DATA PROTECTION POLICY

1. INTRODUCTION

We appreciate the trust you have demonstrated by entrusting us with your data. Aware of the responsibility this entails, we strive to manage your data in a lawful, fair and transparent manner. Below listed is the key information regarding data processing, our obligations and your rights arising from the General Data Protection Regulation (GDPR) and the Personal Data Protection Act of the Republic of Slovenia (ZVOP-1).

You have entrusted your personal data to:
Halcom d.d.
Tržaška 118
1000 Ljubljana
t: +386 (0)1 200 33 69
f: +386 (0)1 200 33 56
info@halcom.si

The data controller is Halcom d.d., Tržaška 118, 1000 Ljubljana, Slovenia. For any inquiries please contact us by phone (+386 1 200 33 69), fax (+386 1 200 33 56) or email (info@halcom.si).

Halcom's personal data processing is monitored by an external Data Protection Officer (DPO), who constantly monitors the compliance of our processes with the applicable regulations and international standards, assesses impacts of the processing of personal data, and cooperates with supervisory authorities.

Data Protection Officer

Lemur Legal d.o.o.
Peter Merc

The Data Protection Officer is available for any questions or help exercising your rights by prior appointment at the headquarters of Halcom (Tržaška 118, 1000 Ljubljana) or via email (dpo@halcom.si).

dpo@halcom.si

2. TYPES OF DATA AND THE PURPOSES OF PROCESSING

To provide you with safe, user-friendly and effective operation of electronic banking and electronic commerce services and products, we process different types of data:

We process different types of data to ensure secure, user-friendly and effective electronic banking and electronic commerce.

We process different types of data for different activities:

- *for trust services* (electronic signatures and stamps, digital certificates, time stamping), technical and user support for electronic banking and payment services;
- *for electronic commerce services* (electronic applications, approvals and document exchange), technical support to electronic services and customer support;
- *for the purpose of notification*, user-friendly website visits, marketing, and analytics.

We act as a data processor for numerous commercial banks, issuers of electronic money and other clients, storing and processing data in our secure private cloud

We act as a data processor in the private cloud for our numerous clients.

3. TRANSPARENCY OF PROCESSING AND YOUR RIGHTS

We strive to provide you with all the necessary information concerning the processing of your data and all your rights and our obligations in this area. A considerable part of decisions on data protection is up to each individual. We are inherently different from one another, and so are our decisions about privacy. Therefore, we will treat your data exactly as you want, unless otherwise provided by applicable legislation

Providing information and hiding nothing. Complying with your choices. Assisting you with your rights.

The constitution of the Republic of Slovenia and the applicable European and Slovenian regulations grant you numerous rights regarding privacy and protection of personal data, including in particular the following:

- right to be informed about the processing of your personal data (the text you are reading is part of our effort to comply with your right);

  Right to be informed – information available to you

- right of access to personal data means that you have the right to find out if Halcom as data controller is processing your personal data, and if so, to access such personal data and additional information (purpose of processing, data types, users of data, rights and possibilities of appeal, data sources, information on any automated decision or special profiling);

  Right of access – you can request access to all your data at any time

- right of rectification means that you have the right to challenge the accuracy of personal data held about you by us, and ask for it to be corrected; taking into account the purposes of the processing, you also have the right to have incomplete personal data completed, including by means of providing a supplementary statement;

  Right of rectification – we will rectify incorrect data at your request

- right to erasure also known as the "right to be forgotten" means that you have the right to ask that your data be deleted without undue delay provided certain prescribed conditions are met (processing is no longer necessary, you withdraw your consent, and no other legal basis exist for processing, well-founded objection, unlawful processing, erasure required by applicable regulations and so on);

  Right to erasure – in some circumstances you may request data be deleted (right to be forgotten)

- right to restriction of processing means the right to limit the way we use your personal data if you are concerned about the accuracy of the data or how it is being used (upon filing an objection) or if the processing is unlawful or if we no longer need to process your data, and you still want us to store it for establishment, exercise or defense of legal claims;

  Right to restriction – under certain circumstances you may request data to be stored but not processed

- right to data portability is the right to receive your personal data, which you have provided to us, in a structured, commonly used and machine-readable format and the right to transmit those data to another controller without hindrance from us (applies to data processed by automated means on the basis of your consent or our contractual relationship);

  Right to data portability – request export of data (for transfer) at any time

- right to object means you can object against certain types of processing of your personal data (based on public interests, our legitimate interests, the purposes of marketing) and we need to demonstrate compelling legitimate grounds for processing or stop processing (always when used for marketing purposes);

Right to object – you may request at any time that we prove our legal basis for data processing

- rights with regard to automatic processing and profiling mean that we may not make decisions based solely on automated processing, including the creation of profiles which have legal or similar effects in relation to you, if it is not necessary for entering into, or performance of, a contract, prescribed by law, or based on your explicit consent.

