HMSI Privacy Policy

Honda Motorcycle and Scooter India Private Limited

Document Control

S. No.	Type of Information	Document Data
1.	Document Title	HMSI Privacy Policy (Internal)
2.	Document Code	HMSI-ISMS-P3.0-12
3.	Date of Release	29 May, 2020
4.	Document Revision No	3.0
5.	Document Revision Date	20 Jan, 2026

Document Approval

S. No.	Name	Designation	Signature
1.	Katsuyuki Ozawa	Chief Compliance Officer Director - HR & Admin	Katsuyuki Ozawa
2.	Vinay Dhingra	Risk Management Officer Senior Director - HR & Admin	Vinay Dhingra
3.	Bhaskar Chhabra	Chief Information Officer/ Data Protection Officer Operating Head – IT	Bhasker Chhabra
4.	Sanjeev Kr. Chaubey	Chief Legal Officer Operating Officer – Governance, Risk & Compliance	Sanjeev Kumar Chaubey

Kandla Joshi Mohit Bhola Goji Sugita Vimal Bansal

Table of Contents

Kandla Joshi 24e4f809-05bd-457e-85c7-44f8c1399ac6
Mohit Bhola 881092a3-b31b-4763-8a45-7774644f4635
Goji Sugita 9e970017-0bfc-41dd-87b0-5c6065924d90
Vimal Bansal 3f8acc3b-cd12-4dbc-a348-b23cc84e47d6

Chapter 1: Background & Purpose of HMSI Privacy Policy

1.1 Purpose

This Policy specifies the special rules applicable to the management of **Personal Information**, in addition to the rules w.r.t. Personal Information contained in the HMSI Data Governance Policy.

This Policy applies whether such Personal Information is managed by Honda Motorcycle and Scooter India Pvt. Ltd. (HMSI) hereinafter called Company or Organization or a third party.

1.2 Objective

HMSI values the trust placed in us and therefore, we assure that we follow the highest standards of privacy guidelines to protect the information shared with HMSI in accordance with applicable laws.

The Policy intends to describe what personal information can be collected, why we collect and the intended use i.e. processing/ sharing & transfer of the personal information. Further, this policy also describes your personal data protection rights including a right to object. This policy shall be followed in accordance with the applicable laws, rules & regulations.

1.3 Scope

1. This Policy applies to all HMSI locations and Operations.

2. This Policy shall apply to all HMSI and other third-party employees (hereinafter called “Associates").

Every Associate shall ensure that the content of this Policy is extended to business partners (including suppliers, joint research and development collaborators and vendors) by an appropriate agreement to the extent possible.

1.4 Definitions

1. Personal Data

   Personal Data means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information including any inference drawn from such data for the purpose of profiling and also includes sensitive personal information as defined under the applicable law, rules & regulations.

2. Personal Information

   PII means any Information which is the personally identifiable information (PII) of any individual such as customers, associates (employees), or business partners, as defined by applicable laws, regulations, and industry standards. PII is a subset of Personal data.

3. Protected Systems

   For the purposes of this Policy, Protected Systems means those computers, computer systems or computer network to which the appropriate Government, by issuing gazette information in the official gazette, has declared as a protected system.

4. Data Fiduciary

   Data Fiduciary means any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of collecting or processing of personal data.

5. Data Principal

   Data Principal means the natural person to whom the personal data relates. The role of Data Principal also extends to certain representatives in specific situations:
   - For children under 18: The parent or lawful guardian is the Data Principal.
   - For persons with disabilities: Their lawful guardian acts as the Data Principal.

6. Data Processor

   Data processor means any person, including the State, a company, any juristic entity or any individual, who processes personal data on behalf of a data fiduciary.

7. PII Controller

   A PII Controller is a Process Activity Owner - a person/ persons designated by a company to collect/ manage access/ handle to Personal Data.

8. Consent Manager

   Consent Manager is a person or entity that is officially registered with the Data Protection Board of India (Board). It provides an accessible, transparent, and interoperable platform to enable data principals to give, manage, review, and withdraw their consent.

9. Processing

   Processing in relation to personal data, means an operation or set of operations performed on personal data, and may include operations such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction.

10. Data

    Data includes a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by humans or by automated means.

11. Financial Data

    Financial Data means any number or other personal data used to identify an account opened by, or card or payment instrument issued by a financial institution to a data principal or any personal data regarding the relationship between a financial institution and a data principal including financial status and credit history.

12. Health Data

    Health Data means the data related to the state of physical or mental health of the data principal and includes records regarding the past, present or future state of the health of such data principal, data collected during registration for, or provision of health services, data associating the data principal to the provision of specific health services.

