QTSP PRIVACY STATEMENT FOR THE PROTECTION OF PERSONAL DATA & GENERAL INFORMATION

20 April 2023

Version 1.5

Document History

Version	Date	Author	Reason for Change
1.0	26/07/2018	Paris Erotokritou	Initial publication
1.1	26/06/2019	Paris Erotokritou	Minor changes in the text, addition of section 13
1.2	15/07/2020	Paris Erotokritou	Change regarding section 6
1.3	04/12/2020	Paris Erotokritou	Changes regarding chapters 2,5,9,13 due SH signing platform
1.4	06/12/2021	Paris Erotokritou	Revised Date
1.5	20/04/2023	Paris Erotokritou	Change regarding cookies & Simple Signatures

Document Approvals

Version	Date	Approved By
1.0	26/07/2018	Steering Committee
1.1	26/06/2019	Nicodemos Damianou
1.2	15/07/2020	QTSP Policy Management
1.3	04/12/2020	QTSP Policy Management
1.4	06/12/2021	QTSP Policy Officer
1.5	20/04/2023	QTSP Policy Management

Document Distribution List

Version	Date	Role/Name
1.0	26/07/2018	All QTSP Staff
1.1	26/06/2019	All QTSP Staff
1.2	20/07/2020	All QTSP Staff
1.3	04/12/2020	All QTSP Staff
1.4	06/12/2021	All QTSP Staff
1.5	20/04/2023	All QTSP Staff

Contents

1. WHO WE ARE....4
2. WHAT PERSONAL DATA WE PROCESS AND WHERE WE COLLECT IT FROM 5
3. WHETHER YOU HAVE AN OBLIGATION TO PROVIDE US WITH YOUR PERSONAL DATA....7
4. WHY WE PROCESS YOUR PERSONAL DATA AND ON WHAT LEGAL BASIS ..8
5. SHARING INFORMATION....8
6. TRANSFER OF YOUR PERSONAL DATA TO A THIRD PARTY OR A THIRD COUNTRY OR TO AN INTERNATIONAL ORGANISATION....10
7. TO WHAT EXTENT THERE IS AUTOMATED DECISION-MAKING AND WHETHER PROFILING TAKES PLACE....10
8. HOW WE TREAT YOUR PERSONAL DATA FOR MARKETING ACTIVITIES AND WHETHER PROFILING IS USED FOR SUCH ACTIVITIES....11
9. HOW LONG WE KEEP YOUR PERSONAL INFORMATION FOR....11
10. YOUR DATA PROTECTION RIGHTS....11
11. CHANGES TO THIS PRIVACY STATEMENT....12
12. COOKIES....12
13. DATA SECURITY....13

This Privacy Statement aims to give you information on how JCC Payments Systems Ltd (referred to as 'we', 'us', 'our', 'JCC Payment Systems' or 'JCC') collects, uses, discloses and processes your personal data through your use of the https://trust.jcc.com.cy and https://sign.jcc.com.cy (hereinafter referred to as "the Websites") and the means by which this is done. The Privacy Statement as a means of notifying the website visitors of their rights in accordance with local law and the EU General Data Protection Regulation (EU) 2016/679.

JCC Payment Systems Ltd is committed to protecting your privacy and developing technology that gives you the most powerful and safe online experience.

By accessing, browsing and/or using this Website, you consent to the data practices described in this Privacy Statement and acknowledge that you have read, understood, and agree, to be bound by these terms conditions, and notices contained herein and to comply with all applicable laws and regulations.

For the purposes of this Privacy Statement "Personal Data" refers to all data which relates to a living individual who can be identified from such data such as for instance, name, address and/or identification number. It does not include data where the identity has been removed (anonymous data).

1. WHO WE ARE

JCC Payment Systems Ltd is a licensed payment institution registered in Cyprus under registration number HE29914 as a private limited liability company having its registered office and head offices at 1 Stadiou Street, 2571 Industrial Area Nisou, P.O. Box 21043, 1500 Nicosia, Cyprus which is primarily engaged in the business of card-processing and acquiring.

In accordance with the European Union's Regulation for Electronic Identification and Authentication Services ("eIDAS")[1] JCC acts as a qualified trust service provider (QTSP).

