Operated by Evrotrust

Declaration of Consent for Automated Processing of Biometric Personal Data

The use of Version 2.0 Mobile Application (the Application) of Evrotrust Technologies AD (Evrotrust), UIC 203397356, having its registered office and business address at: 1113 Sofia City, Izgrev District, Iztok Residential Complex, No. 2 Nikolay Haytov Str., entrance 5, 2nd floor, head office: Sofia City, No. 101 Tsarigradsko Shosse Blvd., 6th floor, tel. (+359 2) 448 58 58, e-mail address: office@evrotrust.com, website: https://www.evrotrust.com/, and the services provided through it requires that Evrotrust processes your personal data, including biometric data, as well as makes decisions based on the automated processing of such data.

By checking the checkbox in front of the field “I give my explicit consent in accordance with this Declaration of Consent for automated processing of biometric data” and by clicking the “Continue” button, you give your explicit consent to the processing of your biometric data and to decision making based on the automated processing of your personal data by Evrotrust for the purposes described below. In order for the biometric data processing activities described below to be lawful, your explicit consent is required.

1. Purposes of the processing of biometric personal data and of making decisions based on automated processing of personal data:

   A. Initial automated identification

In order to securely identify you through the Application, Evrotrust needs:

- To process your biometric data - a one-time analysis and comparison of specific features of the facial image (from a video session and from a photo on an identity document) will be performed, and indicators of whether a living person is involved in the identification video session; **and, at the same time,**
- To make a decision, based on the automated processing of your data, which has a legally significant result for you - confirmation of your identification and issuance of a qualified certificate for qualified electronic signature (QCQES), or unsuccessful identification and a refusal to issue a QCQES remotedly, respectively.

A peculiarity of the processing performed by Evrotrust is that it is one-time - it is entirely completed within the current identification session and after its completion the processed biometric data are automatically deleted. Evrotrust keeps in a secure and encrypted manner only the result of the automated identification performed, in the form of a percentage of degree of correspondence between the analyzed images, which does not contain any biometric data.

During the automated identification, a 3D FaceMap (Biometric Identifier) will be generated. This Biometric Identifier will be stored in a secure enclave on your device only and will be entirely under

your control. Evrotrust in no way stores the 3D FaceMap generated in its systems and does not have any access to the secure enclave on your device.

The Biometric Identifier does not allow for the reverse recovery of your biometric data, but does allow for confirming in a unique and secure manner, in each subsequent activation of the facial recognition function within a video identification session in the Application, that you are the only one to identify yourself before the Application.

B. Automated re-identification

B1. Restoration of account access

In order for you to be able to restore your access to the Application, to your account and to your issued QCQES and other services, at each reinstallation of the Application, regardless of whether on the same or on a new device, you need to again go through automated identification and Evrotrust nees to again process your biometric data, through an analysis of specific features of your facial image within a new video session in the Application - a new temporary 3D FaceMap will be generated, which will be compared with your initial 3D FaceMap (Biometric Identifier) stored on your device or in a backup file, respectively, which you transferred when reinstalling your new device.

Before each start of such automated re-identification in the Application, a screen for starting a video identification session will appear and by pressing the “I'm ready” button, you express your explicit consent for the automated processing of your biometric data to start and for the identification to be performed.

Access to the Application, your account and your already active services (e.g. an already issued QCQES) will only be restored in case of exact matching of the two biometric identifiers – the initial and the current 3D FaceMap.

The processing of biometric data is one-time and immediately after their comparison, the biometric identifiers will be automatically deleted from the Evrotrust systems and only the initial 3D FaceMap (Biometric Identifier) will be saved in the secure enclave space on your device which Evrotrust does not have access to.

Going through automated re-identification is the only way in which Evrotrust can establish with certainty that the person requesting restoration of access to your user account is actually you and restore it accordingly. If at that time you no longer agree with the processing of your biometric data and with the decision making based on the automated processing of your personal data, you will not be able to restore your user account and use the Application through it. In such a case, if you wish to use the services of Evrotrust, you can request those that are related to in-person identification at an office of our Registration Authority.

