PERSONAL DATA PROCESSING AGREEMENT

(hereinafter referred to as the "**Data Processing Agreement**")

TTC apki, s.r.o.
with its registered office at Třebohostická 987/5, Strašnice, 100 00 Praha 10
Company ID No.: 194 03 429
VAT ID No.: CZ19403429
Bank account No.: 2800185401 / 2010
registered in the Commercial Register kept by the Municipal Court in Prague, File No. C 386033
represented by Ing. Jakub Laurich, MBA, Managing Director
(hereinafter referred to as the "**Processor**")

and

the TOUCHGUARD Customer, under any licence type and licence tier, identified as an entity that has entered into the Agreement as defined below with the Processor and identified by the details provided therein, or, as applicable, by the details provided during registration or in the Customer Account, in particular its business name or name and surname Company ID No., registered office or place of business, e-mail address and Customer Account ID, if assigned
(hereinafter referred to as the "**Controller**")
The Processor and the Controller are hereinafter collectively referred to as the "**Parties**" and individually as a "**Party**".

1 INTRODUCTORY PROVISIONS

1.1 The Parties have entered into an agreement or order for the provision of a software product, and/or accepted the General Terms and Conditions, or a combination thereof (the "**Agreement**"), pursuant to which the Processor, as Provider, undertook to grant the Controller, as Licensee, a non-exclusive right to use software solutions based on the TOUCHGUARD platform on a temporary basis and to provide related services (hereinafter collectively referred to as, "**TOUCHGUARD**").

1.2 This Data Processing Agreement is entered into between the Processor and the Controller, who entered into the Agreement with the Processor by accepting it during registration, ordering, activation of a Customer Account or by any other demonstrable means.

1.3 In the course of using TOUCHGUARD, the Controller enters into the system Personal Data relating to its employees and/or third parties, or such Personal Data is generated as a result of the use of the system and activated functionalities. The Controller determines the purposes and means of the processing of such Personal Data. The Processor processes such Personal Data on behalf of the Controller as a processor within the meaning of Article 4(8) of the GDPR.

1.4 The Parties enter into this Data Processing Agreement for the purpose of regulating their respective rights and obligations relating to the processing of such Personal Data by the Processor on behalf of the Controller in accordance with 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 (hereinafter referred to as the "**GDPR**") and Act No. 110/2019 Coll., on the Processing of Personal Data, as amended (hereinafter referred to as the "**Personal Data Processing Act**").

2 SUBJECT MATTER AND SPECIFICATION OF PERSONAL DATA PROCESSING

2.1 The Processor processes the Personal Data on behalf of the Controller to the extent necessary for the provision of TOUCHGUARD under the Agreement and solely on the basis of the Controller's documented instructions.

2.2 The Parties agree that, for the purposes of this Processing Agreement, the Controller's documented instructions include, in particular:

- the Agreement and its annexes;
- this Data Processing Agreement and its annexes;
- the documentation and technical specifications of TOUCHGUARD;
- the system settings selected by the Controller, activated modules, roles, retention settings and other configurations implemented within TOUCHGUARD;
- the Controller's written or electronic requests within the scope of the agreed services.

2.3 The Processor is not obliged to accept or implement any instruction of the Controller that:

- is contrary to the GDPR, the Personal Data Processing Act or any other applicable legal regulations;
- exceeds the agreed scope of the services;
- would require modification of the system architecture or the provision of additional services not included in the Agreement;
- could jeopardise the security, availability or integrity of the system or the data of other customers.

2.4 The specification of the processing is set out in Annex 1 to this Processing Agreement.

2.5 The Controller acknowledges that TOUCHGUARD is a standardised software product with predefined functionalities and data structures. The scope of the Personal Data actually processed depends primarily on which modules and functionalities the Controller activates and how it uses them. The Processor processes Personal Data on behalf of the Controller only to the extent to which such Personal Data has been entered into TOUCHGUARD by the Controller. The list of categories and their individual items is exhaustive, and the Controller is not obliged to use all of them.

2.6 TOUCHGUARD includes a tool for creating digital forms. The Controller creates form templates within the system (i.e. defines the individual form fields), and the end user works with such forms (i.e. enters the data required by the Controller). The Controller is responsible for the content, structure and configuration of the forms, for determining which Personal Data will be collected through the forms, and for the lawfulness of such processing. The Processor does not restrict the Controller in the selection of form fields. The Processor is not obliged to review the content of the forms on an ongoing basis or assess in advance their compliance with applicable legal regulations.

