SCHEDULE B

SOME KEY PRINCIPLES HIGHLIGHTED	SAUDIA ARABIA (PDPA)	DUBAI (DIFC)	SINGAPORE (PDA)	CALIFORNIA (CCPA)	INDONESIA (PDA)	DELAWARE (DPDPA)
LAWFULNESS, FAIRNESS AND TRANSPARENCY	1) Organizations must handle personal data fairly and openly.	1) Personal data must be handled legally, fairly, and transparently.	1) Organizations must not collect, use, or share personal data without	1) Businesses must inform consumers about what personal data is	1) Personal data must be processed legally, fairly, and transparently.	1) Organizations must disclose their privacy policies and inform
CONSENT	**REQUIREMENTS**: **Explicit**: Must be clear and explicit. **Specific**: Must be for specific processing activities. **Informed**: Individuals must know the purpose and extent of data use. **Withdrawal**: Can be withdrawn anytime.	**REQUIREMENTS**: **Freely Given**: No coercion or undue influence. **Specific**: Must relate to specific processing purposes. **Informed**: Individuals must understand what they are consenting to. **Withdrawal**: Can be withdrawn anytime. **Unambiguous**: Must be explicit.	**REQUIREMENTS**: **Informed**: Individuals must be informed of the purpose of data collection. **Voluntary:** Consent must be given voluntarily. **Withdrawal:** Individuals can withdraw consent at any time.	**REQUIREMENTS**: **Opt-Out Mechanism:** Consumers have the right to direct businesses to stop selling their personal information. **Informed:** Businesses must inform consumers about their rights and provide an opt-out mechanism. **Explicit:** For certain types of sensitive personal information under CPRA, explicit consent might be required. **Withdrawal:** Consumers can opt-out of data sales at any time.	**REQUIREMENTS**: **Explicit**: Must be a clear affirmative action. **Informed**: Data subjects must be provided with information regarding the purposes of data processing. **Specific**: Must be for specified processing activities. **Withdrawal**: Data subjects have the right to withdraw consent at any time.	**REQUIREMENTS**: **Freely Given**: Consent must be given without any form of pressure or coercion. **Specific**: Consent must be specific to the purpose for which the data is being collected and processed. **Informed**: Individuals must be fully informed about what they are consenting to, including the purpose of the data processing and any third parties with whom the data will be shared. **Unambiguous**: Consent must be given through a clear affirmative action, such as a written or oral statement, or by ticking a box on a website. **Withdrawal**: Can be withdrawn anytime.

