GENERAL TERMS ON COMPLIANCE ASSURANCE FOR INFORMATION SOLUTIONS AND INFORMATION SERVICES FOR CLIENTS

1 INTRODUCTION

Article 1

(1) These General terms by company Halcom d.d. (hereinafter: General terms) define the conditions of the partnership cooperation and the rights and obligations of the contractor, supplier Halcom d.d. (hereinafter: Halcom or contractor or processor) and the buyer or client (hereinafter referred to as the client or controller) relating to the data protection (personal data, trade secrets), compliance of processes and solutions, and other areas to ensure compliance with applicable Slovenian and European legislation as well as international and European technical standards and recommendations. These General terms apply to clients who have a contract with Halcom for the purchase of a license, installation and maintenance of an electronic banking software product from the Hal E-Bank family of solutions (Hal E-Bank/B2B, Hal E-Bank/Personal, Hal E-Bank/Corporate, Hal E-Bank/WEB Retail, Hal E-Bank/WEB Corporate, Hal E-Bank/SMS, etc.) or the use of OneSign solution.

(2) The provisions of these General terms define the rights and obligations of the controller and the processor when the processing of personal data takes place in the name and on behalf of the controller. The provisions have been drafted in order to ensure that the parties comply with the provisions of Article 28 (3) of Regulation (EU) 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). The purpose of these provisions is to protect the rights of individuals, mitigate the specific risks to the protection of personal data and ensure transparency in the relationship between the controller and the processor regarding their rights and obligations. Where the controller and the processor rely only on parts of the provisions of these General terms, they shall not be considered to rely entirely on the provisions of the General terms.

(3) These General terms are contractual in nature and form an integral part of the contractual relationship between the parties and legally bind them. By entering into a contract with Halcom d.d. the client declares that he is completely and fully familiar with these General terms. The provisions of these General terms shall take precedence over other similar provisions contained in other agreements between the parties, unless the parties in the contract agree otherwise on individual issues, if this is necessary. The provisions do not exclude the liability of the parties for their obligations under the General Data Protection Regulation or other legislation.

(4) Details of the processing of personal data not covered by the provisions of these General terms, including the purpose and nature of the processing, the types of personal data, the categories of data subjects and the duration of processing, the controller's conditions regarding the use of sub-processors by the processor and the list of sub-processors, approved by the controller, the controller's instructions on the processing of personal data, the minimum set of data security requirements and a description of the course of audits on the operation of the processor and sub-processors and provisions on other activities not covered by these provisions are regulated by contract.

(5) The provisions of the General terms shall be kept by both parties in writing, including in electronic form. Halcom delivers a copy of these General terms to the client at the time of contract signing. The current version of the General terms is also always available at Halcom's seat.

Article 2

(1) The parties agree to guarantee conditions and measures to ensure the protection of personal data and prevent any abuse in accordance with the regulations on personal data protection.

(2) Halcom declares that it has a registered data processing activity according to the standard classification of activities or other relevant activity required by the applicable data protection regulations as a condition for performing contractual processing of personal data.

(3) Halcom will contractually process personal data as part of the provision of its services in the name and on behalf of the client in accordance with the valid Slovenian and European laws, international and European standards, and other professional rules, these General terms, and the Client's instructions.

Article 3

(1) In these General terms the party, which reveals certain information is called the "Disclosing party" and the party receiving this information, the "Receiving party".

(2) "Confidential Information" under these General terms are all trade secrets and information of commercial, financial and technical nature as well as any other information that the Disclosing party marks as confidential and are prepared in any form, including software, analyzes, tables, data, studies or other documents prepared by the receiving party under or in respect of confidential information. As confidential informations are also considered all documents held by the receiving party prepared on the basis of such information, or that contain, or are completely or partially prepared on the basis of such information.

2 AUTHORITY FOR PROCESSING DATA

Article 4

(1) The controller is responsible for ensuring that the processing of personal data takes place in accordance with the provisions of the General Data Protection Regulation (see Article 24 of the General Data Protection Regulation), the Union or the member state law governing the protection of personal data and these General terms.

(2) The controller has the right and obligation to determine the purposes and means of personal data processing.

(3) The controller shall be responsible, inter alia, for ensuring that there is a valid legal basis for the processing of personal data entrusted to the processor.

Article 5

The client authorizes Halcom to process personal data in accordance with the terms of these General terms which are an integral part of the contractual relationship.

Data set:

a. data on proxies in bank accounts, including personal name, address of residence, tax number, e-mail address, telephone number, serial number of the identification mean and other data regarding the proxy, authentication, and authorizations;
b. activities, messages, and documents of proxies in the electronic bank (connection time, IP address, identification mean, performed actions and forwarded messages or documents in the electronic bank);
c. activities, messages, and documents of the bank (connection time, IP address, identification mean, received messages or documents in the electronic bank);
d. audit trails (time of activity, personal or username, data on activity or entry, change, or access to data).

