

V. 3.0/ 20.12.2025

This document entitled Clause “Personal Data Protection” (hereinafter – the “Clause”) forms an integral part of the General Terms of Agreement with Corporate Clients (hereinafter – the “General Terms”), under which Evrotrust Technologies AD, with registered address at 251G (Г) Okolovrasten Pat Str., MM Business Center, floor 5, 1766 Sofia, Bulgaria, provides services to corporate clients and contains the terms of the agreement on the processing and the protection of personal data between Evrotrust and the Partner identified in the relevant Special Terms and Conditions.

1. Definitions

In the application and interpretation of this Clause, the following terms shall have the following meanings:

1.1. “Regulation” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. All references to the Regulation should also be read as references to all applicable provisions of the legislation of the Republic of Bulgaria or of another Member State which transpose or are adopted on the basis of the Regulation into Bulgarian national law or the national law of another Member State, respectively.

1.2. “Applicable Rules/Applicable Data Protection Rules” for the purposes of this Clause means the Regulation and all other applicable laws in force (regulations, statutes, ordinances, etc.), governing the protection and processing of Personal Data.

1.3. “Agreement” has the meaning as defined in the General Terms;

1.4. “SCC” means the Standard Contractual Clauses adopted by the European Commission with Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries (outside the EU/EEA) pursuant to the Regulation and available at the following link or another link as may be publicly provided by the European Commission:

https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en.

1.5. All terms and definitions used in this Clause which are not defined herein shall have the meaning given to them in the General Terms or any relevant Clause(s), applicable between the Parties hereto and, if none, shall have the meaning given to them in the Regulation or, if not defined in the Regulation, the meaning given to them in the relevant other Applicable Rules. This includes the terms "Personal Data", "Processing"/ "Data Processing", "Data Controller", "Data Processor", "Data Subject", etc., irrespective of whether used with a capital letter or not.

2. Subject Matter and Term

2.1. The purpose of this Clause is to regulate the rights and obligations of the Parties in relation to the exchange of personal data between them for the purposes of the performance of the Agreement, when Parties act as independent data controllers (Section I below), as well as, if applicable, in certain specific instances where one of Parties may act as Data Processor for the other Party. These specific instances include Partner acting as Data Processor and processing personal data on behalf of Evrotrust for the purposes of the performance of its activities as a Registration Authority (Section II below), and Evrotrust acting as Data Processor and processing persona data on behalf of the Partner for the purposes of the provision of the basicID service (Section III below). For the avoidance of doubt, Section II and Section III below shall only be applicable in case the Agreement between the Parties expressly provides for the specific conditions or services resulting in one of the Parties to act as Data Processor for the other.

2.2. This Clause is an inseparable part of the General Terms and applies in addition to any other data protection rules in force between the Parties as per the Agreement.

2.3. This Clause is in force between the Parties for the term of the Agreement.

SECTION I**CONTROLLER - CONTROLLER RELATIONS**

This Section applies to all Partners, unless otherwise specified.

3. Personal Data of employees**3.1. Processing of personal data relating to employees and other persons of Evrotrust's organization**

3.1.1. The Parties agree that in connection with the conclusion and performance of the Agreement the Partner will process personal data relating to Data Subjects who are authorized to represent, work for or cooperate with Evrotrust – contact persons, employees, managers, attorneys, representatives, etc. of Evrotrust. Such personal data may include names, form of representation, position/function within Evrotrust's organization, signature, duration of the representative authority, contact details (e-mail address, phone/fax number, etc.); information contained in documents generated in the course of the performance of the Agreement and/or provided by Evrotrust in connection with the performance of the Agreement; information contained in correspondence between the Parties relating to the conclusion, performance and/or termination of the Agreement, and any other information provided to the Partner.

3.1.2. The Partner will process the personal data referred to in item 3.1.1:

(a) for the following own purposes:

- Purposes of the processing of personal data by the Partner related to compliance with legal obligations: financial and accounting activities; fulfillment of statutory obligations related to financial, tax and accounting activities; fulfillment of legal obligations to keep documents and to provide information and reporting to the competent authorities; compliance with obligations related to the implementation of anti-money laundering measures; other regulatory requirements as applicable to the Partner's activities.
- Purposes of the processing of personal data necessary for the purposes of the legitimate interests of the Partner, the Partner's employees or third parties: activities to ensure the exchange of data and document checksums (hash) between the Partner's Systems and Evrotrust's Systems, and to maintain and administer the integration between the Systems,

authentication management and control, authorization and access to various information resources within the Systems, employee's identity identification and control, ensuring the access to necessary information taking into account the access rights of employees, exercise and protection of the legal rights and interests of the Partner.

(b) for the following terms:

- For the entire term of the Agreement and for up to five (5) years from its termination;
- In case personal data is contained in documents necessary for the purposes of tax and social security control - for a period of up to ten (10) years, starting from the beginning of the year following the year in which the payment of the public obligation for taxes or compulsory social security contributions related to the records kept for the respective financial year is due, or another period set by the applicable legislation;
- In the event of legal/judicial disputes arising in connection with the conclusion or performance of the Agreement or any activity in connection with its performance, or other administrative or judicial proceedings relating to the performance or activities under the Agreement, the personal data referred to in item 3.1.1 may be processed by the Partner for longer periods than those specified above if necessary for the establishment, exercise or defense of legal claims (e.g. in the event of a legal dispute or other proceedings for the period during which the case is pending, and for up to five (5) years after the date of final conclusion of the respective proceedings), or if the applicable legislation provides for data retention for a longer period.

3.1.3. Data Subjects under item 3.1.1. may exercise their rights against the Partner by using the Partner's contact details for personal data matters set out in the Special Terms and Conditions.

3.2. Processing of personal data relating to employees and other persons in the Partner's organization

3.2.1. The Parties agree that for the purposes of the performance of the Agreement Evrotrust will process personal data relating to Data Subjects who are authorized to represent, work for or cooperate with the Partner - contact persons, employees, managers, attorneys, representatives, etc. of the Partner. Such personal data may include names, form of representation, position/function within Partner's organization, signature, duration of the

representative authority, contact details (e-mail address, phone/ fax number, etc.); information contained in documents generated in the course of the performance of the Agreement and/ or provided by the Partner in connection with the performance of the Agreement; information contained in correspondence between the Parties relating to the conclusion, performance and/or termination of the Agreement, and any other information provided to Evrotrust.