Rights with regard to automatic processing – you may always discuss matters with a human and do not need to argue with a computer

To exercise your rights or to obtain further information or clarification, our Data Protection Officer (DPO) will be happy to assist you by appointment at the headquarters of our company (Tržaška 118, 1000 Ljubljana) or email (dpo@halcom.si).

Contact our Data Protection Officer (DPO) to exercise your rights

If you believe that your rights or data protection rules have been breached in any way, you can complain to the competent national authority (in Slovenia: Information Commissioner of RS (Dunajska cesta 22, 1000 Ljubljana, Slovenia; phone: +386 1 230 97 30, email: gp.ip@ip-rs.si)

Infringements may be reported to the Information Commissioner of the Republic of Slovenia

In Ljubljana, on 16 March 2023

Tomi Šefman

Chief Executive Officer

APPENDIX 1

DATA PROCESSING FOR TRUST SERVICES, TECHNICAL SUPPORT FOR ELECTRONIC BANKING AND PAYMENT SERVICES AND USER SUPPORT

1. TYPES OF DATA

We store and use different types of data for a safe, user-friendly and beneficial use of qualified digital certificates, electronic signature and stamping, time stamping, technical support and improving software solutions, our services and user support in the areas of electronic banking and electronic signature.

To enable secure and user-friendly e-banking and e-business, we store and use different types of data.

We store and use the following types of data of holders and users of qualified digital certificates and other users of trust services and electronic operations:

To ensure security and trust in electronic transactions, we use user data on your digital certificates.

- information on the identity of the prospective, current or former holder of a qualified certificate for electronic signature;
- information on the identity of the person representing or authorized by the business entity that has ordered a qualified certificate for electronic signature or stamp or other trust services;
- information on a potential indication of a person representing or being authorized by a business entity in the lists of international sanctions of the following countries: the Republic of Slovenia, European Union, Australia, Canada, the Swiss Confederation, the United States of America, and the United Kingdom of Great Britain and Northern Ireland; details of any indications in the media about the unlawful or illegal activities of the staff;
- certificate life cycle information (from issuance until expiration), including details of any revocations (date and time of the revocation, cause of revocation, revocation implementation);
- documents and communications relating to the persons and actions mentioned above (purchase orders, revocation requests, other messages);
- information and documents relating to the electronic signing in the cloud (signature requests and related documents, signature approval or rejection, security and communication data, and other data related to cloud signing).

When offering technical and customer support, we store and use data on contacts, use, problems, and solutions.

When offering technical and customer support for electronic banking and electronic commerce we collect and store the following information:

- contact data (for example, first and last name, business entity, telephone number, email address, etc.);
- information about support services or maintenance (application error description, questions or requests, and transactions, information regarding software used, descriptions of actions and communications, screenshots, examples of files with errors);

- recordings of telephone calls to technical assistance;
- documents and communications relating to the support and maintenance (application failures, orders, messages, files with errors, screenshots, etc.).
- if you have given explicit content in our mobile applications, we are allowed to use, for the purpose of enhancing information security, efficiency and user-friendliness of our operations and for the purpose of eliminating errors and deficiencies, analytical tools of mobile providers (Google, Apple), which use mobile operating systems (iOS, Android) to collect and transfer information about the error or crash (i.e. UUID compliant with RFC-4122 enabling reproduction of the environment), error or crash audit trails (time stamp, application data, application and system settings or a 'breakpad minidump' and other similar technical information on the use of the mobile application); in particular, please note that as regards the use of Google-based solutions (e.g. Firebase) Halcom normally acts as a data controller and Google acts as a processor according to the GDPR and the resulting contractual clauses; more detailed information can be acquired from Google and will depend on your use of other Google services and third-party mobile applications.

When you call our helpdesk, we collect support call data and record the call.

When you call our helpdesk, we process the following information:

- contact data (first and last name, phone number, email address, etc.);
- information about support or maintenance services (error report or claim, description of an error, query or claim and related transactions, information regarding the software used, descriptions of actions and communications, screenshots, examples of files with errors);
- recordings of telephone calls to customer support and recordings (or screenshots) of the actions taken;
- documents and communications relating to the support and maintenance (application failures, orders, messages, files with errors, screenshots, etc.).