Purpose of processing: provision of payment services and other services between the client and one or more commercial banks, ensuring the efficiency of the operation of services and ensuring information security and other tasks in accordance with these General terms.

Processing time: in accordance with applicable regulations - 10 years from the transaction according to the regulations on the prevention of money laundering and terrorist financing; 3 or 5 years, depending on the obligatory limitation period from the termination of the contractual relationship between the client and the bank, limited by the duration of the contractual relationship under the contract and these General terms. In accordance with the regulations on data protection, the statute of limitations, and the criminal limitation period, audit trails are kept for 6 years from the day of an individual information event, measure, or transaction.

Location of personal data processing: The processing of personal data in accordance with these General terms may not take place in locations other than the following without the prior written consent of the controller:

- At the registered office of the personal data processor and other locations under the control of the personal data processor (Ljubljana, Slovenia).

Unless otherwise provided by the provisions of these General terms or the contract, and unless the controller subsequently provides documented instructions regarding the transfer of personal data to third countries, the processor is not entitled to transfer personal data to third countries under these provisions.

Article 6

(1) The processor will process personal data only on the basis of documented instructions from the controller, unless required to do so by the Union or member state law applicable to the processor. The instructions are specified in these General terms. The parties may agree otherwise on individual issues in the contract, if this is necessary.

(2) The controller may give further instructions throughout the processing of personal data, whereby the instructions will always be documented and in writing, including electronically, in accordance with these provisions. In the event that the processor considers that the controller's instructions violate the General Data Protection Regulation or the provisions of Union or member state law on the protection of personal data, it will immediately inform the controller.

Article 7

(1) Halcom shall process personal data solely to the extent and only for the purposes and within the period as specified in the authorization referred to in the article 5 and in strict compliance with these General terms.

(2) The processor and, where applicable, the processor's representative shall, in accordance with the provision of the second paragraph of Article 30 of the General Data Protection Regulation, keep records of all types of processing activities carried out in the name and on behalf of the controller.

(3) The processor undertakes to delete all personal data processed in the name and on behalf of the controller upon termination of the provision of personal data processing services and to assure to the controller that he

has done so. Upon termination of the contractual relationship or at any time at the request of the client, Halcom shall ensure the erasure or blocking of personal data received or processed on the basis of authorization from the article 5.

(4) The processor undertakes to return all personal data to the controller and delete existing copies of personal data upon termination of the provision of personal data processing, unless further storage of personal data is required by Union or member state law. Upon termination of the contractual relationship or at any time at the request of the Client, Halcom shall ensure the return to the client all or part of the personal data received or processed on the basis of authorization from the article 5 in accordance with the provisions of the General terms.

(5) Halcom may not condition obligations under this Article in any way and shall execute them regardless of the status of the contract, any disputes with the client, or any outstanding obligations of the client. Halcom may deny fulfillment of obligations only if required by law or legal act or decision of the European Union at least equivalent to national law.

3 BUSINESS SECRETS

Article 8

The Disclosing party is the sole owner and holds all intellectual property rights regarding any confidential information shared with the Receiving party. Sharing of the confidential information shall not constitute any transfer or grant of any such rights regarding such information to the Receiving party.

Article 9

(1) Obligations set out in these General terms shall not apply to confidential information where:

- the Receiving party already possesses before having it received from the Disclosing party;
- such information becomes public for another reason than due to a breach of these General terms;
- such information is independently developed by the Receiving party;
- the Receiving Party may based on the prior express written authorization from the Disclosing party share such information with a third party;
- such information is received from a third party without similar restrictions and not in breach of these General terms;
- such information is disclosed by the Receiving party to comply with the request from the competent court or another government body.

(2) When disclosing confidential information to government bodies the Receiving party shall notify the other party before releasing the information so that the Disclosing party may take all necessary measures for adequate protection of its rights in relation to the requested confidential information. The Receiving party shall, in any case, release the Confidential information to the government body only to the extent as required by law and shall try its best to obtain non-disclosure agreement or other adequate assurance that the information submitted shall be treated confidentially.

(3) With the exception of the points mentioned above the obligations under these General terms shall remain in effect even after the attainment of the business purpose or termination of the contractual relationship for any reason.

Article 10

(1) The parties shall disclose confidential information to each other to the extent necessary to achieve the common business purpose. The parties agree that the confidential information belonging to the other party shall not be disclosed to a third party, whether a natural person, firm, company, association or any other entity for any reason or purpose.

(2) The parties may disclose confidential information to their employees to the extent needed for performance of their duties.

Article 11

(1) The parties agree that they shall not without the prior express written consent of the Disclosing party use the confidential information or exploit it in any other way except to achieve the stated common business purpose.

(2) The Receiving party shall restrict its employees access to confidential information and disclose only the information necessary for their duties. Confidential information shall not be shared with other parties if this is not expressly stated in these General terms.