2.7 Unless expressly agreed otherwise in writing, TOUCHGUARD is not intended for the processing of special categories of Personal Data within the meaning of the GDPR or other particularly sensitive data, in particular data concerning health, biometric data processed for the purpose of unique identification, personal identity numbers or copies of identity documents, except where the relevant system functionality expressly envisages such data and the Parties expressly agree thereto or where such processing is necessary for a functionality activated by the Controller.

2.8 The Processor has adopted the technical and organisational measures specified in Annex 1 for the purpose of securing the processing of Personal Data. The specific scope of such measures may vary depending on the operating model, in particular whether TOUCHGUARD is operated within the Processor's infrastructure or on-premises within the Controller's infrastructure. TOUCHGUARD includes the functionality "Anonymisation of Deleted Persons (Users)", which may be activated by the Controller in the system settings. Once activated, the functionality ensures that immediately upon deletion of a user from the system database (within the "Users" function), the user's first name and surname are replaced with the system message "~~Anonymised Deleted Record~~". Deleted users and their links to other Personal Data and generated information can no longer be identified within the system.

2.9 TOUCHGUARD includes the functionality "Information Retention Settings". The standard retention period for information generated through the use of the system (reports, logs and records) is set at 12 months. Data older than 12 months is automatically deleted by the system. The Controller, as a user, may shorten this period through the system settings. The basic unit for shortening the retention period is one calendar month. The processing period continues for the duration of the Agreement and thereafter for the period necessary to settle obligations and to carry out deletion/return of the data.

3 CONTROLLER'S RIGHTS AND OBLIGATIONS

3.1 The Controller undertakes:

3.1.1 to ensure the appropriate legal basis for the processing of the Personal Data covered by this Data Processing Agreement;

3.1.2 to ensure that all Personal Data of the Controller is collected and disclosed to the Processor in a lawful manner;

3.1.3 to ensure that data subjects have been provided, in accordance with the GDPR and applicable Personal Data protection legal regulations, with sufficient information relating to the processing, including information that the Processor may/will process Personal Data on behalf of the Controller;

3.1.4 not to issue any instructions to the Processor that are contrary to the GDPR, applicable Personal Data protection laws or any other legal rights of data subjects;

3.1.5 to be responsible for the content of the data entered into TOUCHGUARD, in particular for the content of user-defined forms, fields, notes, attachments and other inputs entered by the Controller or its users;

3.1.6 not to enter into TOUCHGUARD Personal Data beyond the agreed purpose and functionalities and, without prior agreement, in particular not enter special categories of Personal Data or other sensitive data;

3.1.7 to inform the Processor without undue delay of any incorrect, rectified, updated or deleted Personal Data subject to processing by the Processor;

3.1.8 to grant the Processor a general written authorisation to engage additional processors for the performance of the Agreement and the Data Processing Agreement;

3.1.9 provide the Processor in a timely manner with lawful and documented instructions relating to the Processor's processing of Personal Data.

4 PROCESSOR'S RIGHTS AND OBLIGATIONS

4.1 The Processor undertakes:

4.1.1 to process Personal Data solely on the basis of the Controller's documented instructions, unless such processing is required by the European Union or Member State law;

4.1.2 to ensure that all persons involved in the processing of Personal Data are bound by confidentiality obligations, or to ensure that they are subject to an equivalent statutory duty of confidentiality;

4.1.3 to adopt security measures in accordance with the requirements of Article 32 GDPR;

4.1.4 to comply with the conditions for the engagement of additional processors set out in this Processing Agreement;

4.1.5 to take into account the nature of the processing, assist the Controller in the performance of its obligations and in responding to requests for the exercise of data subjects' rights;

4.1.6 provide reasonable assistance to the Controller in ensuring compliance with the obligations set out in Articles 32 to 36 of the GDPR, taking into account the nature of the processing and the information available to the Processor;

4.1.7 where a data subject submits a request directly to the Processor, the Processor shall forward such request to the Controller without undue delay, unless the Processor is authorised to respond directly on the basis of the Controller's instructions or applicable legal regulations;

4.1.8 in accordance with Controller's decision, to delete the Personal Data or anonymise it upon completion of the processing and delete any existing copies, unless European Union or Member State law requires the storage of such Personal Data;

provide the Controller with the information necessary to demonstrate compliance with the obligations set out in Article 28 of the GDPR, provided that the Controller and any persons authorised by it to conduct an audit undertake to maintain confidentiality regarding any information obtained in the course of such audit. The Processor shall demonstrate compliance with the above obligations primarily by means of certificates or certification reports issued under ISO/IEC 27001 and ISO/IEC 20000-1, where available, or by means of security assessment reports, provided that such reports correspond to the nature of the provision of TOUCHGUARD. If such documentation is objectively insufficient to demonstrate compliance and the Controller demonstrates a justified need for an audit, an audit may be carried out no more than once every 12 months, subject to at least 30 days' prior notice, during normal business hours and in a manner that does not jeopardise the Processor's ordinary business operations, system security, the Processor's trade secrets or the Personal Data of other customers. Any costs incurred in connection with such audit shall be borne by the Controller;