3.2.2. Evrotrust will process Personal Data under item 3.2.1:

(a) for the following own purposes:

- Purposes for the processing of personal data by Evrotrust related to compliance with legal obligations: financial and accounting activities; compliance with statutory obligations related to financial, tax and accounting activities; compliance with legal obligations to keep documents, to provide information and to report to the competent authorities; compliance with other regulatory requirements as applicable to the activities of Evrotrust;
- Purposes for the processing of personal data necessary for the purposes of the legitimate interests of Evrotrust, its employees or third parties: activities to ensure the exchange of data and documents between the Partner's Systems and Evrotrust's Systems and to maintain and administer the integration between the Systems, authentication management and control, authorization and access to various information resources within the Systems, employees' identity identification and control, ensuring the access to necessary information taking into account the access rights of employees, exercise and protection of the legal rights and interests of Evrotrust.

(b) for the following terms:

- For the entire term of the Agreement and for up to five (5) years from termination;
- *Applicable to Partners acting as a Registration Authority:* In the event that the personal data relate to actions performed by the persons referred to in item 3.2.1 in their capacity as Agents or are contained in documents created in connection with the implementation of the Partner's activities as a Registration Authority of Evrotrust – for a period of up to ten (10) years from the termination of the Agreement, including in cases where access to the profiles and/or their contractual relationship with the Partner is terminated prior to the termination of the Agreement, after which time Evrotrust is obliged to delete the personal data of the Partner's

Agents. The personal data of the Partner's Agents may also be processed by Evrotrust for a longer period than the specified 10-year period if it is necessary for the establishment, exercise or defence of legal claims (e.g. in the event of a legal dispute or other proceedings up to five (5) years from the date of the final conclusion of the relevant case before all instances) or if the legislation in force provides for the processing of the data for a longer period.

- In case personal data is contained in documents necessary for the purposes of tax and social security control – for a period of up to ten (10) years, starting from the beginning of the year following the year in which the payment of the public obligation for taxes or compulsory social security contributions related to the records kept for the respective financial year is due;
- In the event of legal/judicial disputes arising in connection with the conclusion or performance of the Agreement or any activity in connection with its performance, or other administrative or judicial proceedings relating to the performance or activities under the Agreement, the personal data referred to in item 3.2.1 may be processed by Evrotrust for longer periods than those specified above if necessary for the establishment, exercise or defense of legal claims (e.g. in the event of a legal dispute or other proceedings for the period during which the case is pending, and for up to five (5) years from the date of the final conclusion of the relevant case before all instances) or if the applicable legislation provides for the processing of the data for a longer period.

3.2.3. The Data Subjects referred to in item 3.2.1 may exercise their rights against Evrotrust by using the contact details of the data protection officer of Evrotrust set out in the Special Terms and Conditions.

4. Personal Data Relating to customers

4.1. Provision of technical support by Evrotrust to Data Subjects using Evrotrust's services within the framework of the Agreement

4.1.1. The Parties agree that for the purposes of such provision of technical support by Evrotrust to Data Subjects-customers of the Partner using Evrotrust's services within the Partner's software/ systems under the scope of the Agreement:

- a) The following Personal Data may be provided by the Partner to Evrotrust: names, e-mail,

company e-mail, phone number, company phone number, name of company the User works for or represents, position in the company, department, other data that may be connected to the above data, e.g. by being provided in the User's contact details;

b) The following Personal Data may be provided by Evrotrust to the Partner: Information about the status of the User's account with Evrotrust, reasons for that status (e.g. invalid document, unclear image of document, other facts concerning the registration process or the use of Evrotrust services), information about actions recommended to User, information about updated status of the User's account.

4.1.2. The Parties will exchange the Personal Data under item 4.1.1:

a) for the following purposes:

- Legitimate interest of the Parties: Provision of services by Partner and Evrotrust to the Data Subject in his/her capacity of user of Evrotrust/ customer of the Partner, respectively. The following Personal Data under item 4.1.1 may be provided for this purpose – e-mail, company e-mail, phone number, company phone number. Said Personal Data will be provided via the technical API integration between Partner's software and Evrotrust's system for provision of trust service to users via Evrotrust's mobile application;
- Legitimate interest of the Parties: Provision of support services to the Data Subject in the course of his/her use of Evrotrust services via Partner's software, under respective agreements concluded with said Data Subject in his/her capacity of user of Evrotrust/customer of the Partner, respectively. All data under item 4.1.1 may be provided for this purpose;
- Legitimate interest of the Parties: Execution of obligations of the Parties under the Agreement pertaining to customer support and exercise and protection of the legal rights and interests of the Parties. All data under item 4.1.1 may be provided for this purpose.

b) for the following terms:

- For the entire term of the Agreement and for up to five (5) years from termination;
- In case the personal data are contained in documents necessary for the purposes of tax and social security control – for a period of up to ten (10) years, starting from the beginning of the year following the year in which the payment of the public obligation for taxes or compulsory social security contributions related to the records kept for the respective financial year is due;

- In the event of legal/judicial disputes arising in connection with the conclusion or performance of the Agreement or any activity in connection with its performance, or other administrative or judicial proceedings relating to the performance or activities under the Agreement, the Personal Data referred to in item 4.1.1 may be processed by Evrotrust for longer periods than those specified above if necessary for the establishment, exercise or defence of legal claims (e.g. in the event of a legal dispute or other proceedings for the period during which the case is pending, and for up to five (5) years from the date of the final conclusion of the relevant case before all instances) or if the applicable legislation provides for the processing of the data for a longer period.

4.1.3. The Data Subjects referred to in item 4.1.1 may exercise their rights against Evrotrust by using the contact details of the data protection officer of Evrotrust set out in the Special Terms and Conditions.

4.2. Partner acting as Registration Authority and providing data of previously identified customers, incl. when using an Electronic Channel

This section 4.2 applies only to Partners who, while acting as a Registration Authority for Evrotrust, provide to Evrotrust personal data of customers who have been previously identified by them on their own legal ground, incl. in the context of these Partners' Registration Authority activities carried out via Electronic Channels, if any.