Article 12

(1) The Disclosing party may at any time request in writing the return of any written confidential information disclosed in accordance with these General terms and any eventual copies, together with a written statement by the Receiving party that it has not consciously retained in its possession or under its control - directly or indirectly - any confidential information or copies thereof. The Receiving party shall comply with such a request in 8 (eight) days after receipt of such a request.

(2) Such part of the confidential information, composed only of analysis, charts, studies or other documents prepared for the Receiving party, as is not returned under these General terms to the Disclosing party shall be destroyed by the Receiving party on request of Disclosing party and its destruction confirmed to the Disclosing party in writing.

Article 13

Each party represents and warrants to the other party that it is established and operates in accordance with the applicable laws of the country in which it is established. Each party confirms that it is legally executing these General terms and shall carry out all necessary activities related to the implementation of these General terms. The Disclosing party warrants that by providing confidential information it does not violate any other agreement with third parties.

4 PERSONNEL SECURITY

Article 14

(1) The processor will provide access to personal data processed in the name and on behalf of the controller only to those persons under the control of the processor who have committed themselves to confidentiality or are duly legally committed to confidentiality and only according to the demonstrated need for access to data. The list of persons who have access to personal data will be regularly reviewed. On the basis of regular checks,

access to personal data will be suspended if it is no longer necessary, thus making personal data no longer accessible to the persons concerned.

(2) At the request of the controller, the processor will demonstrate that the persons concerned, under the control of the processor, are bound by the above stated confidentiality requirements and have access to the data only when there is a need for access to personal data.

(3) Halcom shall ensure that the processing of personal data involves only its reliable employees who:

- were properly checked during recruitment procedures and continuously during employment;
- are contractually or by a way of declaration, legally required to protecting sensitive data;
- adequately trained for their tasks and their knowledge and skills continuously maintained.

(4) Halcom shall only allow employees access to personal data or confidential information, which is essential for their work in relation to the tasks under the contract in accordance with these General terms. Halcom shall also ensure that all sensitive tasks are properly managed, and their implementation separated (segregation of duties) with critical tasks requiring the joint action of at least two authorized and trained employees (four-eyes principle) and measures in place to prevent any one of the employees to alone endanger the security and integrity of personal data or confidential information.

(5) The parties also agree that confidential information, but not necessarily personal data, may be disclosed to their professional advisors, agents and consultants, provided that such a person signs a nondisclosure agreement providing the same terms and conditions contained in these General terms.

(6) The provisions of the preceding paragraphs shall apply mutatis mutandis to external associates or employees of subcontractors if cooperation with them is approved by the client.

5 TECHNICAL SECURITY

Article 15

(1) Article 32 of the General Data Protection Regulation provides that, taking into account the latest technological developments and implementation costs and the nature, scope, circumstances and purposes of the processing, as well as the risks to the rights and freedoms of individuals, that differ by probabilty and seriousness, the processor shall ensure an adequate level of security in relation to the risk by implementing appropriate technical and organizational measures.

(2) The controller will assess the risks to the rights and freedoms of individuals caused by the processing of personal data and implement measures to mitigate these risks. These measures shall, as appropriate, include the following measures:

a. pseudonymization and / or encryption of personal data;
b. the ability to ensure the continued confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to recover in a timely manner the availability and access to personal data in the event of a physical or technical incident;
d. the process of regular testing, evaluation and evaluation of the effectiveness of technical and organizational measures to ensure the security of processing.

(3) In accordance with the provisions of Article 32 of the General Data Protection Regulation, the processor will also - independently of the controller - assess the risks to the rights and freedoms of individuals arising

from the processing of personal data entrusted to it by the controller and apply mitigation measures. To this end, the controller will provide the processor with all necessary information to identify and assess such risks.

(4) The processor will assist the controller in ensuring compliance with the controller's duties under Article 32 of the General Data Protection Regulation, inter alia by providing information concerning technical and organizational measures already provided by the processor under the provisions of Article 32 of the General Data Protection Regulation, together with any other information necessary for the controller to ensure compliance with the provisions of Article 32 of the General Data Protection Regulation.

(5) To the extent that subsequently - according to the controller's assessment - mitigation of identified risks would require additional measures to be provided by the processor, given the measures already provided by the processor in accordance with Article 32 of the General Data Protection Regulation, the controller will specify in the contract additional measures to be provided.

Article 16

(1) The parties agree to protect received confidential information by the same standards of information security used to protect their own confidential information and to manage confidential information in such a way as to prevent unauthorized disclosure thereof.

(2) Halcom shall for tasks under the contract and these General terms use internationally renowned software or established open source solutions and the services by renowned and tested suppliers (service quality, technological competence, financial strength, etc).