2. PURPOSE AND USE OF DATA PROCESSING

We process your data based on our contractual relationship and applicable regulations.

We process personal data in line with the provisions of the applicable regulations, in particular Regulation (EU) No. 910/2014 of 23 July 2014 concerning electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS Regulation) and Electronic Identification and Trust Services Act, as well as based on contracts with subscribers of qualified digital certificates or trust services. Halcom is a qualified trust service provider and registered in the trust list published by the European Commission (https://webgate.ec.europa.eu/tl-browser/#/).

For the purpose of security of electronic commerce and in accordance with the above-listed law and regulations on trust services, we check the correctness of personal data against public records managed by government bodies, or make inquiries with other data controllers to obtain personal data you have not submitted and are necessary to implement your purchase order and issue a qualified certificate or provide you with another Halcom trust service.

When served with a reasonable and lawful demand, we are obliged to provide your personal data to domestic or foreign government bodies, other public authorities, public service providers or alternative dispute resolution bodies.

For the purposes of the safe and user-friendly electronic signing in the cloud, we in addition to data on digital certificates and trust services also process data and documents regarding electronic signatures in the cloud when you use such services.

We store some of your data based on your consent that you may revoke at any time. However, any such revocation might impact the usability of your certificate or another service.

For the purposes of safe and user-friendly electronic commerce we process data relating to your identity and mobile devices, as well as used services and exchanged documents.

We store contact details and other information regarding support services based on your consent. Data contained in the digital certificate is publicly available in the Directory of issued digital certificates in accordance with our trust service policies. Based on your explicit consent, we provide entities with whom you do business electronically (e.g., banks, insurance companies, government departments and others) with access to your certificate listed in the directory and publicly available information contained within. You may cancel your consent at any time in writing. However, such cancellation may impact the validity of the qualified certificate or provision of trust services. Also, please note that withdrawal of consent does not affect the storage of information, prescribed as mandatory by applicable legislation.

To ensure user-friendly and efficient e-commerce and e-banking, we make data on your digital certificates available to banks and other providers on the basis of your consent, which you may revoke at any time.

Based on your consent and for the purposes of user-friendly and efficient electronic banking we provide commercial banks and other payment institutions where you or business entities you represent have a payment account with data on issued certificates for electronic signature. We also provide information on the identification and verification process to the partners providing related services (e.g., electronic identification, electronic signatures, electronic banking, mobile payments) if you agree to this when using their service and insofar as the applicable legislation require mandatory identification. You may revoke your consent at any time in writing, and this will not impact the validity of qualified certificates or provision of trust services.

However, you might have to provide data manually yourself to banks and other payment institutions or companies.

In accordance with data protection regulations, all other information not contained in the digital certificate is strictly protected and is not made public. This information is used exclusively for the purposes of certificate management and secure electronic banking and electronic commerce, and is not used for any other purposes.

We process your data for purposes of proof of business relationships (customer service recordings of calls and recordings of the actions taken, the content and scope of the service) up to 6 years after the termination of the contractual relationship and on the basis of your consent, which you can cancel at any time, until revoked for the purposes of technical and customer support for electronic banking and electronic commerce.

Personal data concerning digital certificates and trust services are kept in accordance with European (ETSI) standards for 7 years after the expiry of certificates. Other data is stored up to 6 years after the termination of the contractual relationship unless otherwise stipulated by the applicable legislation on data retention.

If you submit your email address through the website to access licensed software (e.g., drivers or middleware), it shall be used exclusively to check that you have actually been issued with a qualified digital certificate and to forward the link to the software. Your e-mail address is not stored and not processed for any other purpose.

Your data may also be processed if the processing is necessary for the legitimate interests that we pursue as a controller or a third person, except where your interests or fundamental rights and freedoms, which require the protection of personal data, override such interests. The processing and retention periods are aligned with the applicable regulation (e.g., statutes of limitation).

We process your data as a data controller. For certain services we may collaborate with external processors (our subcontractors), for whom we assume full liability. The Appendix includes a list of external providers.

As we do business increasingly digitally, all decisions which produce legal effects concerning you or affect you in a similarly significant manner are taken by our employees on the basis of appropriate information support. We implement comprehensive measures to protect your rights and freedoms and legitimate interests. You can always exercise at least your right to human intervention on the side of the controller, to express your own views and challenge decisions.

We process your personal data also for the purpose of technical and user support to e-banking and e-commerce.

We store data concerning trust services up to 7 years after the end of validity, and other data for 6 years after the termination of the contract.