13. Generic Data

    Generic data means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the behavioural characteristics, physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

14. Collection

    Collection means, in relation to personal data, any action or activity that results in the company obtaining, or coming into the knowledge or possession of, any personal data of another person.

15. Communication

    Communication means a word or words, spoken, written or indicated, in any form, manner or language, encrypted or unencrypted, meaningful or otherwise, and includes visual representations of words, ideas, symbols and images, whether transmitted or not transmitted and, if transmitted, irrespective of the medium of transmission.

16. Disclosure

    Disclosure (with its grammatical variations and cognate expressions) means, in relation to personal data, any action or activity that results in a person coming into the knowledge or possession of any personal data of another person.

17. Biometric Data

    Biometric Data means any data relating to the physical, physiological or behavioral characteristics of a person which allow their unique identification including, but not restricted to, facial images, fingerprints, handprints, footprints, iris recognition, handwriting, typing dynamics, gait analysis and speech recognition.

18. Notification

    Notification published in the Official Gazette and the expression notify shall be construed accordingly.

19. Official Identifier

    Any number, code, or other identifier, assigned to a data principal under a law made by Parliament or any State Legislature which may be used for the purpose of verifying the identity of a data principal. Person includes:
    - an individual
    - a Hindu undivided family
    - a company or firm
    - an association of persons or a body of individuals, whether incorporated or not,
    - the State, and
    - every artificial juridical person, not falling within any of the preceding sub-clauses

20. Personal Data Breach

    Any unauthorized or accidental disclosure, acquisition, sharing, use, alteration, destruction of or loss of access to, personal data that compromises the confidentiality, integrity or availability of personal data to a data principal.

21. Primary Purpose of Collection of Information

    Primary Purpose of Collection of information means to collect any information which is necessarily required by HMSI to perform one or more of its functions or activities which is collected by lawful and fair means and not in an unreasonable intrusive way.

22. Secondary Purpose of Collection of Information

    Secondary Purpose of Collection of information means any purpose other than the Primary Purpose of Collection of information as specified in Section 5.5 Retention or Erase or Deletion or Suspension of Use Point No #4.

23. Child

    Child means a person who has not completed 18 years of age.

24. Consent

    The consent given by the Data Principal shall be free, specific, informed, unconditional and unambiguous with a clear affirmative action, and shall signify an agreement to the processing of her personal data for the specified purpose and be limited to such personal data as is necessary for such specified purpose.

25. Prescribed

    Prescribed means prescribed by rules made under this Act.

26. Profiling

    Profiling means any form of processing of personal data that analyses or predicts aspects concerning the behavior, attributes or interests of a data principal.

27. Regulations

    Regulations means the regulations made by the Authority under this Act.

28. Damage includes:

- loss, distortion or theft of identity
- financial loss or loss of property
- loss of reputation or humiliation
- loss of employment
- any discriminatory treatment
- any subjection to blackmail or extortion
- any denial or withdrawal of a service, benefit or good resulting from
- an evaluative decision about the data principal
- any restriction placed or suffered directly or indirectly on speech
- movement or any other action arising out of a fear of being observed or surveilled
- any observation or surveillance that is not reasonably expected by the data principal

1.5 Positioning of Policy

This Policy is intended to set minimum standard controls with respect to the handling of Personal data in accordance with the applicable laws, rules and regulations.

1.6 Amendments to Policy

Any revisions to this Policy shall be determined and approved by Chief Compliance Officer (CCO). For more details refer HMSI Data Governance Committee.

This policy shall be reviewed/ approved on yearly basis or whenever any significant changes in the process, to continuously improve and enhance HMSI's management of personal data and to meet changes in HMSI's business environment or in the Indian legal environment(s) in which HMSI operates.

Chapter 2: Personal Information Management Organization

Personal Information Management Organization governed by HMSI Data Governance Committee Organization. Refer HMSI Data Governance Policy Section 2.1.01.

2.1 Data Protection Officer (DPO)

DPO is the management representative, will assist and monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIA). Refer HMSI Data Governance Committee/ ISMS Organization.

2.2 Chief Privacy Officer

The Data Protection Officer (DPO) of the Company shall also be the Chief Privacy Officer of the Company.

The role of Chief Privacy Officer shall be as follows:

1. To proactively implement policies and programs to enhance the protection of Personal data, to promote such programs, and to create training programs designed to bolster the handling of Personal data.

2. To report to the Company/ Regional Data Governance Committee and all other appropriate parties when a leakage or violation occurs within the Company, and to formulate and implement corrective measures.

3. Advising on data breach monitoring, management and reporting; and advising on responses to privacy rights requests from individuals.