If you are located in the India, this section applies to you.	***If you are located in Dubai, this section applies to you.***	***If you are located in SAUDI ARABIA, this section applies to you.***	***If you are located in Singapore, this section applies to you.***	***If you are located in Indonesia, this section applies to you.***	***If you are located in California and Delaware, this section applies to you.***
Legal Bases for Processing Personal Data under the Digital Personal Data Protection Act (DPDPA), 2023	**Legal Bases for Processing Personal Data under Dubai International Financial Centre (DIFC) Data Protection Law**	**Under the Personal Data Protection Law (PDPL) in Saudi Arabia, the legal basis for processing personal data is crucial and is outlined primarily in Article 6 of the law. Accordingly, we may rely on the following legal bases to process your personal information:**	The following are potential legal bases for processing personal data:	**If you are located in Indonesia, The PDP Law also requires a legal basis for processing personal data. These legal bases are:**	**If you are located in California and delaware, organizations may process personal data only if one or more of the following conditions explicitly stated in the California Consumer Privacy Act (CCPA), California Privacy Rights Act (CPRA), Digital Personal Data Protection Act (DPDPA) and Delaware Online Privacy and Protection Act (DOPPA) apply:**
The Digital Personal Data Protection Act (DPDPA), 2023 requires us to explain the valid legal bases we rely on to process your personal information. Accordingly, we may rely on the following legal bases to process your personal information:	We may process your information if you have given us specific permission (i.e., express consent) to use your personal information for a specific purpose, or in situations where your permission can be inferred (i.e., implied consent). You can withdraw your consent at any time. Learn more about withdrawing your consent.	**Consent:** data subject has given consent to disclosure of his or her personal data.	Appropriate notice has been provided to or made available to the data subject	Explicit consent of the *data subject* to the purpose(s) of the personal data processing disclosed to the *data subject* ;	**1. Consent**: The individual has given explicit consent for the processing of their personal data for specific purposes. Consent must be informed, meaning the individual understands the purposes for which their data will be processed.
1. Notice: We will provide you with notice regarding the collection and processing of your personal data, including the purposes for which it is processed, the categories of personal data collected, and the identity and contact details of the data fiduciary. This notice will be provided in a clear and concise manner at the time of data collection or as soon as practicable thereafter.	In some exceptional cases, we may be legally permitted under applicable law to process your information without your consent, including, for example:	**Publicly available data:** personal data has been collected from a publicly available source.	The data subject has provided consent to the processing for the identified purposes	Fulfilment of a contractual obligation in favour of the data subject who is a party to an agreement or as requested by the data subject at the time of entering into an agreement;	**2. Necessary for Performance of a Contract**: The processing is necessary to perform a contract to which the individual is a party, or to take steps at the individual's request before entering into a contract.
2. Consent: We may process your information if you have given us permission (i.e., consent) to use your personal information for a specific purpose. You can withdraw your consent at any time. Learn more about withdrawing your consent.	**Vital Interests**: If collection is clearly in the interests of an individual and consent cannot be obtained in a timely way.	**Public interest or security purposes:** the entity requesting disclosure is a public entity, and the collection or processing of the personal data is required for public interest or security purposes, or to implement another law, to fulfill judicial requirements.	The personal data is necessary to perform a contract with the data subject	Fulfilment of legal obligations of the data controller in accordance with applicable laws and regulations;	**3. Legal Compliance**: The processing is necessary to comply with a legal obligation imposed on the organization, such as regulatory requirements or court orders.
3. Performance of a Contract: We may process your personal information when it is necessary to fulfill our contractual obligations to you, including providing our services or at your request prior to entering into a contract with you.	**Investigations and Fraud Detection**: For investigations and fraud detection and prevention.	· **Public health and safety:** the disclosure is necessary to protect public health, public safety, or to protect the lives or health of specific individuals.	The personal data is necessary to comply with a legal obligation	Fulfilment of the vital interest of the data subject;	**4. Vital Interests**: The processing is necessary to protect the vital interests of the individual or another natural person.
4. Legitimate use: We may process your information when it is reasonably necessary to achieve our legitimate business use, provided that these purposes do not override your interests and fundamental rights and freedoms. For example, we may process your personal information for the following purposes:	**Business Transactions**: For business transactions provided certain conditions are met.	· **Anonymised data:** the disclosure will only involve subsequent Processing in a form that makes it impossible to directly or indirectly identify the data subject.	The personal data is necessary to protect the vital interests of a natural person	Implementation of duties for the purpose of public interest, public service and/or implementation of data controller's authority pursuant to applicable laws and regulations; and/or	**5. Public Interest**: The processing is necessary for reasons of public interest, such as research purposes or exercising official authority.
Sending users information about special offers and discounts on our products and services.	**Insurance Claims**: If it is contained in a witness statement and the collection is necessary to assess, process, or settle an insurance claim.	· **Legitimate interest:** the disclosure is necessary to achieve legitimate interests of the Controller, without prejudice to the rights and interests of the data subject, and provided that no sensitive data is to be processed**.**	The personal data is necessary for a public interest	Fulfilment of another legitimate interest, in consideration of the purpose and interest of the data controller and the *data subject's* rights.	**6. Legitimate Interests**: The processing is necessary for the legitimate interests pursued by the organization or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the individual.