4.2 The Processor is entitled to provide Personal Data received from the Controller to another third party acting as a subcontractor for the purpose of the processing thereof. In such case, however, the Processor is obliged to notify the Controller of the name or business name of the selected subcontractor before disclosing any Personal Data to it, except where such subcontractor

already processes Personal Data as of the date of conclusion of this Data Processing Agreement. The Controller is entitled to raise a justified objection to the selection or replacement of a subcontractor within five days after being notified of the subcontractor's name or business name. Such objection must be submitted electronically to e-mail address obchod@apki.cz and demonstrably delivered to the Processor. If the Controller raises an objection to a particular subcontractor and the Processor thereby incurs additional costs in connection with the processing of Personal Data under this Data Processing Agreement and/or due to the need to select an alternative subcontractor on less favourable terms, the Processor is entitled to require the Controller to reimburse such additional costs.

5 DELETION OR RETURN OF THE CONTROLLER'S PERSONAL DATA

5.1 The Processor undertakes to delete the Controller's Personal Data within ten business days following the termination of this Data Processing Agreement and/or the Agreement, or following the termination of the last Licence Agreement (under the Processor's TOSs). The Processor shall delete the Personal Data, including any copies thereof. Deletion of the Controller's Personal Data constitutes termination of the processing of Personal Data under this Data Processing Agreement.

5.2 The Processor undertakes to delete all records and all user data created and entered by the Controller through the use of TOUCHGUARD within ten business days following the termination of the Agreement, or the last Licence Agreement (under the Processor's TOSs).

5.3 Notwithstanding Clause 5.1, the Processor may retain the Controller's Personal Data to the extent required by European Union or Member State legal regulations and only to the extent and for the period required under such regulations, provided that the Processor secures the confidentiality of all Controller‘s Personal Data and ensures that such Personal Data is processed solely to the extent necessary for the purpose specified by the applicable legal regulations of the Europan Union or a Member State equiring its retention and for no other purpose.

6 REMUNERATION

6.1 The Parties agree that the remuneration payable to the Processor for the ordinary processing of Personal Data under this Data Processing Agreement is included in the remuneration agreed under the Agreement.

6.2 Notwithstanding the provisions of the previous paragraph, the Parties agree that the Processor is entitled to claim reimbursement of additional costs where the Controller requires the Processor to undertake additional activities or implement additional measures beyond the scope agreed in this Data Processing Agreement. The Processor is also entitled to claim reimbursement of costs incurred in connection with, for example, handling data subject requests, extensive or repeated data exports, completion of security questionnaires beyond the ordinary scope, ad hoc audits, assistance with data protection impact assessments (DPIAs) or individual technical or legal measures requested by the Controller beyond the scope of the standard service.

7 INTERNATIONAL TRANSFERS OF PERSONAL DATA

7.1 With respect to Personal Data originating from the Controller or processed on its behalf within

the EU/EEA, where such Personal Data is accessed or processed by the Processor, its subcontractors or affiliated entities in jurisdictions outside the EU/EEA (including through the use of cloud-based IT solutions), the Controller hereby authorises the Processor to enter into, in the name and on behalf of the Controller, an agreement incorporating the EU Standard Contractual Clauses pursuant to Commission Decision C(2010) 593 with the third-country recipient of such Personal Data. An agreement incorporating the EU Standard Contractual Clauses will not apply where the laws of the country in which the relevant subcontractor or affiliated entity of the Processor is established recognise the EU as a jurisdiction providing a suffiicent level of Personal Data protection, or where the Processor and/or its subcontractor or affiliated entity located in the United States has joined the EU–US Privacy Shield framework.

8 RESPONSIBILITY AND LIABILITY

8.1 Each Party is responsible for fulfilling its obligations under the GDPR to the extent corresponding to its role (Controller/Processor). Liability for damage vis-à-vis data subjects and supervisory authorities is governed by Article 82 of the GDPR and applicable legal regulations.

9 FINAL PROVISIONS

9.1 This Data Processing Agreement becomes effective upon execution by both Parties. This Data Processing Agreement is entered into in connection with the Agreement and its effectiveness is dependent upon the effectiveness of the Agreement. The Parties confirm that, in such case, the agreements constitute mutually dependent contracts within the meaning of Section 1727 of Act No. 89/2012 Coll., the Civil Code, as amended. Any termination of the Agreement by a means other than performance or a substitute for performance, or the invalidity of the framework agreement, will also result in the termination of the framework agreement, with corresponding legal effects.

