LEGALPAY INFORMATION SECURITY POLICY, 2022

1.1. Objective

The purpose of this policy is to maintain the privacy of and protect the personal and proprietary information of Legalpay Technology Private Limited, its subsidiaries, sister concerns, associate concerns, and any other entity (including Limited Liability Partnerships), which may be incorporated by Legalpay Technology Private Limited or any of its authorized representatives (hereafter collectively referred to as "LegalPay" or "the Company"). The Policy is also aimed at maintaining the privacy of and protect the personal and proprietary information of the Company's employees, contractors, vendors, interns, associates, clients and business partners of LegalPay (hereafter collectively referred to as "Policy Subjects"), and to ensure compliance with laws and regulations applicable to the Company.

1.2. Scope

This policy is applicable to LegalPay, its employees, contractors, vendors, interns, associates, clients and business partners who may receive personal and proprietary information, have access to personal and proprietary information collected or processed, or who provide information to the Company, regardless of their geographic location.

All employees of LegalPay are expected to abide by the privacy policy and principles when they collect and/or handle personal and proprietary information, or are involved in the process of maintaining or disposing of personal and proprietary information. This policy provides the information to successfully meet the Company's commitment towards data privacy.

All partner firms and any Third-Party working with or for LegalPay, and who have or may have access to personal and proprietary information, will be expected to have read, understand and comply with this policy. No Third Party may access personal and proprietary information held by the Company without having first entered into a confidentiality agreement.

1.3. Responsibilities

The owner for the LegalPay Information Security Policy, 2022 shall be the Data Privacy Officer . The Data Privacy Officer shall be responsible for maintenance and accuracy of this policy. Any queries regarding the implementation of this Policy shall be directed to the Data Privacy Officer.

This policy shall be reviewed for updates by Data Privacy Officer on an annual basis. Additionally, the Data Privacy Policy shall be updated in-line with any major changes within the Company's operating environment or on recommendations provided by internal/external auditors.

1.4. Policy Compliance

Compliance to the Data Privacy Policy shall be periodically reviewed by Privacy Review Team to ensure continuous compliance monitoring through the implementation of compliance measurements and periodic reviewprocesses.

In cases where non-compliance is identified, the Data Privacy Officer (hereafter, referred to as

"DPO") shall review the reasons for such non-compliance along with a plan for remediation and report them to Privacy Review Team. Depending on the conclusions of the review, need for a revision to the policy may be identified. In instances of persistent non-compliance by the individuals concerned, they shall be subject to action in accordance with the LegalPay Service Rules, 2022.

1.5. Data Privacy Principles for Personal Information

This Policy describes generally acceptable privacy principles (GAPP) for the protection and appropriate use of personal information at LegalPay. These principles shall govern the use, collection, disposal and transfer of personal information, except as specifically provided by this Policy or as required by applicable laws:

- **Notice:** LegalPay shall provide data subjects with notice about how it collects, uses, retains, and discloses personal information about them.

- **Choice and Consent:** LegalPay shall give data subjects the choices and obtain their consent regardinghow it collects, uses, and discloses their personal information.

- **Rights of Data subject:** LegalPay shall provide individuals with the right to control their personal information, which includes the right to access, modify, erase, restrict, transmit, or object to certain uses of their information and for withdrawal of earlier given consent to the notice.

- **Collection:** LegalPay shall collect personal information from data subjects only for the purposes identified in the privacy notice / SoW / contract agreements and only to provide requested product or service.

- **Use, Retention and Disposal:** LegalPay shall only use personal information that has been collected for the purposes identified in the privacy notice / SoW / contract agreements and in accordance with the consent that the data subject shall provide. LegalPay shall not retain personal information longer than is necessary to fulfil the purposes for which it was collected and to maintain reasonable business records. LegalPay shall dispose the personal information once it has served its intended purpose, on a request made by the data subject to do so, within a period of one (1) month from the date of such request by data subject.

- **Access:** LegalPay shall allow data subjects to make inquiries regarding the personal information about them, that LegalPay shall hold and, when appropriate, shall provide access to their personal information for review, and/or update.

- **Disclosure to Third Parties:** LegalPay shall disclose personal information to Third Parties / partner firms only for purposes identified in the privacy notice / SoW / contract agreements. LegalPay shall disclose personal information in a secure manner, with assurances of protection by those parties, according to the contracts, laws and other segments, and, where needed, with consent of the data subject. However, LegalPay may disclose any and all personal information to authorities as and when required by law.