4.2.1. Partner shall provide to Evrotrust the following categories of data of Data Subjects who have previously been identified by Partner as per the requirements of Evrotrust's Clause "Registration Authority" and who, as of the moment of providing the data, are Partner's customers or are in a pre-contractual relations with the Partner, and with regard to this the Partner has gathered and processes these data as an independent data controller for its own purposes and on its own legal ground: full names as provided within personal ID document, country of issuance of the ID document, personal unique identifier, number of ID document, mobile phone number, e-mail address.

4.2.2. Evrotrust shall process the data provided under item 4.2.1 for the purpose of identifying the Data Subject and concluding a contract for provision of Trust Services between Evrotrust and the Data Subject. The data will be processed by Evrotrust only for this purpose until the

conclusion of the contract with the Data Subject. Further processing of the same data may be performed by Evrotrust on the basis of the contract concluded with the Data Subject, for the purposes and under the terms defined in Evrotrust's Privacy policy applicable to the trust, information, cryptographic and other services provided by Evrotrust, its current version published on Evrotrust's website here: <https://evrotrust.com/resources/tsp-documents>.

4.2.3. Partner is solely responsible, and with each provision of data under item 4.2.1 above declares that:

- (a) Partner has a valid legal ground under the Regulation and Applicable Data Protection Rules to process the data under item 4.2.1 above, including to provide it to Evrotrust as specified in this Clause;
- (b) Partner has duly informed Data Subject of the processing of the data as specified in this Clause, including of the provision of said data to Evrotrust for the purpose under item 4.2.2 above; and
- (c) the data provided to Evrotrust is complete, correct and up to date.

4.3. Processing of personal data in relation to the bioID functionality

4.3.1. The Parties agree that, in connection with the processing of Data Subjects' biometric data necessary to provide the bioID functionality under the Agreement, Evrotrust will collect the necessary consent of the Data Subjects to do so, and the Partner will notify, as required by applicable law, the relevant Data Subjects of the need for their confirmation, through facial recognition, of certain actions with respect to the Partner and will provide such Data Subjects with an alternative way to execute such actions in case the Data Subjects do not want to go through the process of facial recognition through the bioID functionality. Biometric data processed in connection with bioID does not reach and is not accessed by the Partner at any moment during the process of requesting and using this functionality.

4.4. Data Subjects who are customers to both Parties

4.4.1. For the purposes of the performance of the Agreement and the implementation thereof, each Party may also process personal data concerning Data Subjects who are customers of its services and who request the conclusion of a contract with the other Party

and/or use and/or request services provided by the other Party, including where Data Subjects require a Party to provide their Personal Data to the other Party on their behalf as a part of and in the course of using a service. Each Party is a data Controller in respect of the processing of personal data it carries out for the purposes of providing its own services to its customers and of carrying out its other activities and will process such data in accordance with the Applicable Rules and its rules and policies.

4.4.2. The Parties undertake, in cases where the performance of the Agreement requires additional data exchange concerning Data Subjects who are their customers, to sign additional agreements concerning the respective integrations and data exchanges settling the specific categories of personal data that will be subject to such exchange, purposes and periods for processing of such data, the rights and obligations of Parties in relation to said exchanges, as well as the specific technical and organisational measures they will apply to protect the data exchanged, if these are not already regulated by this Clause.

5. Obligations of the Parties when processing Personal Data as Data Controllers

5.1. In connection with the processing of Personal Data referred to in this Section I, each Party warrants to the other Party:

- (a) that it implements appropriate technical and organizational measures in accordance with the requirements of the Regulation and the Applicable Data Protection Rules and undertakes to ensure the protection of the rights of Data Subjects;
- (b) that staff who will have access to the personal data have undergone introductory and regular training on the processing and protection of personal data, tailored to the specific processing activities and the specific risks associated with the processing of personal data, and that any person who will have access to personal data has undertaken a confidentiality obligation or is legally bound to respect confidentiality.

5.2. In connection with the processing of personal data referred to in this Section I, each of the Parties undertakes:

- (a) to be fully compliant with the applicable legislation concerning the treatment of the information it processes in the course of its business;
- (b) to make appropriate arrangements with Data Subjects to ensure the lawful exchange of

personal data necessary for the performance of the Agreement, including but not limited to providing them with full, clear and comprehensible information about the exchange of data;

(c) to comply with its obligation to notify the supervisory authority in case of a personal data breach;

(d) to comply with its obligation to notify the Data Subject of a personal data breach;

(e) to notify the other Party accordingly in the event:

- that it determines that the legal basis on which it processes personal data received from the other Party in accordance with this Clause has ceased to exist;
- of rectification, erasure or restriction of the processing of personal data which have been transmitted to the other Party, carried out in accordance with Articles 16, 17 (1) and 18 of the Regulation, unless this is impossible or requires a disproportionate effort.

SECTION II

CONTROLLER - PROCESSOR RELATIONS - PARTNER ACTING AS PROCESSOR ON BEHALF OF EVROTRUST

This Section applies only to Partners having the role of a Processor of personal data for Evrotrust in the course of their activities as a Registration Authority for Evrotrust, and does not include Registration Authority activities carried out as described under item 4.2 above.

6. Nature of the processing of Personal Data by the Partner as a Processor

6.1. The Partner has the role of a Processor for Evrotrust where Partner operates as a Registration Authority under Article 3, para. 2 of Evrotrust's Clause "Registration Authority", i.e. where the Partner identifies natural persons for the purposes of issuing of qualified certificates for qualified electronic signature (QCQES) with short-term validity, and the identified person applies for the short-term QCQES on site before the Partner's Registration Agent, as per the relevant rules and conditions of Clause "Registration Authority". In the course of these activities the Partner will process personal data on behalf and by assignment of Evrotrust solely for the purposes of carrying out these activities, in accordance with the requirements of the Agreement, the Policies and the requirements of applicable law.

6.2. The processing of personal data by the Partner as a processor on behalf of Evrotrust

shall be carried out in strict compliance with the requirements set out by Evrotrust in this Clause regarding the purpose, extent, scope and duration of the processing of personal data and in accordance with all Applicable Rules.

6.3. The processing of personal data by the Partner in its capacity as Processor of personal data on behalf of Evrotrust will be carried out for the territory of the European Union ("Processing Territory"), unless and only as expressly otherwise provided in this Clause. The Partner shall not be permitted to use any equipment for processing personal data as a processor located outside the designated Processing Territory, unless and only as expressly otherwise provided in this Clause.