Developing and displaying personalized and relevant advertising content for our users.	**Identification and Communication**: For identifying injured, ill, or deceased persons and communicating with next of kin.	In legal terms, we are generally the "data controller" under Saudi Arabian data protection laws of the personal information described in this privacy notice, since we determine the means and/or purposes of the data processing we perform. This privacy notice does not apply to the personal information we process as a "data processor" on behalf of our customers. In those situations, the customer to whom we provide services and with whom we have entered into a data processing agreement is the "data controller" responsible for your personal information, and we merely process your information on their behalf in accordance with your instructions. If you want to know more about our customers' privacy practices, you should read their privacy policies and direct any questions you have to them.	The personal data is necessary to fulfil a legitimate interest of the controller or third party (provided that the interest is not overridden by the data subject's privacy interests and the data subject has not made use of his/her right to object)		
Analyzing how our services are used so we can improve them to engage and retain users.	**Financial Abuse**: If we have reasonable grounds to believe an individual has been, is, or may be a victim of financial abuse.		Other: a full list of circumstances under which personal data (regardless of sensitivity) can be collected and processed without consent can be found in the first and second schedules to the pdpa.		
Supporting our marketing activities.	**Legal Investigations**: If it is reasonable to expect collection and use with consent would compromise the availability or accuracy of the information, and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of the DIFC.				
Diagnosing problems and/or preventing fraudulent activities.	**Legal Requirements**: If disclosure is required to comply with a subpoena, warrant, court order, or rules of the court relating to the production of records.				
Understanding how our users use our products and services so we can improve user experience.					
5. Legal Obligations: We may process your information when it is necessary to comply with our legal obligations, such as to cooperate with a law enforcement body or regulatory agency, exercise or defend our legal rights, or disclose your information as evidence in litigation in which we are involved.	**Employment Context**: If it was produced by an individual in the course of their employment, business, or profession and the collection is consistent with the purposes for which the information was produced.				

In legal terms, we are generally the "data fiduciary" under Indian data protection laws of the personal information described in this privacy notice, since we determine the means and/or purposes of the data processing we perform. This privacy notice does not apply to the personal information we process as a "data processor" on behalf of our customers. In those situations, the customer to whom we provide services and with whom we have entered into a data processing agreement is the "data fiduciary" responsible for your personal information, and we merely process your information on their behalf in accordance with your instructions. If you want to know more about our customers' privacy practices, you should read their privacy policies and direct any questions you have to them.	**Journalistic, Artistic, or Literary Purposes**: If the collection is solely for journalistic, artistic, or literary purposes.				
	Public Information: If the information is publicly available and is specified by the regulations.				
	In legal terms, we are generally the "data controller" under DIFC data protection laws of the personal information described in this privacy notice, since we determine the means and/or purposes of the data processing we perform. This privacy notice does not apply to the personal information we process as a "data processor" on behalf of our customers. In those situations, the customer to whom we provide services and with whom we have entered into a data processing agreement is the "data controller" responsible for your personal information, and we merely process your information on their behalf in accordance with your instructions. If you want to know more about our customers' privacy practices, you should read their privacy policies and direct any questions you have to them.				

SCHEDULE B

Right	Saudi Arabia (PDPA)	California (CCPA/CPRA)	Dubai (DIFC)	Singapore (PDPA)	Indonesia (PDP Law)	Delaware (DPDPA)
Right to Access	Yes	Yes	Yes	Yes	Yes	Yes
Right to Rectification	Yes	Yes	Yes	Yes	Yes	Yes
Right to Erasure	Yes	Yes	Yes	Yes	Yes	Yes
Right to Restriction	No specific provision, but data minimization principles apply.	Not explicitly mentioned, but can opt-out of data sale.	Yes	Not explicitly mentioned.	Yes	Yes
Right to Data Portability	Not explicitly mentioned.	No explicit right, but can request specific data information.	Yes	Not explicitly mentioned.	Not explicitly mentioned.	Not explicitly mentioned.
Right to Object	Yes	Yes	Yes	Not explicitly mentioned.	Yes	Yes
Right to Withdraw Consent any time	Yes	Not explicitly mentioned, but can opt-out of data sales.	Yes	Yes	Yes	Yes

