availability control:**

Ensuring that the data are protected from destruction and loss.

**Separation control:**

Ensuring that data collected for different purposes are processed separately.

Persons employed in data processing shall not collect, process or use personal data without authorization.

**Data Privacy objectives and measures**

The data importer has implemented stringent data privacy structures within the company. This structures ensure adequate data privacy with the measures required by applicable privacy laws.

- Organization
- Entry
- Admission
- Access
- Transmission of data
- Input of data
- Commissioned data processing
- Data availability
- Data separation

The specific details regarding the technical and organizational measures are explained below.

**Data Privacy Structures at the Data Importer****A. OBJECTIVES**

The data importer is addressed by a variety of national and European regulations. Data Privacy is a key competence of the data importer. The data importer has implemented certain measures in order to protect the personal data of its customers. The measures in place are based on internal guidelines, customer requests and the European Data Protection Directive 95/46/EC.

**B. ORGANISATIONAL CONTROL**

Measures, which comply with the specific requests of Data Protection, regarding the internal organization:

- Commitment of employees to confidentiality
- Disaster recovery plan
- Data back-up concept (for production data)
- Regulations regarding the correct and secure processing of duties done by data processing
- Control of compliance with the regulations

- Organizational, spatial and/or personal separation of data processing from other business units and other customers
- Regulations and instructions for entry control
- Regulations and instructions for admission control
- Regulations and instructions for access control
- Regulations and instructions for transport of data storage media and transmission control
- Regular information and instruction of the employees
- Description of activities in working instructions
- Data deletion concept
- External Certifications for data privacy audit
- Documentation of IT-procedures, software, IT-configuration

## **C. ENTRY CONTROL**

Measures to limit entrance of unauthorized persons to areas where personal data is used or processed with electronic data processing devices.

- Entry control
- Regulations and instructions of entry control
- Camera monitoring
- Identification badges / code cards
- Entry regulations organization for employees
- Entry regulations for third parties
- Classification of security areas
- Identification of admission authorized persons
- Safeguarding by alarm system, intrusion detector, police emergency call
- Security locks with centralized key administration and master key plan
- Revision secure organization of admission rights
- Revision secure grant and revocation of admission rights

## **D. ADMISSION CONTROL**

Measures to limit admission of unauthorized persons to systems where personal data is used or processed with electronic data processing devices.

- Safeguarding of physical network infrastructure
- Firewall for internal networks against external vulnerabilities
- Control of use for electronic data processing
- Regulations and instructions of admission control
- Control and identification of authorized persons
- Logging of use for entry rights
- Admission only with User-ID and password only
- Separation of function principle when granting entry authorization
- Identification of terminal or terminal user (e.g.: login with user-ID and password)
- Automatic screensaver protection in case of inactivity
- Lockable terminals and decentralized IT-systems
- Safeguarding of electronic data processing systems correspondent with the requirements
- Functional and/or timely limited use of terminals

## **E. ACCESS CONTROL (ELECTRONIC DATA PROCESSING)**

Measures to limit access of unauthorized persons to systems where personal data is used or processed with electronic data processing devices.

- Regulations and instructions for access control
- Processes for file organization
- Rights- and role-concept
  - Assignment of rights for data-input as well as for information, modification and deletion of stored data
  - Regulated procedure for granting, changing and revocation of access rights
  - Selective access regulations for procedures, operation control tickets
  - User adaptive access protection

- Selective access for files and functions
- Automatic screensaver protection in case of inactivity
- Requirement of user identifiers (Passwords) for files, system data, application data
- Machine control of authorizations
- Logging access to specific data (e.g.: Console log, machine log)
- Functional and/or timely limited use of terminals
- Password policy at the level of configuration of IT-systems
- Identification and authentication of users
- Control of administrator activities
- Limitation of free style queries in data bases (excluding administrators)
- Safeguards for access by self-acting organizations
- Use of encryption

## **F. ACCESS CONTROL (DATA MEDIA)**

Measures to limit access of unauthorized persons to data and/or applications being stored on storage devices outside of an electronic data processing system.

- Identification of authorized personnel
- Rules regarding the production of copies
- Labelling obligation for data media with classification
- Guidelines for the organization of data storage
- Data privacy conform elimination of out of use data media with protocol
- Controlled storage of in use and swapped out data media in a secure area (systems and discs)
- Definitions of areas which are suitable or scheduled for the storage of data media (e.g.: disc; volume)

## **G. TRANSMISSION CONTROL**

Measures to ensure that personal data cannot be read, copied, modified or removed without authorization during electronic transmission or transport.