(3) Halcom shall have an effective information security system in place in accordance with international standards (ISO 27001), which is proven by regular independent external audits and a valid certificate.

(4) For any key tasks under the contract and these General terms, which may significantly affect client's interests or personal data protection, Halcom shall use subcontractors in accordance with the provisions of Article 18 of these General terms.

(5) Halcom shall be required to keep an information resources inventory (information resources, threat levels, security measures, responsible persons, etc.) and up to date documentation on all important activities, key equipment settings, user credentials, equipment inventory, and contacts for each location.

(6) All hardware maintenance work shall be carried out at the location where the equipment is located. When this proves impossible, the data media shall be removed from equipment and safely stored. If data can not be removed or otherwise protected the whole maintenance process shall be specially controlled. The equipment shall be security screened after maintenance work and before being put back into service.

Article 17

Halcom provides security and data retention in accordance with its internal regulations and security policies, which provide all the necessary organizational, technical, and logical-technical procedures and measures to ensure information security and personal data protection.

Internal regulations or security policies cover at least the following obligations:

- Halcom shall ensure that all premises housing an information system or its components, data backups or personal data on physical or electronic media are physically or electronically protected;
- Halcom shall provide physical and electronic security of all hardware, system and application software, including the input-output devices and safety of personal data in physical or electronic form in accordance with the principles of information security;

- Halcom shall ensure operational security (electronic protection and network security, application security, audit trails, etc.);
- Halcom assures identity and access management (authorizations, identities and key management, encryption, authentication, audit trail);
- Halcom provides resource management (inventory information resources, authorization, and resources management responsibilities, strict segregation of resources or at least data pertaining to different clients);
- Information system provides an effective way to erase personal database on the decision of the client, the competent government bodies or valid laws and regulations;
- Halcom and the client shall jointly ensure secure data transfer and prevent unauthorized access to personal data during transfer, including the transfer by use of public telecommunications resources and (obligatory encryption);
- Halcom shall prevent unauthorized access to personal data on physical media format by using at least these security measures:
    - data media containing personal data is not left unattended in open areas or equipment or any other places accessible to unauthorized persons,
    - all printed data shall be safely removed from the printer,
    - waste paper and other discarded media containing personal data shall be destroyed in a way that prevents recovery of all or part of destroyed data; the same requirement applies to any support material;
    - data media containing personal data shall not be discarded in garbage bins, but instead securely destroyed;
- ensure compliance with all other obligations arising from the provisions on the data protection regulations, the contract, and these General terms.

6 SUBCONTRACTORS

Article 18

(1) When using the services of other processors (sub-processors), the processor will comply with the requirements set out in paragraphs 2 and 4 of Article 28 of the General Data Protection Regulation.

(2) For the performance of contractual tasks involving the processing of personal data, Halcom may hire subcontractors, provided that as a processor it will not use the services of other processors (sub-processors) to meet the provisions of these General terms without prior general written permission of the controller.

(3) The processor has the general permission of the controller to use the services of sub-processors. The processor will notify the controller in writing at least 30 days in advance or in writing of the intended changes regarding the use of the services of additional or other sub-processors or a significant change in the contractual relationship with the existing subcontractor, prior to the commencement of the tasks, thus enabling the controller to oppose such changes before using the services of the sub-processors concerned. A longer period for prior notification of the sub-processors concerned may be specified in the contract. A list of sub-processors already approved by the controller can be found in the appendix to the contract. If the client/controller does not object in writing within 8 days of receiving the notification, it is considered that he agrees with the selected sub-processor.

(4) For any the tasks under these General terms, which do not include the processing of personal data, Halcom may hire subcontractors at its own discretion.

Article 19

(1) Where a processor employs another processor to carry out specific processing activities on behalf of the controller, that other processor shall be subject to the same data protection obligations as set out in these General terms and shall be enforced by contract or other legal act in compliance with Union or Member State law, in particular to provide sufficient guarantees for the implementation of appropriate technical and organizational measures in such a way that the processing complies with the requirements of these General terms and the General Data Protection Regulation.

(2) The processor is responsible for the requirement that the sub-processor fulfills at least the obligations that apply to the processor in accordance with these General terms and the General Data Protection Regulation. Halcom shall guarantee for any tasks performed by subcontractors as performed by Halcom itself.

(3) A copy of the sub-processing agreement and subsequent amendments will be submitted to the controller at the request of the controller, giving the controller the opportunity to ensure that the same personal data protection requirements as these General terms apply to sub-processor as well. Contractual provisions on business aspects of sub-processing that do not affect the legal content of personal data protection in the sub-processing agreement do not need to be submitted to the controller.

(4) In the event of bankruptcy of the processor, the controller will become a creditor under the sub-processing contract and will have the right to enforce the contract to the sub-processor employed by the processor (the controller has the right to instruct the sub-processor regarding deletion or return of personal data).