The overall purpose of eIDAS is to set an electronic identification standard to achieve safe and streamlined online transactions across Europe.

Via the Websites JCC offers secure qualified trust services to you, the customer, for the generation and use of an Authentication Certificate or an EU Qualified Certificate for Electronic Signatures/Seals. In the instance that you apply for a Digital Certificate, JCC (as a Trust Service Provider, as such term is defined in the eIDAS Regulation) requires personal information, so as to proceed with the issuing of your digital certificates. This information may include your name, email address, physical address, phone number and/or post code or other personal information.
What personal information may be required from you depends on the type of Trust Services you require. Please note that simple signatures are not legally equivalent to the traditional handwritten signatures. So, the responsibility of the use of a simple signature lies upon the client.

[1] eIDAS was set out in order to give consistency to regulations in the EU regarding electronic signatures, thereby improving trust. It seeks to enhance trust in electronic transactions in the EU's internal market by providing a common foundation for secure electronic interaction between citizens, businesses and public authorities cross-borders, in order to increase the effectiveness of public and private online services, electronic business and electronic commerce in the Union.

For further information on JCC's different types of Trust Services, please refer to our JCC's Certificate Practice Statement (CPS) available at: https://pki.jcc.com/repository.

JCC is committed to protecting your privacy and handling your data in an open and transparent manner. The personal data that we collect, and process depends on the service requested and agreed in each case.

2. WHAT PERSONAL DATA WE PROCESS AND WHERE WE COLLECT IT FROM

We collect and process different types of personal data which we receive from our customers (potential and current) in person or via their representative or via our alternative channels of communication such as https://trust.jcc.com.cy and https://sign.jcc.com.cy, in the context of our business relationship.

We may also collect and process personal data from publicly available sources (e.g. the Department of Registrar of Companies and Official Receiver) which we lawfully obtain and we are permitted to process.

If you have any questions, or want more details about how we use your personal information, you can contact our Data Protection Officer at 1 Stadiou Street, 2571 Industrial Area Nisou, 1500 Nicosia, Cyprus, email: dpo@jcc.com.cy.

Following is the list of information gathered automatically by JCC SigningHub:

IP Address (system identified)

This is identified automatically (when your browser communicates with our cloud servers). JCC SigningHub later processes the IP address to guide the user if his physical location has changed and hence prompts the user to automatically switch the country and time zone information. Change of time zone helps our users to view the dates shown inside the product using the user's time zone hence avoiding any confusion.

Usage Data

Information related to the ways in which you interacted with our services, such as: referring and exit pages and URLs, platform type, the number of clicks, domain names, landing pages, pages and content viewed, the amount of time spent on particular pages, the date and time you used the services, the frequency of your use of the services, and other similar information.

Transactional Data

This includes Activity logs, Workflow history and Workflow evidence report. Activity log contains user initiated activities like login/logout, update to profiles, settings etc. Workflow history contains activities performed on a document. Workflow evidence report provides a detailed auditable report in PDF (digitally signed) on the activities performed on a document.

Country / Location

This is used at the time of signing and set inside the signature if a specific signature appearance was selected which shows country information. This helps the recipients to know from which location the user has signed the document.

Logs

JCC SigningHub generates server-side logs which helps administrators to debug any application related issues. Logs are kept for a period of seven (7) years according to eIDAS regulation.
Note: Name, Email, Phone No, User Agent, IP Address is also documented in the workflow evidence report information which is then visible to the document owner. This information is also recorded in the workflow history.

Documents

You can upload/manage your documents for signing, approving or editing (i.e. form-filling). Depending on your use case requirements these documents may contain your personal data. All of the documents are stored as encrypted with powerful AES-256 based encryption algorithms.
The processed documents can also be optionally uploaded to your configured cloud storage drives e.g. OneDrive, Google Drive, Dropbox etc. It is your duty to ensure that you have configured your cloud drives correctly and it is your choice on whether to use these cloud providers as part of the JCC SigningHub service.

