

Privacy Policy of JioSign

Version 1.3

1. Scope:

1.1. This electronic signing application (“Application”) is operated by Jio Things Limited, located at 101, Saffron, Nr. Centre Point, Panchwati 5 Rasta, Ambawadi, Ahmedabad, Gujarat – 380006, and which may mean and include any of its affiliates, assignees or successors-in-interest as determined by it at its sole discretion and without requiring any prior notice or intimation, from time to time (“**Company**”, “**we**”, “**our**” or “**us**”) and developed by Jio Platforms Limited.

1.2. We are committed to protecting and respecting your privacy.

1.3. This Privacy Policy, together with the **General Terms and Conditions of the JioSign (“Application T&C”)**, outlines Application’s privacy practices regarding the collection, use and safeguard of your information through the Application and the Services offered thereupon.

1.4. Your clicking of the “I agree” button (and entering your authorization PIN if required) means that you understand, accept and agree to be bound this Privacy Policy.

1.5. Capitalized terms and expressions not expressly defined hereinunder shall have the meaning ascribed to it in the Application T&C.

2. Data we collect:

2.1. “**Personal data**” is defined as information that can be used to identify you and may include details such as your name, age, gender, contact information and your interests as personally identified in products and services. Insofar as sensitive personal information is concerned, it will carry the meaning as may be defined by applicable laws from time to time.

2.2. The Personal data we may collect while offering Services depends on the Identity Verification Provider you choose to use for signing and whether you are using a free or paid Services. The list of personal data may include:

2.2.1. Name, e-mail address, address and the mobile phone number;

2.2.2. Personal data including sensitive personal data required as per the Identity Verification Provider chosen to process your request for an electronic signature, key creation and certificate issuance.

2.2.3. Your signature image and image of your initials;

2.2.4. Identifier received from the Identity Verification Provider;

2.2.5. Payment details (e.g. credit card details such as card type, card number, expiration date, name, address);

2.2.6. Personal data including sensitive personal data contained in Your Electronic Records;

2.2.7. Public IP address, device and browser information;

2.2.8. Your actions while using the Services as a reflection of Your consent and intention to approve the contents of an electronic document;

2.2.9. Geolocation information.

2.3. The processing of your personal data including sensitive personal data takes place on your consent. You may withdraw your consent any time. You can withdraw consent by sending an e-mail to jjosign@jio.com.

3. Usage:

3.1. The Application seeks your personal data and sensitive personal data either to (i) validate and process your request for the Services; (ii) to improve the quality of the Application; or (iii) or assist to determine which services best meet your needs; or (iv) to facilitate our internal business operations, including the fulfilment of any legal and regulatory requirements; or (v) to provide you with recommendation about services you may be interested in, based on your use of the Application; or (vi) to provide you with marketing communications and advertising that the Application believe may be of interest of you.

3.2. We also retain any earlier data submissions made by you, including any personal data provided by you, in the case of your updating or correcting such data or information, upgrading or downgrading your account or subscription package for establishing and maintaining a system trail and/or audit trail of your usage of the Application for fraud detection purposes.

4. Sharing:

4.1. We will strive to keep your personal data including sensitive personal data confidential and will place reasonable security controls to protect it. Your personal data will be kept confidential as required under applicable laws.

4.2. In order to provide the Services, we may need to share your personal data with the Controller of Certifying Authorities (CCA), Government Appointed Aadhaar eSign Certifying Authority/eSign Service Provider and the Identity Verification Provider.

4.3. In the course of providing Services, we use certain data processors who help us in delivering Services or to detect, prevent or otherwise address fraud, security or technical issues, provide advertising and promotional services or customer services.

4.4. We may disclose personal information to our affiliates when necessary to perform services on our behalf or on your behalf.