6.4. When Partner processes personal data on behalf of Evrotrust, the Partner may not involve another processor without the prior express written permission of Evrotrust for each specific processor. The Partner undertakes to keep an up-to-date register of all sub-processors it has involved in the processing as provided under this paragraph. The register shall contain the full name and contact details of each sub-processor, the Data Protection Officer (if any) or, if none, other relevant contact person, and the categories of processing activities carried out by the sub-processor. Where a processor or sub-processor is appointed by Partner under the conditions of item 11.1 (b) of this Clause, the agreement with the third party shall be governed by the relevant texts of the SCC, as completed in accordance with this Clause.

7. Personal data processing activities of the Partner as a Data Processor

7.1. For the purposes of item 6.1 above, the Partner will carry out the following personal data processing activities:

7.1.1. **Activity 1:** Acceptance and processing of applications from Users for the issuance and maintenance of electronic signature certificates under the trademark Evrotrust® on the territory of the European Union as a Registering Authority of Evrotrust and personal identification of Users for the purpose of issuing a Qualified Certificate for Qualified Electronic Signature (QCQES).

a) Categories of Data Subjects: Users who request to the Partner as a Registration Authority of Evrotrust the conclusion of a contract for the issuance and maintenance of qualified

electronic signature certificates under the trademark Evrotrust®;

b) Types of personal data processed by the Partner:

- identification data: names, personal identification number, address, photo of the person on the identity document, information related to the identity document (identity document number, date and authority of issuance, country of issuance);
- contact details: mobile phone number and email address;
- a scanned image of an identity document;
- other data included in the application for electronic signature as requested services.

c) Term of the processing: for the duration of the Agreement;

d) Nature of the processing and its requirements: Performing all actions necessary for the acceptance and processing of applications for the issuance and maintenance of electronic signature certificates, including but not limited to:

- comparison of and confirmation of the correspondence between the physical characteristics of the User appearing in person with the data from the identity document (photo, other information about physical identity);
- confirmation/verification of the conformity of the data sent with the data on the identity document submitted by the User;
- entering and sending the User's identification data, contact details and other data necessary for requesting and issuing an electronic signature to the Evrotrust System via the specialized API for connectivity with the Evrotrust System in accordance with the forms approved by Evrotrust and confirming the compliance of the entered data with the data from the identity document submitted by the User;

All of the activities described above are performed only by an authorized Agent of the Partner through the provided personal access account.

7.1.2. **Activity 2:** Assistance to the client to enable the use of the Evrotrust eID service

a) Categories of Data Subjects: Users who request the Evrotrust eID service (available only with the simultaneous using of the Evrotrust-branded QCQES) to the Partner as Evrotrust Registration Authority.

b) Types of Personal Data processed by the Partner:

- identification data: name, personal identification number (if available), information

related to the identity document (identity document number, date and authority of issuance, country of issuance, photograph, scanned image of the identity document);

- contact details: mobile phone number and email address;

c) Term of the processing: for the duration of the Agreement.

All of the described activities are performed only by an authorized Agent of the Partner through the provided personal access account.

8. Obligations of the Partner acting as Processor on behalf of Evrotrust

8.1. When carrying out the personal data processing activities under this Section II, the Partner:

8.1.1. undertakes to implement appropriate technical and organizational measures in accordance with the requirements of the Regulation and the Applicable Rules and to ensure the protection of the rights of Data Subjects. For the avoidance of doubt, the Partner shall ensure that it implements, as a minimum, the technical and organizational data protection measures described in Annex II to this Clause.

8.1.2. ensures that each of the Agents (Partner's staff) who have access to personal data has received introductory and regular training on the processing and protection of personal data, tailored to the specific processing activities and the specific risks associated with the processing of personal data. The Partner shall ensure that any person who has access to personal data has committed to confidentiality or is required by law to respect confidentiality.

8.1.3. is obliged to notify Evrotrust immediately in the event of:

- a) any investigative activities undertaken by a data protection supervisory authority in relation to personal data processing activities pursuant to this Section II;
- b) that it finds that it is unable to perform its obligations under this Clause for any reason;
- c) it becomes aware of any breach of security of personal data it processes on behalf of Evrotrust. Notification of a breach of security should be made to Evrotrust promptly, but no later than twenty-four (24) hours from the time of discovery, and should contain at a minimum the following information:
 - a description of the nature of the breach and of the facts relating to the personal data breach, including, if possible, the categories and approximate number of data subjects

affected, the categories of data and the approximate quantity of personal data records affected;

- a description of the possible consequences of the personal data breach;
- a description of the measures taken or proposed by the Partner to address the personal data breach, including, as appropriate, measures to mitigate any adverse effects.

In the event that it is objectively impossible to provide all the information necessary for the notification within the abovementioned time limit, the Partner shall notify Evrotrust within this time limit by providing it with the information available at that time and, in agreement with Evrotrust, supplement the notification.

d) to assist Evrotrust in every possible way in fulfilling Evrotrust's obligations to document the personal data breach and in notifying the supervisory authority of the breach, by promptly providing Evrotrust with any information requested by the latter that is necessary to document the breach and to notify the supervisory authority;

e) where a Data Subject makes a direct enquiry to the Partner in relation to the personal data processing activities carried out pursuant to this Section II, unless the Partner, pursuant to further documented instructions from Evrotrust, has committed to respond directly to such enquiries;

f) where the Partner establishes that there is a legal obligation to, or there is a request from a governmental, administrative, judicial and/or other authority to provide personal data that it processes on behalf of Evrotrust, except where such notification is contrary to mandatory provisions of law;

8.1.4. to provide Evrotrust with access to all information necessary to demonstrate the Partner's compliance with its obligations under this Clause relating to the processing activities on behalf of Evrotrust, and to permit and assist audits, including inspections, by Evrotrust or any other auditor authorized by Evrotrust and to respond to any enquiries by Evrotrust regarding the processing activities under Section II of this Clause;

8.1.5. to assist Evrotrust, in any way possible, including but not limited to, complying with Evrotrust's specific instructions and providing it with requested information, in fulfilling its obligation to respond to requests to exercise the Data Subjects' rights under Chapter III of the Regulation;

8.1.6. not to transfer personal data it processes pursuant to this Section II to a third country or an international organization, except where it is obliged to do so under Union or Member State law applicable to the Partner, in which case the Partner shall inform Evrotrust of this legal requirement prior to the transfer, unless that law prohibits such information on important public interest grounds;

8.1.7. not to process personal data on behalf of Evrotrust outside the territory of the European Union ("Processing Territory"), unless Data Subject has physically appeared before Partner's Agents outside of the Processing Territory. In those cases, processing shall be carried out as per the requirements of Section IV of this Clause.