B2. Signing documents or electronic identification (at the highest level of security)

In order to ensure the highest possible level of security, the Application does not support functionalities for the creation of security codes that require knowledge of the type of PIN code. Rather than by a PIN code, the access to the Application, as well as the activation of/request for services in the mobile application (e.g. request for the issuance of a QCQES, signing via a QCQES, etc.), and the confirmation of the making of any legally valid electronic statements in or through the Application, are confirmed using the biometric data recognition functionalities supported by your device (e.g. fingerprint, facial recognition, etc.). When using the biometric data recognition functionalities supported by your device, the biometric data remain completely under your control and do not reach, nor are stored by Evrotrust. Such data are only processed on your device.

In individual cases, however, a given Relying Party (e.g. a bank which you request a service from) may designate a given transaction as requiring the highest level of security - e.g. the highest level of security in signing a document via a QCQES or the highest level of security in electronic identification. In such cases, the standard biometric data recognition functionalities of your device is not sufficient for the signing of the relevant electronic document or for the provision of the electronic identification service, and automated re-identification will be performed in the manner described in “B1”. Such identification will only be performed after you have confirmed in the Application that it be performed. If you do not agree with such processing of your biometric data and the decision making based on the automated processing of your personal data, you may refuse to be identified in the relevant session. Such refusal will not prevent you from continuing to use the Application but, according to your relationship with the relevant Relying Party, may result in the Relying Party's refusal to deliver you the service for whose purpose it requested the signing of the document or your identification (e.g. remote opening of a bank account which requires your secure identification) or in the necessity for you to be identified by it in another manner (e.g. by appearing in person before the Relying Party), etc.

The screen for starting a video identification session will be displayed on your screen and by pressing the “I’m ready” button, you confirm your consent to proceed with it. Upon successful confirmation of your identification by the matching of the compared biometric identifiers, you successfully confirm the signing of the relevant electronic document and/or your electronic identification to the Relying Party.

Upon the completion of the video identification session, the biometric identifiers will be automatically deleted from the Evrotrust systems and only the initial 3D FaceMap (Biometric Identifier) will be saved in the secure enclave on your device, to which Evrotrust does not have access. The Relying Party does not have access to the biometric identifiers.

2. In the event of any change in your facial biometrics (e.g. as a result of trauma, surgical intervention, etc.), your automated re-identification will not be possible. In such a case, you can restore your access to the Application and your account if you have an updated identity document.

For this purpose, you will need to update your ID information and go through an automated identification process in accordance with “A”.

3. The giving of this consent is entirely voluntary and you may refuse to give it. However, in order to ensure the required level of security in your identification and in the provision, in a completely non-present manner, of qualified certification services, Evrotrust is obliged to apply an identification method that provides a level of security equivalent to the physical presence in terms of reliability. Therefore, automated (initial and re-) identification in the manner described herein and in the Personal Data Protection Policy, including the processing of biometric data, is a prerequisite for the activation of and the access to the Application, and for the use of qualified certification services through the Application. If you do not agree with the processing of your biometric data as described herein and/or do not agree with the decision making based on the automated processing of your personal data, please interrupt the registration process in the Application. In such a case, you may use the services of Evrotrust which are provided upon in-person identification (e.g. issuance of a qualified certificate for qualified electronic signature (QCQES) on a flash drive) after you have been identified in person at an office of Evrotrust’s Registration Authority.

Pursuant to Regulation (EU) 2016/679, a consent to the processing of personal data (in this case, biometric data) may be withdrawn at any time and such withdrawal shall not affect the lawfulness of the processing based on the consent prior to its withdrawal. In this regard, you may withdraw the consent given herein at any time. In order to withdraw the consent given herein, you need to deactivate your account and discontinue using the services of Evrotrust accessible through the Application. If, after having withdrawn your consent, you wish to continue using the services of Evrotrust, you may request services that require in-person identification (e.g. issuance of a qualified certificate for qualified electronic signature (QCQES) on a flash drive) after you have been identified in person at an office of Evrotrust’s Registration Authority. Upon deactivation of your account, access to all services activated by you in the Application will be terminated (e.g. a remotely issued QCQES will be terminated).

Before giving or refusing to give your consent, please check our Personal Data Protection Policy. The contact details of our Data Protection Officer are: telephone number: (+359 2) 448 58 58; e-mail address: dpo@evrotrust.com, address: Sofia City, No. 101 Tsarigradsko Shosse Blvd., 6th floor.

Once you have given your consent, you will proceed to the automated identification process. If you refuse to give your consent, the registration process will cease.