Profile Picture

You can set this as your digital avatar. This picture is sent in the notifications emails to recipients hence helps recipients relate to the person in a more user-friendly way. You can set any picture, i.e. not necessarily your own photo. Also it's not mandatory to set this and is only aimed at improving the user experience.

Delegate Signing

This setting allows you to configure a contact to whom you are delegating all your signing actions for a specified period of time.

3. WHETHER YOU HAVE AN OBLIGATION TO PROVIDE US WITH YOUR PERSONAL DATA

In order that we may be in a position to proceed with a business relationship with you, you must provide your Personal Data to us which are necessary for the required commencement and execution of a business relationship and the performance of our contractual obligations.

We are furthermore obligated to collect such Personal Data given the provisions of the Law for the Prevention and Suppression of Money Laundering Activities of 2007 to 2018 ('the AML/CFT Law'), that requires that We verify your identity before we enter into a contract or a business relationship with you or the legal entity for which you are the authorized to act as representative and/or agent and/or are the beneficial owner.

You must, therefore, provide us at least with your identity card/passport so that we may comply with our statutory obligation as mentioned above. In case of non-Cypriot nationality, identity is NOT accepted and passport must be accompanied with an official attestation of Passport is required in the case of non-Cypriot Nationality natural person that must be in the Greek or English language

Kindly note that if you do not provide us with all required Personal Data, then we will not be allowed to commence or continue our business relationship either to you as an individual or as the authorized representative/agent or beneficial owner of a legal entity.

4. WHY WE PROCESS YOUR PERSONAL DATA AND ON WHAT LEGAL BASIS

We are committed to protecting your privacy and handling your Personal Data in an open and transparent manner and as such we process your Personal Data in accordance with the GDPR and the local data protection law for one or more of the following reasons:

A. For the performance of the Services provided to you

Your information, whether public or private, will not be sold, exchanged, transferred outside of our Company and its subsidiaries, or given to any other company for any reason without your consent and will not be used for any other than the purposes specified below:

- With respect to process applications for JCC Products and Services in relation to Electronic Identification and Authentication Services.
- With respect to the processing of all and/any certificate purchase requests;
- To provide you with technical and customer support
- To issue and/or, revoke and/or process Digital Certificates in accordance with our CPS;
- So as to verify your identity and entitlement to products or services in accordance with our CPS;

B. For compliance with a legal obligation

We collect your Personal Data so as to comply with the legal obligations emanating from the eIDAS regulation and Applicable National Law.

C. For the purposes of safeguarding legitimate interests

Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests. We process Personal Data so as to safeguard the legitimate interests pursued by us or by a third party. A legitimate interest is when we have a business or commercial reason to use your information. But even then, it must not unfairly go against what is right and best for you.

D. You have provided your consent

By using the Websites or our Services you consent to the use of your personal information as described in this Privacy Statement. Except as set forth in this Privacy Statement, your Personal Data will not be used for any other purpose without your consent. You may withdraw your consent to our processing of your personal information at any time by informing us in writing. However, withdrawing your consent may result in your inability to continue using the Websites and/or the Services.

5. SHARING INFORMATION

In the course of the performance of our contractual and statutory obligations your personal data may be provided to various departments within JCC. Various service providers and suppliers (sub-processors) may also receive your Personal Data so that we may perform our obligations. Such service providers and suppliers enter into contractual agreements with JCC by which they observe confidentiality and data protection according to the data protection law and GDPR.

It must be noted that we may disclose data about you for any of the reasons set out hereinabove, or if we are legally required to do so, or if we are authorized under our contractual and statutory obligations or if you have given your consent. All data processors appointed by us to process Personal Data on our behalf are bound by contract to comply with the GDPR provisions.

Under the circumstances referred to above, recipients of personal data may be, for example:

- Supervisory and other regulatory and public authorities, in as much as a statutory obligation exists.
- Companies who assist us with the effective provision of our services to you by offering technological expertise, solutions and support.

You Sharing with Other Users

As part of your business requirements to have documents signed, you can share documents with other users as you desire.

In addition, in case of purchasing enterprise plan, you can also invite users to join your JCC SigningHub enterprise account as your enterprise users. Such users will then be able to view any shared templates, documents held in the enterprise library, enterprise contacts etc. as per the role you configure for them.