- **Obligations for Sub-processor:** Where a processor (vendor or 3rd party acting on behalf of LegalPay's data processor) engages another processor (Sub-processor) for carrying out specific processing activities on behalf of LegalPay (controller), the same data protection

obligations as set out in the contract or other legal act between LegalPay and the processor shall be imposed on the Sub-processor, by way of a contract or other statutory provisions, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of law. Where the Sub-processor fails to fulfil its data protection obligations, the initial processor (relevant vendor or 3rd party acting on behalf of LegalPay's data processor) shall remain fully liable to LegalPay for the performance of that Sub-processor's obligations.

- **Security for Privacy:** LegalPay shall reasonably protect the personal information from unauthorized access, data leakage and misuse.

- **Quality:** LegalPay shall take steps to ensure that personal information in its records is accurate and relevant to the purposes for which it was collected.

- **Monitoring and Enforcement:** LegalPay shall monitor compliance with its privacy policies, both internally and with Third Parties, and establish the processes to address inquiries, complaints and disputes, in accordance with LegalPay Service Rules, 2022.

1.6. Data Privacy Principles for Proprietary Information

This Policy describes generally acceptable privacy principles (GAPP) for the protection and appropriate use of proprietary information at LegalPay. These principles shall govern the use, collection, disposal and transfer of proprietary information, except as specifically provided by this Policy or as required by applicable laws:

- Policy Subjects shall not improperly use for the benefit of, bring to any premises of, divulge, disclose, communicate, reveal, transfer or provide access to, or share with any unauthorized entity / person any confidential, proprietary or non-public information or intellectual property relating to LegalPay, a former employer, a business partner, or any other third party. However, LegalPay may disclose any and all proprietary information to authorities as required by law.

- The Policy Subjects shall indemnify, hold harmless and agree to defend the Company and its officers, directors, partners, employees, agents, and representatives from any unauthorized breach of confidentiality of the proprietary information belonging to either LegalPay or any of its Clients or Business Partners.

- LegalPay shall monitor compliance with its privacy policies, both internally and with Third Parties, and establish the processes to address inquiries, complaints, and disputes, in accordance with LegalPay Service Rules, 2022.

1.7. Notice

Notice shall be made readily accessible and available to data subjects before or at the time of collection of personal and proprietary information or otherwise, notice shall be provided as soon as practical thereafter. Notice shall be displayed clearly and conspicuously and shall be provided through online (e.g., by posting it on the website, sending mails, newsletters, etc.) and / or offline methods (e.g., through posts, couriers, etc.). All the web sites and any product or service that collects personal and proprietary information internally, shall have a privacy notice.

In case of any cross-border transfer of personal and proprietary information, the data subjects shall be informed by a notice sufficiently prior to the transfer.

1.8. Choice and consent

Choice refers to the options the data subjects are offered regarding the collection and use of their personal and proprietary information. Consent refers to their agreement to the collection and use, often expressed by the way in which they exercise a choice option.

- LegalPay shall establish systems for the collection and documentation of data subject consents to the collection, processing, and/or transfer of personal and proprietary data.
- Data subjects shall be informed about the choices available to them with respect to the collection, use, and disclosure of personal and proprietary information.
- Consent shall be obtained (in writing or electronically) from the data subjects before or at the time of collecting personal and proprietary information or as soon as practical thereafter.
- The changes to a data subject's preferences shall be managed and documented. Consent or withdrawal of consent shall be documented appropriately.
- The choices shall be implemented in a timely fashion and respected. If personal and proprietary information is to be used for purposes not identified in the notice / SoW / contract agreements at the time of collection, the new purpose shall be documented, the data subject shall be notified, and consent shall be obtained prior to such new use or purpose.
- The data subject shall be notified if the data collected is used for marketing purposes, advertisements, etc.
- LegalPay shall review the privacy policies of the Third Parties and types of consent of Third Parties before accepting personal and proprietary information from Third-Party data sources.

1.9. Collection of Personal and Proprietary Information

Personal and proprietary information may be collected online or offline. Regardless of the collection method, the same privacy protection shall apply to all personal and proprietary information.

- Personal and proprietary information shall not be collected unless either of the following is fulfilled:
    - the data subject has provided a valid, informed and free consent;
    - processing is necessary for the performance of a contract to which the data subjectis a party or in order to take steps at the request of the data subject prior to enteringinto a contract;
    - processing is necessary for compliance with the LegalPay's obligation;

- processing is necessary in order to protect the vital interests of the data subject; or;
- processing is necessary for the performance of a task carried out in the public interest.

- Data subjects shall not be required to provide any more personal and proprietary information than is necessary for the provision of the product or service that data subject has requested or authorized. If any data not needed for providing a service or product is requested, such fields shall be clearly labelled as optional. Collection of personal and proprietary information shall be avoided or limited when reasonably possible.