(5) If the sub-processor fails to fulfill its obligations regarding the protection of personal data, the processor shall remain fully liable to the controller regarding the fulfillment of the obligations of the sub-processor. This does not affect the exercise of the rights of individuals under the General Data Protection Regulation - in particular as regards the rights set out in Articles 79 and 82 of the General Data Protection Regulation - to the controller and the processor, including the sub-processor.

7 TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES AND INTERNATIONAL ORGANIZATIONS

Article 20

(1) Any transfer of personal data to third countries (i. e. countries outside the European Economic Area) or an international organization by the processor shall take place solely on the basis of documented instructions from the controller and shall always comply with the provisions of Chapter V of the General Data Protection Regulation.

(2) In the case of transfers of personal data to third countries or international organizations where the processor has not been instructed to do so by the controller or required by Union or Member State law applicable to the processor, the processor shall inform the controller of the relevant legal requirement. unless that legislation prohibits such information on important grounds in the public interest.

(3) A processor without documented controller instructions, e.g. the approval of the controller or a specific requirement of Union or Member State law applicable to the processor may not, under these General terms:

- transfer personal data to a controller or processor in a third country or international organization;

- transfer personal data to a sub-processor in a third country or international organization;
- enable the processing of personal data by a processor in a third country or an international organization.

(4) The instructions of the controller regarding the transfer of personal data to third countries, including, where appropriate, the method of transfer under the provisions of Chapter V of the General Data Protection Regulation on which the transfer of personal data is based, shall be defined by these General terms.

(5) The provisions of these General terms may not be equated with standard contractual provisions within the meaning of Article 46 (2) (c) and (2) (d) of the General Data Protection Regulation and the parties may not rely on the provisions of these General terms as a tool for the transmission of data under Chapter V of the General Regulation.

8 CHANGE MANAGEMENT

Article 21

Changes in information solutions, or documentation may under these General terms result from:

- improvements or introductions of new IT solutions, which relate to the contract and these General terms,
- error or bug fixes in information solutions, which relate to the contract and these General terms,
- organizational changes, affecting the solutions that are the subject to the contract and these General terms, or
- pertinent changes in applicable laws and regulations, that affect the solutions that are subject to the contract and these General terms.

Article 22

(1) The development, test, and production IT environments related to these General terms shall be completely separated.

(2) Any change in information solutions, or documentation related to the contract and these General terms shall be first tested solely in the development environment and only with imaginary data or publicly accessible digital content. Any change must be documented in such a way to indicate the new version, to identify any reasons for changes and all implemented essential changes, and determine the place of storage of the new and previous versions.

(3) All previous versions of IT solutions and documentation shall be securely stored.

(4) Real data shall never leave the production environment and may not be transferred to any other environment or distributed to any other party without the explicit legal basis and explicit consent of all contractual partners and end-customers to whom the data relate, and after all aspects have been analyzed to ensure such action is in accordance with all applicable laws and regulations.

Article 23

(1) Before installing the new version of the respective IT solutions Halcom shall with the client:

- provide installation instructions and plan for any possible problems while installing and operating the system;

- successfully test the new version in the test environment and appropriately document such test,
- append, or change project documentation in accordance with changes made.

(2) New versions of IT solutions, subject to the contract and these General terms, shall be installed only after all the tasks from the preceding paragraph are successfully and properly implemented.

(3) New versions of IT solutions, subject to the contract and these General terms, shall be installed based on mutually agreed conditions by both parties.

Article 24

(1) Prior to the installation of new IT solutions or application support services, subject to the contract and these General terms, or installation changes to existing IT solutions, the responsible project manager shall determine all the necessary activities related to training and informing of employees and customers.

(2) Both contractual parties shall jointly assure that all employees or customers are appropriately and effectively informed of new IT solutions or modifications thereof.

9 BUSINESS CONTINUITY

Article 25

(1) Halcom shall provide a valid business continuity plan, which aims to ensure the contractually defined operation of services and 24/7 provision of data protection to the client, to establish procedures to prevent interruption of business activities continuing operations, to ensure the smooth operation of a specific service, describe the procedures in case of failure of the service and ensure compliance with applicable laws and these General terms.

(2) The plan should be based on risk assessment made and the obligations under the contract and the General terms with the proposal of measures to reduce these risks in the event of possible incidents.

(3) The plan must contain at least the following topics:

- the existence of the crisis group, which must assume the management in case of an emergency and to take major decisions and actions that periodically meets with the aim of preventive review of the Business Continuity Plan and its update;
- provided the first steps in the event of an emergency and determination of cause and effect;
- communication plan in case of emergencies;
- mandatory periodic testing of the business continuity plan (at least once a year or every time a major change of processes, equipment, or risk exposure; mandatory operational rules of testing, failure simulation of the entire primary location; recovery operation at the primary location).