If you are using an enterprise account as a user then only the following information can be viewed by your enterprise administrator(s) provided that they hold sufficient system rights: Name, Email, Role, Phone, Job Title, and Company Name. Enterprise admins can only change your Role. *Also enterprise users can also see the enterprise owner's email address and mobile number to help in cases where they need to communicate on any rights/roles related concerns.*

Similarly, an enterprise administrator can also look at your action history which contains details about your login/logout and settings which were updated i.e. delegate settings, contact, signature method, templates and legal notice. Note that Enterprise admin will not be able to see the actual values changed rather only information that certain setting were updated. Also note that your password is never shown to administrators. Similarly, if your document is signed then action history will also record information like: User Agent, IP of the machine from where the signing action was initiated, the actual legal notice shown, mobile number used for sending OTP for login or document viewing, document access permissions set on the document, document name, signing reason, signing location, signing contact information, signature authorisation type/Device ID and hand signature image used.

Sharing with Service Providers

We work with various service provider companies that help us run JCC SigningHub as an effective business service. In some cases, these companies have access to some of your personal information in order to provide services to you on our behalf. It is important to note that they are not permitted to use your information for their own purposes that is they only act as data processors.

The following set of information is shared with different 3rd parties to ensure you get the best possible service:

- Microsoft OneDrive, Google Drive, Dropbox – User held documents can be pulled and pushed back to the respective cloud drives. All of these service providers have ISO 27001

certification. It is your choice on whether to use these cloud providers as part of the JCC SigningHub service.

- Google Push Notification Service (Firebase) – Using this user can get push notifications on their android and iOS devices. This include the message text and a unique mobile ID assigned to the user's mobile to whom the push notification is to be generated. Push notification is only sent if the user has agreed to receive such push notification. Once sent the message is cleared from the service provider servers. Firebase is ISO 27001 certified service provider.

6. TRANSFER OF YOUR PERSONAL DATA TO A THIRD PARTY OR A THIRD COUNTRY OR TO AN INTERNATIONAL ORGANISATION

Your personal data may be transferred to third countries i.e. countries outside of the European Economic Area in the context of providing our Services or if this data transfer is required by law or you have given us your consent to do so.

Whenever we transfer your personal data out of the EEA, we ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

- We will only transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data by the European Commission.
- Where we use certain service providers, we may use specific contracts approved by the European Commission which give personal data the same protection it has in Europe such as the Model Contract of the European Commission for transfers of Personal Data to third countries,
- Where we use providers based in the US, we may transfer data to them if they are part of the Privacy Shield which requires them to provide similar protection to personal data shared between Europe and the US.

In the unlikely event that it will be necessary for JCC Payment Systems to cease all Trust Services operations, JCC Payment Systems has the right to transfer all Trust Services archives and records to a third party.

7. TO WHAT EXTENT THERE IS AUTOMATED DECISION-MAKING AND WHETHER PROFILING TAKES PLACE

In establishing and carrying out a business relationship, We generally do not use any automated decision-making. We may process some of your data automatically, with the goal of assessing certain personal aspects (profiling), in order to enter into or perform a contract with you, in the following cases:

◦Data assessments (including on payment transactions) are carried out in the context of combating money laundering and fraud. An account may be detected as being used in a way that is unusual for you or your business. These measures may also serve to protect you.
◦Credit scoring is used as part of the assessment of your creditworthiness. This calculates whether you or your business will be able to meet any future payment obligations pursuant to a contract. This helps us make responsible financial security decisions that are fair and informed.

8. HOW WE TREAT YOUR PERSONAL DATA FOR MARKETING ACTIVITIES AND WHETHER PROFILING IS USED FOR SUCH ACTIVITIES

A. Marketing / Promotional offers from Us

We may use your Personal Data to form a view on what we think you may want or need, or what may be of interest to you. This is how we decide which products, services and offers may be relevant for you (we call this marketing).

You will receive marketing communications from us if you have requested information from us or have purchased our Services from us and you have not opted out of receiving that marketing. Your consent is therefore needed in such cases.