Measures to ensure and that it is possible to check and establish to which bodies the transfer of personal data by means of data transmission facilities is envisaged.

Measures to ensure, that an automated procedure for the retrieval of personal data is running a log procedure in order to have retrospect information which data has been retrieved by whom.

- Determination of authorized person for transmission and transport
- Documentation of the retrieval and transmission programs
- Determination and documentation of the transmission procedure and the data receivers
  
- Protocol of data transmission and receivers
- Regulations and instructions for data media transport and transmission control
- Secured data lines
- Use of cryptographic procedures as far as useful or mandatory

## **H. INPUT CONTROL**

Measures to ensure that it is possible to check and establish whether and by whom personal data / social data have been entered, modified or removed into/from data processing systems.

- Automatic protocol of input, modification and deletion of personal data
- Protocol of system generation and modification of system parameters
- Complete protocol of all instances
- Revision secure protocol of access rights
- Protocol data can be analyzed in computer assisted processes
- Proof of the organizational defined responsibilities for input of data
- Definition of deletion and retention periods

## **I. JOB CONTROL**

Measures to ensure that, in the case of commissioned processing of personal data, the data are processed strictly in accordance with the instructions of the principal.

The following measures are relevant in case of sub-order for the subcontractor as well.

- Careful selection of the contractor (processor)
- Written agreement based on statutory mandatory law
- Evaluate the principal and contractor in regard to
  - Data security measures
  - Data location
  - Transmission directives
  - Retention- and deletion periods
  - Breach
- Definition of safety measures
- Evaluate control of security measures at the subcontractor
- Control of the correct execution of the contract

## **J. AVAILABILITY CONTROL**

Measures to ensure that personal data is protected from accidental destruction or loss (e.g.: loss of power, lightning, protection from water damage)

- Ordinance of work instructions and safety directives
- Fire preventions
- Definition and control of fire precautions and fire/water early warning system
- Risk- and weak-point-analysis for relevant IT-division
- Safeguarding of the electric power supply by uninterruptable power supply
- Regular instruction of all employees
- Disaster recovery plan
- Recovery Procedures for production data
- Data mirroring
- Regular data back up
- Storage of back up media in safeguarded locations for production data
- Instructions for documentation of procedures and software development
- Centralized procurement for hardware and software
- Database-Logging

## **K. SEPARATION CONTROL**

Measures to ensure that data collected for different purposes can be processed separately

- Company internal directives for data collection, data processing and use of data
- Grant of specific access rights
- Use of separate user roles to ensure separation control
- Use of pseudonyms as far as possible and reasonable
- Documentation of data bases
- Documentation of application programs
- Documentation of the specific purposes of the collection, processing and use of data
- Logical separation of data

## ANNEX B

---

### MODEL CLAUSES

Standard Contractual Clauses (processors)

Name of the data exporting organization:

The entity identified as the "data exporter"

(the data exporter) And

Name of the data importing organization: Heuristic Management Systems Inc.

Address: 189 Hymus, Suite 402, Pointe Claire, QC H9R 1E9

Tel: 514-695-8122

Email: chris.vandersluis@hms.ca

(the data importer)

each a "party"; together "the parties".

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified.

### 1. Definitions

For the purposes of the Clauses:

'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

'the data exporter' means the controller who transfers the personal data;

'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any

other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

'technical and organizational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

## 2. Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable forms an integral part of the Clauses.

## 3. Third-party beneficiary clause

3.1 The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

3.2 The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3.3 The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3.4 The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

## 4. Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organizational security measures in this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, and a summary description of the security measures, as well as a copy of any contract for sub processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

## 5. Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organizational security measures specified before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorized access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

## 6. Liability

6.1 The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

6.2 If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

6.3 The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

6.4 If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

## 7. Mediation and jurisdiction

7.1 The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

- (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
- (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

7.2 The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

## 8. Cooperation with supervisory authorities

8.1 The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

8.2 The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

8.3 The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

## 9. Governing Law

The Clauses shall be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.

## 10. Variation of the contract



The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

## **11. Subprocessing**

11.1 The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

11.2 The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

11.3 The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.

11.4 The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

## **12. Obligation after the termination of personal data processing services**

12.1 The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.