- Personal information shall be de-identified when the purposes of data collection can be achieved without personally identifiable information, at reasonable cost.

- When using vendors, wealth managers, or any other such agents to collect personal and proprietary information on the behalf of LegalPay, the Company shall ensure that the such vendors, wealth managers, or any such agents comply with the privacy requirements of LegalPay as defined in this Policy.

- LegalPay shall periodically review and monitor the information collected, the consent obtained and the notice / SoW / contract agreement identifying the purpose.

- LegalPay shall review the privacy policies and collection methods of Third-Parties before accepting personal and proprietary information from Third-Party data sources.

1.10. Use, Retention and Disposal

- Personal and proprietary information may only be used for the purposes identified in the notice / SoW / contract agreements and only if the data subject has given consent;

- Personal and proprietary information shall be retained for as long as necessary for business purposes identified in the notice / SoW / contract agreements at the time of collection or subsequently authorized by the data subjects.

- When the use of personal and proprietary information is no longer necessary for business purposes, a method shall be in place to ensure that the information is destroyed in a manner sufficient to prevent unauthorized access to that information, if the same is requested by the data subject. Alternatively, the personal information shall be de-identified in a manner sufficient to make the data non-personally identifiable, upon such information having served its intended purpose.

- LegalPay shall have a documented process to communicate changes in retention periods of personal and proprietary information required by the business to the data subjects who are authorized to request those changes.

- Personal and proprietary information shall be erased if their storage violates any of the data protection rules or if knowledge of the data is no longer required by LegalPay or for the benefit of the data subject. Additionally, LegalPay has the right to retain the

personal and proprietary information for legal and regulatory purpose and as per applicable data privacy laws.

- LegalPay may perform an internal audit to ensure that personal and proprietary information collected is used, retained and disposed-off in compliance with the Company's Information Security Policy.

1.11. Access

LegalPay shall establish a mechanism to enable and facilitate exercise of data subject's rights of access, blockage, erasure, opposition, rectification, and, where appropriate or required by applicable law, a system for giving notice of inappropriate exposure of personal and proprietary information.

- Data subjects shall be entitled to obtain the details about their own personal and proprietary information upon a request made and set forth in writing. LegalPay shall provide its response to a request within 72 hours of receipt of written request.

- The data subjects shall have the right to require LegalPay to correct or supplement erroneous, misleading, outdated, or incomplete personal and proprietary information.

- Requests for access to or rectification of personal and proprietary information shall be directed, at the data subject's option, to the manager of the projects team or support function responsible for the personal and proprietary information.

- The Privacy Review Team shall record and document each access request as it is received and the corresponding action taken.

- LegalPay shall provide personal and proprietary information to the data subjects in a plain simple format which is understandable (not in any code format).

1.12. Disclosure to Third Parties

Data Subject shall be informed in the privacy notice / SoW / contract agreement, if personal and proprietary information shall be disclosed to Third Parties / partner firms, or any other such entity, and it shall be disclosed only for the purposes described in the privacy notice / SoW / contract agreements and for which the data subject has provided consent.

- Personal and proprietary information of data subjects may be disclosed to the Third Parties / partner firms only for reasons consistent with the purposes identified in the notice / SoW / contract agreements or other purposes authorized by law.

- LegalPay shall communicate the privacy practices, procedures and the requirements for data privacy and protection to the Third Parties / partner firms.

- The Third Parties shall sign an NDA (Non-Disclosure Agreement) with LegalPay before any personal and proprietary information is disclosed to the Third Parties partner firms. The NDA shall include the terms on non-disclosure of customer information.

1.13. Security

Information security policy and procedures shall be documented and implemented to ensure reasonable security for personal and proprietary information collected, stored, used, transferred and disposed by LegalPay.

- The storage, retention, and transfer of personal and proprietary information shall be done by LegalPay and the Policy Subjects in accordance with the best industry practices, as far as reasonably possible.

- Management shall establish procedures that maintain the logical and physical security of personal and proprietary information.

- Management shall establish procedures that ensure protection of personal and proprietary information against accidental disclosure due to natural disasters and environmental hazards.

- Individuals noticing or becoming aware of any breach of personal and proprietary data shall notify the Data Privacy Officer (by emailing at privacy@legalpay.in) within 2 hours. It shall be the DPO's responsibility to analyze and act on the intimation of the same within three (3) business days.

1.14. Quality

LegalPay shall maintain data integrity and quality, as appropriate for the intended purpose of personal and proprietary data collection and use and ensure data is reliable, accurate, complete and current.

- For this purpose, the DPO and Privacy Review Team shall have systems and procedures in place to ensure that personal and proprietary information collected is accurate and complete for the business purposes for which it is to be used.