10 PROVISION OF INFORMATION AND INCIDENT REPORTING

Article 26

(1) Taking into account the nature of the processing, the processor will assist the controller, by appropriate technical and organizational measures, as far as possible in fulfilling his obligations to respond to the data subject's rights under Chapter III of the General Data Protection Regulation. This means that the processor will, as far as possible, assist the controller in fulfilling the controller's obligations relating to:

a. the right to be informed about the processing of personal data when personal data are obtained from the data subject
b. the right to be informed about the processing of personal data where 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. right to erasure ("right to be forgotten")
f. the right to restriction of processing
g. the obligation to notify in connection with the correction or deletion of personal data or the restriction of processing
h. the right to data portability
i. the right to object
j. the right of the data subject not to be subject to a decision based solely on automated processing, including profiling.

(2) In addition to the processor's obligation to assist the controller in fulfilling the controller's obligations in accordance with the first paragraph of Article 19 of these General terms, the processor shall, taking into account the nature of data processing and information available to the processor, assist the controller regarding:

a. the obligation of the controller to inform the competent supervisory authority (Information Commissioner of the Republic of Slovenia) about the data breach without undue delay and, as far as possible, no later than 72 hours after being informed of the data breach, unless it is unlikely that the personal data breach pose a risk to the rights and freedoms of individuals;
b. the obligation of the controller to inform the data subject without undue delay that a personal data protection breach has occurred where the breach of personal data protection is likely to pose a significant risk to the rights and freedoms of individuals;
c. the controller's obligation for the controller to carry out, before processing, an assessment of the impact of the intended processing operations on the protection of personal data (data protection impact assessment) where the type of processing is likely to pose a significant risk to individuals' rights and freedoms;
d. the obligation of the controller to consult the supervisory authority (Information Commissioner of the Republic of Slovenia) before processing, when the impact assessment related to data protection shows that the processing would cause a high risk if the controller did not take risk mitigation measures.

(3) The parties shall determine with these General terms the appropriate technical and organizational measures with which the processor must assist the controller, including the subject and scope of the necessary assistance. The stated requirement refers to the obligations provided for in the provisions of these General terms in the first and second paragraphs of Article 29.

Article 27

(1) Halcom shall, at the request of the client or the competent national authorities in relation to the tasks or data processed under these General terms, always within a reasonable time prepare and submit a report on the functioning of the information system, the data processing or prepare data extracts for the protection of legal interests of the client or the client's clients or third parties.

(2) Unless otherwise agreed, the client shall pay the cost of such reports or data printouts from the previous article and previous paragraph of this article at its own request or at the request of a competent national authority by man / hours.

Article 28

(1) Halcom shall monitor and record every information security event (incident), which means any event that has or may have resulted in:

- unavailability of the system or part thereof or services,
- disclosure of confidential information or the loss or unauthorized changes to the data,
- damage to or loss of equipment and facilities, or
- other action that violates security policies or procedures.

(2) Halcom shall ensure that authorized and trained employees respond to any information security event and take all necessary measures to prevent the fallout from the incident and future such events.

(3) Halcom shall report to the client any information on security incidents, that could have serious consequences.

(4) If a special report is required and unless otherwise agreed, the client shall pay the cost of such reporting of the incident referred to in the previous paragraphs on the basis of his request or the request of the competent state authority by man / hours, unless the incident occurred due to reasons on the part of Halcom.

Article 29

(1) In the event of a personal data breach, the processor shall, without undue delay after learning of the security breach, officially notify the controller of the personal data breach.

(2) As far as possible, the processor shall notify the controller of the security breach no later than 48 hours after learning of the security breach in order to enable the controller to fulfill its obligations to notify the supervisory authority of the personal data breach in accordance with Article 33 of the General Data Protection Regulation.

(3) In accordance with point (a) of the second paragraph of Article 26 of these General terms, the processor will assist the controller in informing the competent supervisory authority about personal data breach, which means that the processor is obliged to obtain the information listed below, that shall be in accordance with the provisions of Article 33 of the General Data Protection Regulation set out in the controller's notification to the competent supervisory authority:

- the nature of the personal data breach, possibly also the categories and approximate number of data subjects concerned, and the types and approximate number of personal data records concerned;
- the likely consequences of a personal data breach;
- the measures to be taken by the controller or proposed by the controller to address the personal data breach, as well as, where appropriate, measures to mitigate any adverse effects of the breach.

(4) The parties shall with these General terms specify all the elements that the processor must provide in providing assistance to the controller in informing the competent supervisory authority about the personal data breach.

11 AUDIT

Article 30

(1) The client has the right to audit Halcom's actions under the contract and these General terms and/or compliance with applicable European and Slovenian legislation, international standards and recommendations and industry best practices. The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the General Data Protection Regulation and these General terms, and shall allow the controller or other auditor authorized by the controller to carry out audits, including inspections, and cooperate in them.