International Data Transfer Policies

Region	India	Dubai (DIFC)	Saudi Arabia	Indonesia & Singapore	Delaware	California
Transfer Conditions	Allowed to any country unless blacklisted by the Indian government.	Allowed if personal data receives adequate protection mandated by the DIFC Data Protection Law.	Allowed if personal data receives equivalent protection to Saudi law.	Allowed if personal data receives equivalent protection to local laws.	Allowed if personal data receives protection comparable to Delaware law.	Allowed if personal data receives protection comparable to Californian law.
Legal Basis	Must ensure equivalent protection to India's standards.	Transfers only to jurisdictions with adequate protection.	Transfers must comply with fairness, transparency, and proportionality.	Transfers must comply with fairness, transparency, and proportionality.	Transfers must comply with DPDPA and DOPPA requirements.	Transfers must comply with CCPA and CPRA requirements.
Consent	Explicit consent from individuals is required	Explicit consent from individuals is required.	Explicit consent from individuals is required.	Explicit consent from individuals is required.	Explicit consent from individuals is required where necessary.	Explicit consent from individuals is required where necessary.
Approved Mechanisms	Regular reviews and compliance with the DPDP Act of 2023.	Regular reviews and compliance with DIFC Data Protection Law.	Use of Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), or other SDAIA-recognized safeguards.	Use of SCCs, BCRs, or other recognized safeguards.	Use of SCCs, BCRs, or other recognized safeguards.	Use of SCCs, BCRs, or other recognized safeguards.
Contractual Obligations		Contracts must include safeguards for data privacy and security	Contracts must include appropriate safeguards.	Contracts must include appropriate safeguards.	Contracts must include appropriate safeguards.	Contracts must include appropriate safeguards

Process of Notification of Breach in various contries				
Country	**Who to Notify**	**When to Notify**	**Content of Notification**	**Exemptions**
Saudi Arabia	Regulatory Authority, Affected Individuals	Within 72 hours if aware of the breach	Details of the breach, potential consequences, and measures taken to mitigate the breach.	NA
Dubai	Commissioner of Data Protection, Affected Individuals	As soon as possible, within 72 hours if aware of the breach	Nature of the breach, contact details of data protection officer, likely consequences, and measures to mitigate.	NA
Singapore	Personal Data Protection Commission (PDPC), Affected Individuals	As soon as practicable, within 72 hours if aware of the breach	Nature of the breach, types of personal data involved, and measures taken to address the breach.	NA
California	Consumers	When aware of unauthorized access, exfiltration, theft, or disclosure	Types of personal information affected, date(s) of the breach, contact info for the business, steps to protect from harm.	NA
Indonesia	Regulatory Authority, Affected Individuals	Within 72 hours if aware of the breach	Nature of the breach, potential consequences, and measures taken to mitigate the breach.	NA
Delaware	Affected Individuals, Authorities	Without undue delay, within 72 hours if feasible	Nature of the breach, categories and number of data subjects affected, contact info, likely consequences, and measures taken.	1) Data Protection Measures: If strong security measures (like encryption) have been used that make the data unreadable to unauthorized people, notification is not required. Low Risk Assessment: If it can be shown that the breach is unlikely to harm individuals' rights or freedoms,notification is not required.

SCHEDULE B

Comparative Overview of Supervisory Authorities for Data Protection

Country	Supervisory Authority
Saudi Arabia	Saudi Data & Artificial Intelligence Authority (SDAIA)
California	California Privacy Protection Agency (CPPA)
Dubai	Commissioner of Data Protection within the Dubai International Financial Centre (DIFC)
Singapore	Personal Data Protection Commission (PDPC)
Indonesia	Ministry of Communication and Information Technology (Kominfo)
Delaware	Delaware Department of Justice (DOJ)
India	Data Protection Board of India