8.1.8. to assist Evrotrust in fulfilling its obligation to notify the Data Subject of a personal data breach under Article 34 of the Regulation, in any way possible, including, but not limited to, by complying with Evrotrust's specific instructions and providing the requested information;

8.1.9. if and insofar as applicable, assist Evrotrust in fulfilling its obligation to carry out a data protection impact assessment under Article 35 of the Regulation, if necessary, in any way possible, including, but not limited to, by providing it with the requested information;

8.1.10. if and to the extent applicable, assist Evrotrust in fulfilling its obligation to carry out prior consultation with the supervisory authority under Article 36 of the Regulation, in any way possible, including but not limited to, by providing it with the requested information;

8.1.11. maintain a written record of all categories of processing activities carried out on behalf of Evrotrust, at least with the content required by the Regulation;

8.1.12. to compensate for any damages that a person may suffer as a result of processing of personal data carried out by the Partner, which processing violates the Regulation or other Applicable Data Protection Rules, unless the Partner proves that it is in no way responsible for the damages and/or has carried out the processing in accordance with Evrotrust's instructions;

8.1.13. In the event of termination of the Agreement or of the processing activities under this Section II by the Partner, at the option of Evrotrust, to return to Evrotrust all Personal Data it has collected and processed on Evrotrust's behalf or to delete all existing copies of such data, unless there is a proper basis for the Partner to continue processing and Union law requires its retention. The Partner shall confirm in writing to Evrotrust that the personal data has been

returned, deleted and/or stored.

8.1.14. In the event that, following the cessation of specific personal data processing activities under this Section II, the Partner needs to continue to store personal data that it has collected and processed on behalf of Evrotrust, the Partner undertakes to notify Evrotrust of the legal basis for the storage and agrees and warrants that it will store it in compliance with the Regulation and other Applicable Data Protection Rules.

SECTION III

CONTROLLER - PROCESSOR RELATIONS - EVROTRUST AS A PROCESSOR ON BEHALF OF THE PARTNER

This Section only applies in case of provision of the basicID service by Evrotrust

9. Nature of the processing of Personal Data by Evrotrust as a Processor

9.1. Evrotrust has the role of a Processor for the Partner when providing the basicID service to the Partner, pursuant to the Agreement. The basicID service is a non-regulated information society service provided through Software as a Service (SaaS) delivery model, allowing Partner to use the technology integrated into Evrotrust's Mobile SDK for the purpose of gathering individuals' personal data for purposes, scope and duration as defined within Partner's relevant privacy policy/ies and/or other documentation. In the course of the provision of the basicID service by Evrotrust the Partner acts as Data Controller as it is the Partner who determines the purposes of the processing of the personal data through the basicID service. As a Data Controller, the Partner is responsible for ensuring the legal basis for the processing of personal data in compliance with the Applicable Rules and for ensuring that all processing activities adhere to all relevant laws and regulations in force. Evrotrust processes personal data on behalf and under the assignment of the Partner, solely for the purposes of carrying out activities related to the basicID service, in accordance with the requirements of the Agreement, the Applicable Rules, and the Documented Instructions, as defined in item 9.2 below, provided by the Partner.

9.2. The Partner and Evrotrust agree that this Clause, the Agreement, and the instructions provided by the Partner via relevant configuration tools throughout the implementation by

the Partner of the Evrotrust's Mobile SDK in Partner's mobile application, including the selection made by the Partner of specific categories of data, constitute Partner's documented instructions regarding the processing by Evrotrust of personal data through the provision of the basicID service ("Documented Instructions"). Evrotrust will process such personal data on behalf of the Partner only in accordance with the Documented Instructions. Additional instructions outside the scope of the Documented Instructions (if any) require prior written agreement between Evrotrust and the Partner, incl. agreement on any additional fees payable by the Partner to Evrotrust for carrying out such instructions. The Partner is entitled to cease using the basicID service and terminate the Agreement in its part settling the provision of said service, pursuant to its termination terms and conditions, if Evrotrust declines to follow instructions requested by the Partner which are outside the scope of, or changed from, those given or agreed to be given in this Clause.

9.3. Taking into account the nature of the processing, the Partner agrees that it is unlikely that Evrotrust can form an opinion on whether Documented Instructions infringe the Applicable Rules. In case Evrotrust forms such an opinion, it will inform the Partner accordingly.

9.4. The Partner undertakes to comply with all Applicable Rules and relevant regulations, specifically in relation to its capacity as Data Controller, and binding on it in the performance of the Agreement and this Clause. More specifically, the Partner undertakes to ensure the legal basis for the processing, especially when instructing Evrotrust on the processing of scanned identity documents, to provide the necessary information to Data Subjects regarding the processing of their personal data as required by the Applicable Rules, pursuant to item 9.6 below, as well as to gather all necessary Data Subject's consents, notably in relation to the processing of biometric data and to the automated decision-making involved in the process of the provision of the basicID service, pursuant to item 9.5 below.

9.5. The Partner understands that the basicID service includes processing of biometric data extracted in the course of analysis of the facial features of the Data Subject, as well as automated decision-making regarding the matching of facial features of the Data Subject activating the service with those available in the photo extracted from the official identification documents registry, where available, or from the identification document provided by the

Data Subject. Partner is obliged and undertakes to arrange its relationship with Data Subjects by gathering their express prior consent for processing of biometric data and for automated decision-making by using a template “Declaration of Consent for Automated Processing of Biometric Data” provided by Evrotrust for this purpose.

9.6. The Partner is obliged and undertakes to arrange its relationship with Data Subjects in its relevant privacy notice as required by the Regulation, including by adding at least the following text in the relevant section informing data subjects on the engagement of third-party service providers processing their personal data on Partner’s behalf: *“Evrotrust Technologies AD, unified identification code 203397356, headquarters and registered address: Sofia 1766, Mladost region, 251G(Г) Okolovrasten pat Str., 5th floor, tel. (+359 2) 448 58 58, e-mail address: office@evrotrust.com (Evrotrust). Evrotrust provide [Partner] with SaaS solutions and technologies helping identify users accessing [the Application]. Evrotrust processes personal data, including biometric data, on [Partner’s] behalf and pursuant to [Partner’s] instructions, and is contractually obligated to handle your data securely and in compliance with applicable data protection laws, including the General Data Protection Regulation (GDPR).”*

9.7. The basicID service is built upon a technology which automatically gathers the personal data as defined in item 10.1.1 (b) below, on behalf of the Partner. Pursuant to Partner’s Documented Instructions certain data selected by Partner is kept and processed by Evrotrust for the term defined in item 10.1.1 (c) below, while the rest of the data is immediately deleted.