(2) For this purpose, Halcom ensures operations in accordance with the ISO / IEC 27001 standard, which is verified once a year by an independent external audit and Halcom proves it at the request of the client with a valid ISO / IEC 27001 certificate.

(3) The procedures relating to the performance of audits, including inspections of the processor and sub-processors by the controller, shall be specified in the contract.

(4) The processor undertakes to provide access to premisses and means of processing that takes place at processor to supervisory authorities that have access to the controller's and processor's premises and processing facilities in accordance with the relevant legislation, or representatives acting on the basis of the authorization of such supervisory authority, on the basis of appropriate identification.

12 REGULATORY OBLIGATIONS AND CONTRACT MANAGEMENT

Article 31

(1) Halcom shall upon request of the client ensure the participation of its employees and to provide all necessary documents for any client's needs related to enforcement of legal rights or interest and any internal or external audit procedure or supervision by competent national authorities and judicial, arbitration or similar dispute resolution procedures.

(2) Unless otherwise agreed, the client shall pay the price of such assistance by spent man / hours, except in cases where the incident occurred due to reasons under Halcom's control.

Article 32

(1) Halcom shall carry out all processing tasks in such a manner as to ensures that the client is able to transfer data back into its own applications or to another contractor. To this end, the client and Halcom joint working group shall agree the details of data export, data transfer action plan, and other related measures.

(2) After completion of each processing, if so agreed, or at the termination of contract Halcom shall surrender all data and processing results to the client and after the confirmation of a successful data transfer by the client delete or block such data and shall not process personal data in any other way.

13 COMMUNICATION BETWEEN THE PARTIES

Article 33

(1) All messages, requests or other communications relating to the contractual relationship shall be in writing. Communication affecting the validity of the contractual relationship shall be delivered in person or sent by registered post with acknowledgement of receipt or electronically by e-mail, the acceptance of which must be confirmed by the addressee by return e-mail, through the trust service provider or with a proof of receipt signed by a qualified electronic signature, addressed to the party or parties at the official address or address specified in the contract or address communicated by that party.

(2) In the event that the date of receipt cannot be established, the date of receipt shall be deemed to be on the 8th day after the date of the sending postmark.

(3) Each party will designate in the contract the person responsible for the implementation of the provisions of these General terms and the contacts or contact points through which the parties may inform each other. The parties undertake to keep each other informed of changes in contacts or contact points.

14 LIABILITY

Article 34

(1) Halcom shall in accordance with applicable laws of Republic of Slovenia be liable for any unauthorized disclosure of personal data or confidential information belonging to the other party and received under these General terms to achieve the agreed common business purpose. If the client or another person for whom the client is responsible is also to blame for the damage or aggravation of Halcom's position, Halcom's liability shall be reduced proportionately. Halcom is not liable for damage caused by the customer in fulfilling these General terms or the contractual relationship.

(2) In no case shall Halcom assume any material liability for indirect damage resulting from the incorrect operation of Halcom's information solution, which has been accepted by the client to operate in its production environment.

(3) Halcom's liability for damages is, regardless of the basis of liability for damages, limited in amount to the amount paid by the client to Halcom for services in the period of 3 months prior to the occurrence of the loss event.

(4) The client shall in such case request from the contractor the payment of a calculated sum of actual damage or contractual penalty and contractor shall pay the amount within 15 (fifteen) days after receiving such justified request.

(5) The parties shall consider request justified if it is accompanied by the relevant evidence, which indicates that the Receiving party or the contractor acting as processor has breached the provisions of these General terms.

Article 35

(1) Neither party is liable for damages due to delays and / or errors in the provision of services under these General terms or the contractual relationship, if such delay or error occurred due to circumstances beyond the control of either party, including in particular, but not exclusively, the following examples:

- restrictions and measures taken by public authorities,

- wars, riots, and other social upheavals,

- earthquakes, floods or other natural disasters and catastrophes,

- other reasons beyond the control of either party.

(2) A contracting party who, due to the occurrence of force majeure, cannot partially or fully fulfill its obligations under these General terms or the contractual relationship, must immediately, and no later than within two working days from the day of learning of force majeure, notify in writing the other party on the occurrence of force majeure, the expected duration and possible consequences of force majeure and provide it with evidence of its occurrence.

15 FINAL PROVISIONS

Article 36

(1) The provisions of these General terms for each contractual relationship shall enter into force on the day when the parties conclude the contract.

(2) Both parties are entitled to request a renegotiation of the provisions of these General terms if changes to the legislation so require or if the provisions prove to be inappropriate.

(3) The provisions of these General terms shall apply to the entire period of the provision of personal data processing services. They may not be interrupted during the provision of personal data processing services, unless other relevant provisions are concluded between the parties with a change of General terms or the contract regarding the provision of personal data processing services.