B. Third-party marketing

We will get your express opt-in consent before we share your Personal Data with any third party for marketing purposes.

You have the right to object at any time to the processing of your personal data for marketing purposes, which includes profiling, by contacting at any time JCC in person or in writing.

9. HOW LONG WE KEEP YOUR PERSONAL INFORMATION FOR

In accordance with the eIDAS Regulation for Qualified Trust Service Providers We will retain your Personal Data for a period of seven (7) years from the date that the Digital Certificate has expired or has been revoked.

To allow better management of your account storage space, your documents which are unused for a certain 3 years duration to automatically be deleted from your account. A notification email will be sent before the document is deleted so that you can take any necessary action and the deleted document will also be sent via email as a copy to the document owner.

10. YOUR DATA PROTECTION RIGHTS

You have the following rights in terms of your personal data we hold about you:

- **Receive access to your personal data**. This enables you to e.g. receive a copy of the personal data we hold about you and to check that we are lawfully processing it. In order to receive such a copy you can contact us at the email: dpo@jcc.com.cy .
- **Request correction [rectification]** of the personal data we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected.
- **Request erasure of your personal information.** This enables you to ask us to erase your personal data [known as the 'right to be forgotten'] where there is no good reason for us continuing to process it.
- **Object to processing of your personal data** where we are relying on a legitimate interest and there is something about your particular situation which makes you want to object to processing

on this ground. If you lodge an objection, we will no longer process your personal data unless we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms.

- **Request the restriction of processing** of your personal data. This enables you to ask us to restrict the processing of your personal data, i.e. use it only for certain things, if:
  - it is not accurate,
  - it has been used unlawfully but you do not wish for us to delete it,
  - it is not relevant any more, but you want us to keep it for use in possible legal claims,
  - you have already asked us to stop using your personal data but you are waiting us to confirm if we have legitimate grounds to use your data.
- **Request to receive a copy** of the personal data concerning you in a format that is structured and commonly used and transmit such data to other organisations. You also have the right to have your personal data transmitted directly by ourselves to other organisations you will name [known as the right to data portability].
- **Withdraw the consent** that you gave us with regard to the processing of your personal data at any time. Note that any withdrawal of consent shall not affect the lawfulness of processing based on consent before it was withdrawn or revoked by you.

To exercise any of your rights, or if you have any other questions about our use of your personal data, please contact our Data Protection Officer at the email: dpo@jcc.com.cy. We endeavour to address all of your requests promptly.
You have a right to lodge a complaint in the instance that your concerns about how we use your personal data have not been adequately addressed by us. You may inform Us of this by sending an email to our Data Protection Officer at email: dpo@jcc.com.cy or directly lodge a complaint with the Office of the Commissioner for Personal Data Protection at http://www.dataprotection.gov.cy.

11. CHANGES TO THIS PRIVACY STATEMENT

We may modify or amend this Privacy Statement from time to time.

We will notify you appropriately when we make changes to this privacy statement and we will amend the revision date at the top of this page. We do however encourage you to review this statement periodically so as to be always informed about how we are processing and protecting your personal information.

12. COOKIES

This website uses strictly necessary cookies which are essential for you to browse the website and use its features, such as accessing secure areas of the site.

Cookie	Duration	Description
.AspNetCore.Antiforgery.iMLvVsbtAys	End of session	Security cookie to prevent Cross-Site Request Forgery (XSRF/CSRF) attacks.
LB_Cookie	End of session	Cookie used for server high availability. This cookie is deleted when the user closes the browser.

TSxxxxxxxx_xx	End of session	Security cookie Performs domain cookie validation, detects session expiration, and validates integrity of cookies. This cookie is deleted when the user closes the browser.

13. DATA SECURITY

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorized way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

We reiterate that the security of your personal information is important to us and this is why we maintain physical, electronic, and procedural safeguards to secure your personal information. JCC secures the personally identifiable information you provide on computer servers in a controlled, secure environment, protected from unauthorized access, use or disclosure. When personal information are transmitted these are protected through the use of encryption such as the Secure Socket Layer (SSL) protocol.

All user documents are encrypted with AES 256 bit encryption before being stored in the JCC SigningHub database.