10. Personal data processing activities of Evrotrust as a Data Processor

10.1. For the purposes of item 9.1 above, Evrotrust will carry out the following personal data processing activities:

10.1.1. Activity 1: Gathering personal data in a process of facial scanning and extraction of information from the personal identification document via the Data Subject’s mobile device camera, verification in real time of such data against official data from relevant registries of personal identification documents, if available, and provision of gathered data to the Partner through the Mobile SDK, together with information on the percentage of likelihood that the Data Subject being identified is the same as the person on the identity document.

a) Categories of Data Subjects: customers/clients of the Partner whom the Partner wishes

to identify using data gathered through the basicID service provided by Evrotrust.

b) Types of personal data which may be processed by Evrotrust:

- Information extracted from the identity document through the mobile device camera:
 - identification data: names, personal identification number, address;
 - information related to the identity document: identity document number, date and authority of issuance, country of issuance;
 - scanned image of the picture on the identity document;
 - scanned image of personal identification document.
- Information gathered from the live facial scanning of the Data Subject through their mobile device camera: image and video of the person's face.
 - Biometric data: one-time automated analysis and comparison of specific facial features (from a video session and a photo in an identification document) and indicators on whether a living human is participating in the identification video session – subject to express prior consent of the Data Subject as described in item 9.5 above.
 - Biometric identifier (FaceMap), which does not constitute and does not contain any biometric data and does not allow reverse recovery of biometric data.

c) Term for processing of personal data in accordance with item 9.7 above: one (1) year as of gathering or until termination of the Agreement, whichever is sooner.

d) Nature and purpose of the processing: Performing actions necessary to gather information on the person through the basicID service and to establish with a certain degree of certainty whether the person being identified is the same as the person on the identity document, including but not limited to;

- extraction of information from the submitted identity document and from the facial scanning of the Data Subject;
- comparison and confirmation of the correspondence between the physical characteristics of the Data Subject appearing in person before the mobile device camera with the data extracted from the identity document;
- verification of the conformity of the data extracted from the identity document with official data available in relevant registries of personal identification documents, if available;
- provision of the extracted/ verified data to the Partner, along with information on the

level (percentage) of correspondence between the physical characteristics of the Data Subject appearing in person before the mobile device camera with the data extracted from the identity document, through Evrotrust's Mobile SDK.

10.2. The processing of personal data by Evrotrust in its capacity of Processor will be carried out according to the following principles and requirements:

10.2.1. Evrotrust has implemented and will maintain the technical and organizational measures as described in Annex II to this Clause.

10.2.2. Evrotrust ensures that each member of its personnel who has access to personal data has received introductory and regular training on the processing and protection of personal data, tailored to the specific processing activities and the specific risks associated with the processing of personal data. Evrotrust ensures that any person who has access to personal data has committed to confidentiality or is required by law to respect confidentiality.

10.2.3. In case a Data Subject makes a request to Evrotrust, Evrotrust will promptly forward such request to the Partner once Evrotrust has identified that the request is from a Data Subject for whom the Partner is responsible. The Partner authorizes Evrotrust to respond to any Data Subject who makes a request to Evrotrust, to confirm that Evrotrust has forwarded the request to the Partner.

10.2.4. Evrotrust will (i) notify the Partner of a security incident concerning data processed under this Section III without undue delay after becoming aware of such security incident, and (ii) take appropriate measures to address the security incident, including measures to mitigate any adverse effects resulting from the such incident. Evrotrust's obligation to report or respond to a security incident will not be construed as an acknowledgement by Evrotrust of any fault or liability of Evrotrust with respect to the security incident.

10.2.5. To enable the Partner to notify a security incident to supervisory authorities or data subjects (as applicable), Evrotrust will cooperate with and assist the Partner by including in the notification under item 10.2.4 (i) such information about the security incident as Evrotrust is able to disclose to the Partner, taking into account the nature of the processing, the information available to Evrotrust, and any restrictions on disclosing the information, such as confidentiality or requirements stemming from Evrotrust's other regulated activities as Qualified Trust Service Provider within the meaning of Regulation (EU) 910/2014. Taking into

account the nature of the processing, the Partner agrees that, as Data Controller, it is best able to determine the likely consequences of a security incident.

10.2.6. The Partner agrees that an unsuccessful security incident will not be subject to items 10.2.4 and 10.2.5 above. An unsuccessful security incident is one that results in no unauthorized access to personal data processed or stored by Evrotrust on behalf of the Partner, and could include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents).

10.2.7. Evrotrust will make available to the Partner Evrotrust's certificate issued for the ISO 27001 certification (or the certifications or other documentation evidencing compliance with such alternative standards as are substantially equivalent to ISO 27001).

10.2.8. Evrotrust uses external auditors to verify the adequacy of its security measures. Such audit (i) is performed regularly; (ii) is performed according to ISO 27001 standards or such other alternative standards that are substantially equivalent to ISO 27001; (iii) is performed by independent third-party security professionals at Evrotrust's selection and expense; and (iv) results in the generation of an audit report ("Report"), which is considered Evrotrust's internal and Confidential Information. At Partner's written request, and provided that the parties have an applicable NDA in place, Evrotrust will provide the Partner with an excerpt or summarized information from the Report so that the Partner can reasonably verify Evrotrust's compliance with its obligations under this Clause, except for parts of the report that are classified or related to critical infrastructure and systems functionality, or disclosure of which would result in risk of revocation of Evrotrust's right to provide electronic identification and/or trust services under Regulation 910/2014 or other applicable legislation.

10.2.9. In case the Partner wishes to conduct any audit, including any inspection, the Partner has the right to request such audit exclusively by instructing Evrotrust to carry out the audit described in items 10.2.7. and 10.2.8 above. For avoidance of any doubt, the Partner and Evrotrust agree that Evrotrust's mobile application backend and systems can only be accessed by a qualified and experienced auditor at Evrotrust's selection, bound by confidentiality obligations, and in any case such access will be limited to the extent allowed by Regulation

910/2014 and other applicable legislation without invoking risk of revocation of Evrotrust's right to provide electronic identification and/or trust services.