4. Wherever required, to act as the representative of the Company in providing assistance or collaborating with the government to formulate industry standards, regulations, and laws, and in responding to government requests.

5. Monitoring an organization's data protection compliance and informing and advising it on its data protection obligations.

6. Acting as the contact point for Data Protection Board of India for all data protection issues and seeking consultation with legal team where applicable.

7. Such other responsibilities as may be required by applicable law, rules & regulations.

2.3 Role of HMSI Data Governance Committee

The HMSI Data Governance Committee shall be responsible for the overall governance and implementation to achieve the objective of this Policy.

Chapter 3: Personal Information Management

3.1 Personal Data Secrecy

Personal data will be categorized as Secrecy A (Secret). However, employee-related data used operationally within the company such as Employee Code, official mobile phone numbers, and official email addresses, are managed and operated as Secrecy B (Internal).

For details, refer HMSI Data Governance Policy (section 1.5 Handling of Confidential information).

3.2 Personal Inventory

1. HMSI shall maintain a list of Personal Data Collection Inventory or Record of Processing Activities (RoPA) owned by HMSI which include reason for collecting personal data.

2. Inventory shall be updated by Division ISSC (Information Security Steering Committee) members at least once in a year or whenever any change in their process.

3.3 Data Protection Impact Assessment (DPIA) & Audit

HMSI will conduct Data Protection Impact Assessment on periodic basis by an independent auditor to check the effectiveness of data privacy control implementation in HMSI. This impact assessment will be done considering India Personal Data Protection Act (DPDP). Data protection impact assessment contains the following:

1. Detailed description of the proposed processing operation, the purpose of processing and the nature of personal data being processed.

2. Assessment of the potential damage that may be caused to the data principals whose personal data is proposed to be processed.

3. Measures for managing, minimizing, mitigating or removing such risk of damage.

3.4 Responsibilities of Managers

1. For each system (of whatever kind) containing Personal data collected or used by his or her Division, the Division Manager shall use the nominated ISSC member (refer HMSI Data Governance Organization) to supervise the system and to ensure that appropriate confidentiality measures are in place. The ISSC member shall ensure that associates who handle Personal data (PII Controller) in the Division are identified and listed.

2. The Division Manager that collects or uses Personal data shall bear responsibility for the proper maintenance and use of systems containing Personal data within the Division in accordance with this policy.

3.5 Training

1. ISMS Secretariat shall provide training to personnel across all levels to ensure they understand data protection principles and Digital Personal Data Protection Act (DPDP Act) requirements.

2. Where the handling of Personal data is entrusted to a business partner, the Division Manager, of the Division that collects or uses such Personal data shall ensure that the business partner and related associates are trained in the proper handling of Personal Data.

3.6 Assessment and List of Locations Where Personal Information is Stored

To evaluate the type of Personal Information collected or used by each Division, each Division Manager shall prepare a list of places (including electronic systems) where Personal Information so collected or processed is stored and shall submit this list to the ISMS Secretariat which is a part of personal data Collection Inventory, refer section 3.2.

Notwithstanding the preceding provisions, it is not necessary to list categories or types of Personal Information which have been classified as "Secrecy B" according to HMSI Data Governance policy.

The Division Manager shall update the list required by this section when the Division stops collecting or using a listed type or category or information.

3.7 Supervision of Associates

Where a Division collects, uses, or manages Personal Information, the Division Manager shall ensure that associates under his or her supervision are appropriately trained with respect to the handling of Personal Information and that they understand the importance of handling such information with enhanced care, the systems for handling such information, and the consequences of failing to properly manage such information.

3.8 Outsourcing Management of PII to Business Partners

Where it is necessary to outsource the collection or use of Personal Information to a business partner, the Division Manager shall:

1. Confirm that the business partner has sufficient systems, policies, and practices in place to protect such Personal Information, to a standard conforming with the Company's requirements for handling of Personal Information.

2. Conclude a Confidentiality Agreement with the business partner which shall include specific provisions describing requirements such as preventing misuse, unauthorized access to, modification, disclosure or destruction of personal data for handling of Personal Information.

3. Prohibit subcontracting in general with respect to handling of Personal Information and require that the business partner obtain the prior written agreement/consent of the Company if subcontracting with respect to handling of Personal Information is unavoidable.

4. Receive back all Personal Information collected, used, or maintained by the business partner after completion of the outsourced work.

5. Require the business partner to refrain from using any Personal Information collected, used, or maintained because of the outsourced work for any other purpose.

6. The Division Manger also need to notify Data Governance Committee regarding outsourcing management of PII processing. For more detail refer Section 4.4 Notification.