4.5. We may also share personal information with external organizations or individuals if we believe that access, use, preservation or disclosure of the information is reasonably necessary to:

4.5.1. meet any applicable law, regulation, legal process or enforceable governmental request;

4.5.2. detect, prevent or otherwise address fraud, security or technical issues;

4.5.3. protect against harm to the rights, property or safety of our customers or the public, as required or permitted by law.

4.6. We may be required to share your personal data with governmental authorities for the purposes of national security, law enforcement, or other major issues of public importance.

5. Retention and security:

5.1. The personal data collected shall be retained only for a limited duration necessary to fulfil the purposes outlined herein unless a longer retention period is required or permitted by law and only for the purposes defined above. Once the purpose is achieved, all personal information is deleted in a safe and secure mode.

5.2. We maintain appropriate security policies and procedures designed to protect personal information against unauthorized access, loss, misuse, alteration, and destruction. While we take reasonable measures to safeguard your information, no security system can guarantee complete protection against all potential threats.

5.3. Access to your personal information is restricted to individuals who require it to perform their responsibilities. Anyone granted access to such information is required to keep it confidential.

6. Cookies:

6.1. Information collected by cookies and other technologies are treated as non-personal data. However, to the extent that IP addresses or similar identifiers are considered personal information by local law, we treat any information linked to such identifiers as personal information. Similarly, to the extent that non-personal information is combined with personal information, we will treat the combined information as personal information.

7. Third Party Services:

7.1. When you are on our server, your mobile service provider, mobile operating system provider, third party applications on your device, social media platforms, websites that you access, and third-party operators may also collect, use and share information about you and your usage. We cannot control how these third parties collect, use, share or secure this information. For information about third-party privacy practices, please consult their respective privacy policies.

7.2. The Application may include links to other websites/applications or may display advertisements from third parties and other content that links to third party websites. Such websites/applications are governed by their respective privacy policies, which are out of the Application's control. Use of any information you provide while using a third-party website/application through the Application, is governed by the privacy policy of the operator of the website/application/ operator you are using/ visiting. That privacy policy may differ from that of the Application. If you can't find the privacy policy of any of such websites /application via a link from the website's/application's homepage, you should contact the relevant website /application operator directly for more information.

8. Liability:

8.1. We shall not be liable for any indirect, incidental, consequential, special or exemplary damage(s) arising due to loss of data or use arising out of or in connection with your access or use of or inability to access or use the Application.

8.2. We shall not be liable for any third-party products, software or service provided by any third-party applications on the Application. You shall assume all risks arising out of or resulting from any transaction undertaken by you with any third-party application on the Application and you agree that we shall not be responsible or liable for any loss to you due to your usage of such third-party application.

9. Access, Correction and Deletion:

9.1. The Application strives hard to keep its records updated and accurate with your latest information. You shall be responsible to ensure that the information or data you provide from time to time is and shall be correct, current and updated and you have all the rights, permissions and consents to provide such information or data.

9.2. You may note that deletion of certain information or withdrawal of consent may lead to cancellation of your access to the Application or your access to certain features and services of the Application. Additionally, we may not be able to process your request of correction, updating or deletion, in case the same is not supported by valid documents or data retention is required by the applicable law or law enforcement requests or under any judicial proceedings or it is extremely difficult to implement (such as requests related to backup copies or if a new system is required to process the request or change of technical design) or risks the privacy of other users.

10. Queries and Complaints:

10.1. We are committed to protect your personal data collected and processed by us and look forward to your continued support for the same.

10.2. We will respond to your request as soon as possible, and no later than one month from the date we receive it.

10.3. If you have any questions about how we process your personal data, or if you wish to exercise any of your rights, e.g. to request a copy of your personal data, request that your personal data be corrected or deleted, object to its processing, or request that its processing be restricted, you may contact us using the Grievance Officer contact details.

11. Grievance Officer Details:

Mrs. Radha Nair, Reliance Corporation IT Park, TC-22, Thane Belapur Road, Ghansoli, Navi Mumbai 400701

Email id: grievance.officer@jio.com