10.2.10. If the Partner wishes to change the instructions regarding the audit as defined under item 10.2.9 above, then the Partner has the right to request a change to this instruction by sending Evrotrust a written notice as provided for in the Agreement. If Evrotrust declines to follow any instruction requested by the Partner regarding audits, including inspections, the Partner is entitled to terminate the part of the Agreement concerning the provision of the basicID service in accordance with the Agreement's termination terms and conditions.

10.2.11. In the event of partial termination of the Agreement regarding the basicID service or of the processing activities of Evrotrust under this Section III, Evrotrust will, at the option of the Partner, return to the Partner all personal data it has collected and processed on Partner's behalf or to delete all existing copies of such data, unless there is a proper basis for Evrotrust to continue the processing and/or EU law or other applicable legislation requires its retention. Evrotrust will confirm in writing to the Partner that personal data has been returned, deleted and/or stored.

10.2.12. The processing of personal data by Evrotrust as a Processor on behalf of the Partner will be carried out on the territory of the EU/EEA ("Processing Territory"), unless otherwise provided in this Clause or agreed with the Partner, or except where Evrotrust is obliged to do so under Union or Member State law applicable to it, in which case Evrotrust shall inform the Partner of this legal requirement prior to the transfer, unless that law prohibits such information on important public interest grounds. Evrotrust will not use any equipment for processing of personal data located outside the designated Processing Territory, unless otherwise provided in this Clause or agreed with the Partner.

10.2.13. The Partner provides general authorization to Evrotrust's use of sub-processors to provide processing activities on behalf of the Partner for the provision of the basicID service ("Sub-processors") in accordance with item 10.2.14. Evrotrust will inform the Partner at least thirty (30) days prior to engaging a Sub-processor. To object to a Sub-processor, the Partner can cease using the basicID service and terminate the Agreement in its part settling the provision of said service pursuant to its termination terms and conditions.

10.2.14. In case Evrotrust engages any Sub-processor(s), it undertakes to keep an up-to-

date register of such Sub-processor(s). Evrotrust also undertakes (i) to restrict Sub-processor's access to what is strictly necessary for the performance of the service, (ii) to enter into a written agreement with the Sub-processor and to impose to the latter the same data protection obligations as those defined under the present Clause, to the extent that the Sub-processor performs the same data processing activities as those provided by Evrotrust.

SECTION IV

PARTNERS LOCATED AND/OR PROCESSING DATA OUTSIDE THE EU/EEA

This Section only applies to Partners established and/or having their main place of commercial activities and/or processing Personal Data subject to this Clause in a country outside of the European Union and the European Economic Area

11. Partners acting as Processors

11.1. Where Partner processes personal data as a Processor for Evrotrust according to Section II of this Clause outside of the EU/EEA, and only as regards these activities, the provision by Partner of data gathered outside of the EU/EEA directly to Evrotrust for further processing within the EU/EEA does not constitute transfer of personal data to a third country or an international organization within the meaning of the Regulation. In those cases, Partner:

- (a) Shall be permitted to use equipment located outside of the EU/EEA for processing personal data as a Processor for Evrotrust only to the extent necessary for the purpose of collecting data of Data Subjects appearing before Partner outside of the EU/EEA and providing those data to Evrotrust;
- (b) Shall not use any sub-processor for data processed under Section II of this Clause, unless with Evrotrust's explicit prior consent expressed in writing and in the presence of a respective data protection agreement concluded with the sub-processor, as provided in this Clause.

11.2. If, nevertheless, and only to the extent it may be considered that in the cases of item 11.1 above or in the instances under Section III of this Clause there is a transfer of personal data to a third country or an international organization within the meaning of the Regulation, then to the same extent the SCC Module Two shall apply to Personal Data that is protected by the Regulation and processed outside the EEA, completed as follows:

- a) in Clause 7, the optional docking clause will apply;
- b) in Clause 9, Option 2 will apply, and the time period for prior notice of Sub-Processor changes shall be thirty (30) days;
- c) in Clause 11, the optional language will not apply;
- d) in Clause 17, Option 1 will apply, and the SCCs will be governed by Bulgarian law;
- e) in Clause 18(b), disputes shall be resolved before the courts of Bulgaria;
- f) Evrotrust shall be the data exporter outside of the territory of the EU/EEA, and Partner shall be the relevant data importer;
- g) Annex I of the SCC shall be deemed completed with the relevant information set out in Annex I.A to this Clause; and
- h) Annex II of the SCC shall be deemed completed with the information set out in Annex II to this Clause.

12. Partners acting as Controllers

Where Partner is located and/or processes personal data received by Evrotrust outside of the EU/EEA, and only as regards Partner's activities as an independent Controller of Personal Data under this Clause, the SCC shall apply to Personal Data that are protected by the Regulation and processed outside the EEA, completed as follows:

- a) Module One will apply;
- b) in Clause 7, the optional docking clause will apply;
- c) in Clause 11, the optional language will not apply;
- d) in Clause 17, Option 1 will apply, and the SCCs will be governed by Bulgarian law;
- e) in Clause 18(b), disputes shall be resolved before the courts of Bulgaria;
- f) Evrotrust shall be the data exporter outside of the territory of the EU/EEA, and Partner shall be the relevant data importer;
- g) Annex I of the SCC shall be deemed completed with the relevant information set out in Annex I.B to this Clause; and
- h) Annex II of the SCC shall be deemed completed with the information set out in Annex II to this Clause.

13. The Parties do not aim to contradict or restrict any of the provisions of the SCC. If and to the extent the SCC conflict with any provision of the Agreement (including this Clause) the SCC shall prevail to the extent of such conflict.

14. If, in the course of the relationship between the Parties, a situation concerning personal data processing arises which is not expressly provided for in this Clause, the rules of this Clause shall apply accordingly to the extent possible without contradicting the Regulation and Applicable Data Protection Rules, until the situation is expressly arranged with an additional agreement between the Parties, if this is necessary.

ANNEX I**APPLICATION OF SCC UNDER SECTION IV OF THIS CLAUSE****A. Transfers in the framework of Controller - Processor relations****LIST OF PARTIES**

Data exporter(s): Evrotrust Technologies AD, relevant information provided for the in General Terms and Special Terms of the Agreement.