(4) In the event of interruption of the provision of personal data processing services and deletion or return of personal data to the controller in accordance with the first paragraph of Article 30 and the defined deadlines for data retention or procedures for deleting data from these General terms or the contract, the provisions of such contract or the use of these General terms may be terminated only regarding data protection upon written notice of either party.

Article 37

(1) If any of the provisions of the General terms is or becomes void, this does not affect the other General terms provisions. The void provision shall be replaced with the valid one, which most closely approximates the purpose intended by the void provision.

(2) If the provisions of these General terms or the contract concluded on the basis thereof are not implemented or there is no requirement to implement them, such waiver shall not be construed as a termination of the relevant provisions and shall not affect the validity of these General terms, either in part or in whole or in termination of the rights of any parties under these General terms.

Article 38

Any disputes between the parties under these General terms shall be resolved by the competent court in Ljubljana under the laws of the Republic of Slovenia.

Article 39

(1) Halcom may from time to time change or amend these General terms and inform the Client by electronic means at least two month prior to the changes having effect.

(2) The changes or amendments shall be deemed accepted by the Contractor except if the Contractor notifies the Client prior to the new changes taking effect about Contractor's reservations or cancelation of the contract under these General terms.

Article 40

These General terms are valid from 01. 01. 2021

Ljubljana, 02. 11. 2020

Tomi Šefman

Chief Executive Officer

halcom d.d. Ljubljana

APPENDIX 1: Privacy by design

1. Proactivity instead of reactivity

The concept of privacy by design is based on proactive action, on avoiding problems instead of reactively eliminating the consequences. Potential problems from the point of view of personal data protection and privacy should be anticipated in a timely manner and the design of the system adjusted in advance in a way that reduces the risks of abuse instead of waiting for those risks to materialize. If the concept of privacy by design is not followed and once such a solution is designed and used, adapting the solution will cost you time, resources and reputation, and in some cases subsequent repair of the system may cost you more than if the system was demolished and rebuilt.

2. Privacy as the default choice

The privacy-friendly settings should be defined as the default in information solutions. Examples of such settings may be:

- check boxes with which the individual confirms consent to the processing of their data should be blank by default - consent should be actively given by the individual by filling in;
- Data publicity settings (eg. on online social networks) should be set to data confidentiality by default.

3. Privacy, which is an integral part of the design of the solution

Privacy should be embedded in the very design and architecture of information solutions and business practices, not subsequently added. Privacy must be addressed already at the stage of setting the functional requirements of the system, and subsequent ways of ensuring privacy throughout the life cycle of the system must be provided.

4. Full functionality - a game with a positive sum

An essential element of the concept of privacy by design is to ensure full functionality - by embedding privacy, you should not sacrifice the efficiency of the system or other legitimately pursued goals. We often hear that we have to sacrifice privacy for the sake of higher security, practicality or economy, and the concept of privacy by design is based on finding solutions that do not force us to choose between the above, but provide both. And yes, this usually requires knowledge and time, sometimes even higher resources, but it is also usually possible to maintain privacy and still achieve the goals pursued.

5. Data protection throughout the data processing cycle

Data protection is an important element of personal data protection and refers to the prevention of unauthorized processing of personal data and accidental or intentional alteration or loss of personal data. Concern for the proper protection of personal data must be seen as a process and not just as individual tasks that are completed once they are completed. The process of securing personal data must be based on planning, implementing, verifying and responding to detected irregularities and deficiencies. In this regard, the Information Commissioner recommends that all data controllers follow the guidelines of internationally

established information security standards, such as the ISO / IEC 27000 family of standards, as well as periodically check for known vulnerabilities that may completely eliminate other measures.

6. Transparency

Closed solutions that allegedly ensure the protection of personal data and are based on our trust in them, despite the fact that they cannot be verified, are not in line with the concept of privacy by design. Conversely, privacy by design solutions must allow for independent external review and verification of the actual protection of personal data. From the world of cryptography, for example, there are known cases when hidden cryptographic methods were used, which were supposed to be safe due to this secrecy, but unfortunately it has been shown several times that only those solutions are truly safe that have been left to public scrutiny and on which even the best researchers with all available means were »breaking teeth« on. The average developer will find it difficult to write a secure crypto algorithm, so it is necessary to adhere to proven cryptographic methods in this regard.

Of course, the publicity in itself has not yet ensured that a solution will be safe, but public assessment should be necessary in certain cases - such an example is the introduction of future smart ID cards.

7. Respect for the individual

The design of the solutions should also take into account the individual's aspect and provide him with adequate information regarding the processing of personal data, default easy-to-use privacy settings and the like. Solutions that obscure personal data processing information in unreadable privacy policies and in complicated and overly technology-oriented settings that the average user does not understand at all do not satisfy the concept of privacy by design.

The concept of privacy by design is the basis for guidelines for the development of information solutions.

Source and more information: Guidelines for the development of information solutions (Information Commissioner of the Republic of Slovenia)