Your email address provided to access licensed software is used only for verification and not stored.

We process data based on legitimate interests of Halcom and third persons, provided your legitimate interests or liberties do not prevail.

Although we mostly do business digitally, you will never talk to a machine, but to our staff who are always there to help you with your queries.

APPENDIX 2

DATA PROCESSING FOR CORPORATE COMMUNICATION, FRIENDLY AND SECURE WEB EXPERIENCE, AND MARKETING AND ANALYTICS

1. TYPES OF DATA

We store and use different types of data to provide you with a friendly and useful web experience.

We collect content, messages, and other information that you submit or post while using our website. We also collect the following data:

- data about the device you are using (e.g., operating system, hardware, and software version, language used);
- network and connection data (e.g., IP address, language, time zone);
- additional data from your device if you specifically enable it (e.g., GPS and other location data, access to the camera, photos, contacts);
- log data (e.g., the date and time of the visit, internet protocols, data on errors or crashes).

If you use our website without logging into your user account, we collect and store data marked with unique identifiers (e.g., cookies), which are related to a device or browser that you are using. This approach enables persistent settings between browsing sessions

Once you have logged into our website with your username and account, your information is collected and stored together with other data from your user account and protected as personal data.

If you give us your email address or participate in our events, promotions, and sweepstakes, we process your email address and/or ID on social networks, the information about your business entity, and details of your participation in our activities and our communication with you.

If you submit your email address through the website to access licensed software (e.g., drivers or middleware), it shall be used exclusively to check that you have actually been issued with a qualified digital certificate and to forward the link to the software. Your e-mail address is not stored and not processed for any other purpose.

We collect and store your data when you visit our website or use our online services.

Data on website users who are not logged in are collected and stored marked with unique identifiers (e.g., cookies).

Upon login, your data is associated with your account and protected as personal data.

For notification and marketing purposes, we collect data about your email, social networks, and your cooperation with us.

Your email address provided to access licensed software is used only for verification and not stored.

2. PURPOSE AND USE OF DATA PROCESSING

We process your personal data for the purposes described below and in accordance with your consent, until revoked, or based on our legitimate interests or those of a third party for a specific time as long as lawfully needed.

We collect and use your data based on your consent that you can revoke at any time.

Based on your consent we process your email address and/or social networks ID, your business entity information, details of your participation in our activities, and our communication with you to keep you informed about our news, events, new locations, benefits and for other purposes related to marketing and analytics.

Based on your consent we use data for communication and marketing purposes.

You can express your consent in different ways: simply by visiting our website, confirming or rejecting cookies, with a registration and subsequent login to your user account or with the use of a special consent form. You may change or revoke your consent at any time by using our online services or contacting us (for contact information see the first section).

We process data for the purpose of provision, maintenance and development of our websites and services and to ensure the information security of our users, services, and infrastructure. We also process data to ensure a friendly and useful visit to our sites and services (e.g., your personalized content).

We collect and use your data to enable user-friendly and secure online experience.

We process your data as a controller and may for certain services, in accordance with the applicable legislation, engage processors (our subcontractors) for whom we fully guarantee. Your data will not be disclosed to other parties and shall be processed in facilities that are physically located on the territory of the European Union, where strict European data protection rules, including the General Data Protection Regulation (GDPR), are in force. We do not transfer data to third countries (countries outside the European Union) or international organizations

Halcom d.d. acts as a controller of your data within the territory of European Union.

We may also process your data if this is necessary to protect the legitimate interests (information security of Halcom d.d. and users of Halcom's IT solutions, commercial interests of Halcom d.d., etc.) that we pursue as a controller or those of a third person, except where your interests or fundamental rights and freedoms, which require the protection of personal data, override such interest. The processing period is aligned with the applicable deadlines (e.g., statute of limitations and the like – the general statute of limitation between business entities is three years from the termination of the contract, and for relationships with natural persons it is five years from the term of the contract of from the date of the loss event.

We process data based on legitimate interests if your legitimate interest and liberties do not prevail.

As we do business increasingly digitally all decisions which produce legal effects concerning you or similarly significantly affects you, are taken by our employees with appropriate information support. We implement comprehensive measures to protect your rights and freedoms and legitimate interests. You always have at least the rights to human intervention, to express your own views and challenge decisions.

As we do business increasingly digitally, you will always be able to talk to a human and not a computer. We will always be there for you and listen to all queries and requests.

APPENDIX 3

LIST OF CONTRACTUAL PROCESSORS

- Pošta Slovenija (Data Center)
- T-2 (Data Center)