Role: Controller/ Processor

Data importer(s): The entity defined as Partner within the relevant Special Terms of the Agreement.

Role: Processor/ Controller

DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

- a. Data Subjects under item 7.1.1 (a) of this Clause.
- b. Data Subjects under item 7.1.2 (a) of this Clause.
- c. Data Subjects under item 10.1.1 (a) of this Clause.

Categories of personal data transferred

- a. Data under item 7.1.1 (b) of this Clause.
- b. Data under item 7.1.2 (b) of this Clause.
- c. Data under item 10.1.1 (b) of this Clause.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

None anticipated.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous for the term of the Agreement.

Nature of the processing

- a. The activities described in item 7.1.1 (d) of this Clause.
- b. Activities necessary to assist the Data Subject with the activation of the eID service.
- c. The activities described in item 10.1.1 of this Clause

Purpose(s) of the data transfer and further processing

The purposes described in item 6.1 and in item 9.1 of this Clause.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

For the duration of the Agreement or for one (1) year – for basicID service.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Data importer may engage other companies to provide parts of the service on data importer's behalf only after express written consent of data exporter.

COMPETENT SUPERVISORY AUTHORITY

Bulgarian Commission for Personal Data Protection

B. Transfers in the framework of Controller - Controller relations

LIST OF PARTIES

Data exporter(s): Evrotrust Technologies AD, relevant information provided for the in General Terms and Special Terms of the Agreement.

Role: Controller

Data importer(s): The entity defined as Partner within the relevant Special Terms of the Agreement.

Role: Controller

DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

- a. Data Subjects provided in items 3.1.1 and 3.2.1 of this Clause;
- b. Data Subjects provided in item 4.1.1 and 4.2.1 of this Clause;
- c. Data Subjects provided in items 4.3.1 and 4.4.1 of this Clause.

Categories of personal data transferred

- a. Categories of personal data provided in items 3.1.1 and 3.2.1 of this Clause;

- b. Categories of personal data provided in item 4.1.1 and 4.2.1 of this Clause;
- c. Categories of personal data provided in the Privacy policy applicable to the trust, information, cryptographic and other services provided by Evrotrust Technologies AD, as may be amended from time to time, the current version published on Evrotrust's website here: <https://evrotrust.com/resources/tsp-documents>.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

None anticipated.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous for the terms set forth in this Clause.

Nature of the processing

Storage, combination, provision to pre-defined parties in the presence of relevant legal grounds.

Purpose(s) of the data transfer and further processing

- a. The purposes defined in items 3.1.2 (a) and 3.2.2 (a) of this Clause.
- b. The purposes defined in items 4.1.2 (a) and 4.2.2 of this Clause;
- c. The purposes defined in the Privacy policy applicable to the trust, information, cryptographic and other services provided by Evrotrust Technologies AD, as may be amended from time to time, the current version published on Evrotrust's website here: <https://evrotrust.com/resources/tsp-documents>.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

- a. The terms provided for in item 3.1.2 (b) and 3.2.2 (b) of this Clause.
- b. The terms defined in items 4.1.2 (b) and 4.2.2 of this Clause.
- c. The terms defined in the Privacy policy applicable to the trust, information, cryptographic and other services provided by Evrotrust Technologies AD, as may be

amended from time to time, the current version published on Evrotrust's website here:

<https://evrotrust.com/resources/tsp-documents>.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Data importer may engage other companies to provide parts of the service on data importer's behalf only after express written consent of data exporter.

COMPETENT SUPERVISORY AUTHORITY

Bulgarian Commission for Personal Data Protection

ANNEX II**MINIMUM TECHNICAL AND ORGANISATIONAL MEASURES**

Evrotrust has implemented and maintains the minimum technical and organization measures for protection of personal data as described in the table below. These measures ensure the following types of data protection: physical, personal, documentary, protection of automated information systems and/or networks, and cryptographic protection.

Evrotrust applies these measures when it acts as Data Controller pursuant to Section I of the Clause and as Data Processor pursuant to Section III of this Clause, and causes and requires Partners acting as Data Processors to implement these measures when processing personal data on its behalf, pursuant to Section II of this Clause.

Type of protection	Category of measures	Type of measures	Comments
Physical protection	Technical measures	Locking the premises	
		Designation of document storage cabinets	
		Fire extinguishing means/systems	
		Equipment of the premises where personal data are processed	
		Premises security/security systems	
	Organizational measures	Identification of the premises where personal data will be processed	
		Determination of the premises in which the elements of the communication and information systems for the processing of personal data will be located	
		Defining the physical access organization	

		Determination of the technical means of physical protection used	
		Designation of controlled access areas	
		Designation of areas with different levels of access	
Personal protection	Organizational measures	Knowledge of data protection legislation	
		Knowledge of the risks to personal data processed by the controller	
		Consent to undertake not to disclose personal data	
		Failure to share critical information among staff	
		Knowledge of data protection policies and guidelines	
		Staff training to respond to data security events	
Document checksum (hash)	Organizational measures	Determination of the records to be kept on paper	
		Determining the conditions for processing personal data	
		Regulation of access to registers	
		Determination of storage periods	
		Destruction procedures	
		Control of access to registers	
		Rules for propagation and distribution	
		Procedures for verification and control of processing	

Protection of automated information systems and/or networks	Technical measures	Identification and authentication	
		Records management	
		External links/connection	
		Protection against viruses	
		Copies/back-ups for recovery	
		Information carriers	

		Cryptographic protection	
		Pseudonymisation of data	
		Telecommunications and remote access	
		Maintenance/operation	
		Session access control	
	Organizational measures	Personal systems protection	
		Determination of storage periods for personal data	
		Media destruction/deletion/erasure procedures	
		Physical environment / surroundings	
		Data protection policies, security guides and standard operating procedures	
		Contingency planning	
		Staff training to respond to data security events	
Cryptographic protection	Cryptographic protection	Access over secure connection channels, https access and IP- VPN/SSL	
		Cryptographic protection in the transmission of information.	

This document is published in Bulgarian, English or another language. In case of discrepancy between the Bulgarian and English texts, the Bulgarian version of the text shall take precedence. In case of inconsistency between the English and other language versions of the text, the meaning of the English text shall prevail.