- LegalPay shall perform an period assessment on the personal and proprietary information collected to check for accuracy, completeness and relevance of the personal and proprietary information.

1.15. Dispute Resolution and Recourse

Any privacy related incidents and / or breaches can be reported to the following email ID: privacy@legalpay.in. In the event such privacy related incidents and / or breaches remain unresolved or unattended for a period of more than three (3) business days, the Policy Subjects shall have the option to approach the Executive Management and Compliance Department of LegalPay.

The DPO shall perform a periodic review of all the complaints related to data privacy to ensure that all the complaints are resolved in a timely manner and resolutions are documents and communicated to the data subjects.

Communication of privacy incident / breach reporting channels and the escalation matrix (upon reporting of a data privacy incident / breach) shall be provided to all data subjects.

1.16. Dispute Resolution and Escalation Process for Employees

Employees with inquiries or complaints about the processing of their personal information shall first discuss the matter with their immediate supervisor. If the employee does not wish to raise an inquiry or complaint with an immediate manager, or if the manager and employee are unable to reach a satisfactory resolution of the issues raised, the employee shall bring the issue to theattention of the DPO (Emailing at privacy@legalpay.in).

1.17. Dispute Resolution and Escalation Process for Investor(s) / Third Parties

Customers / Third Party with inquiries or complaints about the processing of their personal and proprietaryinformation shall bring the matter to the attention of the DPO in writing. Any disputes concerning the processing of the personal and proprietary information of non-employees shall be resolved through arbitration (according to the Delhi High Court Arbitration Rules, with a seat in New Delhi and a sole arbitrator bench).

1.18. Compliance Review

Privacy Review Team shall conduct an internal audit on reasonable intervals to ensure compliance with the established privacy policies and applicable laws.

The internal audit shall consist of the review of the following:

- personal and proprietary information collected from data subjects;
- the purposes of the data collection and processing;
- the actual uses of the data;
- disclosures made about the purposes of the collection and use of such data;
- the existence and scope of any data subject consents to such activities;
- any legal obligations regarding the collection and processing of such data, and
- the scope, sufficiency, and implementation status of security measures.

The Privacy Review team shall document all the instances of non-compliance with privacy policies and procedures and report the same to the Chief Executive Officer of LegalPay.

The Data Privacy Officer along with the Privacy Review Team shall take actions on the findings from the internal audit and work on the recommendations for improvement of the privacy posture.

Any changes made to the policies shall be communicated to all the employees, the stakeholders and the customers / clients, and all other such Policy Subjects.

GLOSSARY

Term	Definition
Data Subject	A data subject who is the subject of personal, sensitive, and proprietary data.
Personal data or Personally Identifiable Information (PII)	PII is any information about an individual (the data subject) which can • any information that can be used to distinguish or trace an individual's identity; • any other information that is linked or linkable to an individual Examples included but not limited to: Name, Address, Date of birth etc.
Sensitive Personal Information (SPI)	Sensitive personal data means personal data consisting of information but not limited to the following attributes of the data subject: • password; • financial information such as bank account or credit card or debit cardor other payment instrument details ; • physical, physiological and mental health condition; • sexual orientation; • medical records and history; • genetic or biometric information; • racial and ethical origin; • political opinions; • religious or philosophical beliefs; • trade union membership; • any detail relating to the above clauses as provided to body corporate for providing service; and • any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract orotherwise: Provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005

	or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.
Proprietary Information	Proprietary Information shall mean information (whether now existing or which shall be created, acquired, developed, created, discovered by the Company, or which became known by, or was conveyed to the Company, which has a commercial value in the Company's (or any of its Clients' or Business Partners') business. Proprietary Information shall include, but not be limited to the following: • domain names; • trade secrets; • copyrights; • ideas; • techniques; • know-hows; • inventions (whether patentable or not); • any other information of any type relating to designs, configurations, toolings, documentation, master databases, algorithms, flow charts, formulae, works of authorship, mechanisms, research, manufacture, improvements, assembly, installation, intellectual property (including patents and patent applications), and the information containing the Company's, its Clients' and its Business Partners' actual or anticipated business, research, or development, or which is received in confidence by or for the Company from any other person.
Third Party	All external parties – contractors, interns, summer trainees, vendors – who have access to TSL information assets or information systems.
Data protection and security	Anyone collecting personal and customer information must fairly and lawfully process it, process it only for limited, specifically stated purposes, use the information in a way that is adequate, relevant and not excessive, use the information accurately, keep the information on file no longer than absolutely necessary, process the information in accordance with your legal rights, keep the information secure and never transfer the information outside the country without

	adequate protection.