9.2 This Data Processing Agreement has been executed in two counterparts, each having the validity of an original, and each Party will receive one counterpart.

9.3 This Data Processing Agreement may be amended or supplemented only by written amendments executed by the Parties. For these purposes, no means of electronic communication are deemed to satisfy the written form requirement.

9.4 The Parties are not entitled to assign or otherwise transfer any rights or obligations arising under this Data Processing Agreement to any third party.

9.5 Should any provision of this Data Processing Agreement be found invalid, ineffective or unenforceable, the remaining provisions of this Data Processing Agreement will remain unaffected, provided that they can be severed from the invalid, ineffective or unenforceable provision. In such event, the Parties undertake to replace the invalid, ineffective or unenforceable provision with a new provision that most closely reflects the original intent of the replaced provision.

9.6 Annexes 1 and 2 form an integral part of this Processing Agreement.

9.7 The Parties hereby agree that, even in the absence of separate signatures on the text of this Data Processing Agreement, this Data Processing Agreement is concluded with sufficient certainty through the manifestation of the will of both Parties upon conclusion of the Agreement within the meaning of Article 1 of this Data Processing Agreement.

Annex 1 – Specification of processing and security measures

A. Subject Matter and Purpose of Processing

Processing is carried out for the purpose of providing TOUCHGUARD under the Agreement (in particular operation, hosting or on-premises support, user account administration, data synchronisation, logging and security monitoring).

B. Nature of Processing

The processing consists primarily of the storage, structuring, retention, consultation, disclosure to authorised users of the Controller, transmission, retrieval, restriction, deletion, anonymisation and backup of data within TOUCHGUARD.

C. Categories of Data Subjects

- employees of the Controller
- persons performing activities for the Controller under another contractual relationship
- contact persons of the Controller's contractual partners
- other persons recorded by the Controller as users or persons in respect of whom the Controller maintains records within TOUCHGUARD through activated functionalities
- visitors recorded by the Controller (if the Visitor Management module is activated)

D. Categories of Personal Data (typically)

module / functionality	category of data	note / activation condition
TOUCHGUARD BASIC / PRO / WATCH	first name, surname, e-mail address, personal identification number, telephone number (calls/SMS), photograph, IMEI device	depending on the Controller's settings; IMEI only if used
TOUCHGUARD BASIC / PRO / WATCH – GPS	user's location (GPS coordinates)	only when the GPS function is activated or when working with NFC/Bluetooth points with GPS
TOUCHGUARD PRO – Visitors	visitor's first name and surname, visitor's telephone number, vehicle registration number, company name	only when the "Visitor Cards" function is activated
TOUCHGUARD PRO – Document Scanning	first name, surname, document type, issuing country, document number, nationality, date of birth, expiry date	only when document scanning and the "Visitor Cards" function are activated
TOUCHGUARD WATCH – Heart Rate Monitoring	heart-rate status/alert information (without transmission of the exact value to the server)	the exact heart-rate value is not transmitted; only the evaluation result is transferred to the server

E. Place of Processing

Option 1 – hosting provided by the Processor

TOUCHGUARD is operated on infrastructure provided by the Processor and/or an additional processor listed in Annex 2.

Option 2 – On-premise / Controller Infrastructure

TOUCHGUARD is operated within the Controller's infrastructure. In such case, the Controller is responsible in particular for physical security, the network environment, server infrastructure administration and system backups, unless expressly agreed otherwise between the Parties. The Processor is responsible for the scope of processing that it actually performs within the agreed support, application administration or remote-access services.

F. Technical and Organisational Measures (Illustrative Framework)

Depending on the selected operating model, in particular:

• access management (roles, authentication, permission management);
• authentication of users and administrators;
• database protection through passwords and access-control mechanisms;
• logging and audit records of access;
• regular backup and recovery;
• vulnerability management and security updates;
• incident management and reporting of security breaches;
• personnel training and confidentiality obligations;
• the possibility of configuring data retention periods within the application (12 months by default; the Controller may shorten the period or request its reduction);
• an optional anonymisation function for deleted users (replacement of first name and surname with a system-generated value).

G. Custom Forms and User-Defined Fields

The Controller acknowledges that, within certain functionalities, it may create custom forms, fields or other data structures. The Controller bears sole responsibility for the content of the data collected in this manner, its scope, necessity and lawfulness.

Annex 2 – Sub-processors

As of the date of conclusion of this Data Processing Agreement, the following additional processor is engaged::

- SH.cz s.r.o. – managed server / server hosting / infrastructure management
  - Country of processing: Czech Republic
  - Scope of services: production and testing server environments, technical infrastructure administration