Chapter 4: Collection and Use of Personal Information

4.1 Collection

1. HMSI will generally collect personal information, through HMSI Website /Portals/ Applications/ Mobile Apps / Social Media accounts. HMSI may also collect personal information through other methods while interactions through physical visit, post, telephone, email writing or from a third-party source, such as our dealers, vendors, business partners, government authorities or any other source which are legally acquired by HMSI.

2. HMSI will not collect personal information unless the information is necessary for one or more of its functions or activities and the information will only be collected by lawful and fair means not in any un-reasonably intrusive way.

3. When the Company collects Personal Information, it shall clearly state the purpose for which the information will be used. At times, HMSI may request personally information to provide services or correspondence to website visitors (such as new vehicle alerts, promotions, or mailed brochures), this information (such as name, mailing address, e-mail address, type of request, and other relevant details) is collected and stored by HMSI appropriately based on the nature of the data and is used solely to fulfil the visitor's request. Such information is used to improve the services provided by HMSI.

4. HMSI will never sell personal information to any other company for that company's independent use. HMSI also shares user information from time to time with affiliates and business partners such as its authorized Dealer body to provide consistent service, support and marketing to its existing and prospective customers.

5. HMSI shall always adhere to data minimization principle, which mandates that personal data to be collected by HMSI should be limited to what is necessary for the specific purpose. Data minimization is intended to minimize the risk of data leaking, identify important data and restrict extracted data outside the company.

6. HMSI shall encourage privacy as default practices into the systems and processes like data protection obligations (such as purpose limitation, collection limitation, data quality and data storage) are reflected in business practices and in IT systems.

4.2 Notification

At the time of Personal Information collection, HMSI shall notify the person to whom the Personal Information belongs. Such notification may take any form (as specified by the HMSI Data Governance Committee) and shall include the following elements:

1. The identity of the HMSI contact information for the Company to whom the Personal Information belongs.

2. The manner in which Personal Information has been (or will be) collected (for example, the use of cookies in a web browser) and the purpose for which it will be used.

3. The collected Personal Information shall be transmitted, handled & destroyed as per the applicable law or in a manner that will preserve its confidentiality.

4. If necessary, under local laws and regulations, the right of the person to whom the Personal Information belongs to request that HMSI correct, deletes, or suspend the use of the Personal Information, and the method of exercising that right.

5. Any other entities which may receive the information.

6. Any other notice requirements provided by applicable laws or regulations.

7. HMSI will notify or inform Data Protection Board (DPB) about the breach of any personal data processed by the data fiduciary where such breach is likely to cause damage to any data principal.

4.2.1 Notification to Data Governance Committee:

Personal information should be systematically managed and notified to the Data Governance Committee for below cases:

- When acquiring personal information and creating a personal information database
- When entrusting acquisition or handling of personal information to outside parties

PII Controller will share the purpose in the required format (Annexure-B) to the Data Governance Committee for which Personal Information will be collected, stored, used and also control access management of Personal Information.

In case, the Personal Information is shared with Data Processor or other third parties, PII Controller need to ensure that required security controls should implemented at their end.

Further, PII Controller needs to sign an agreement with Data Processor or other third parties before sharing Personal Information which includes the following requirements:

1. In the event a party to this Agreement shall disclose to the other, any information ("Personal Data") relating to an identified or identifiable natural person, then with respect to such Personal Data, the other party shall:

   a. Collect, store, disseminate, retrieve, use or disclose such Personal Data only for the purposes of this agreement / contract. The other party will ensure all personal data security measures while collecting, storing & deletion of Personal Information.

   b. Not disclose Personal Data to any person or entity other than its employees who may be requiring access to such information to provide services in connection with the contract. Data Processor will share updated list of their personnel and / or Sub-Contractor who will have Personal Information access with HMSI.

   c. Not place the other party in breach of any of the requirements of the applicable laws with respect to Privacy.

   d. Promptly notify the other party if it receives any legally binding request for disclosure of the Personal Data.

   e. Promptly notify the other party in case of any accidental or unauthorized access or disclosure of the Personal Data (data leakage) and support for all required investigations.

   f. Promptly return the Personal Information in case agreement between HMSI and Data Processor/ third parties has been expired or terminated.

   g. Promptly delete the Personal Information in case data retention timeline completed after confirmation from the Data Provider.

2. The other party to the contract under no circumstances will become the owner of the Personal Data disclosed under this contact.

3. The party to this agreement agrees and undertakes to comply with the requirements of applicable Data Protection Laws in connection with performance of its obligations under this contract.

4. The parties to this agreement shall be liable to maintain technical and organizational processes and procedures that ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected to safeguard all personal information from and against any accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access. The parties to this Contract shall comply with the "Personal Information Handling Outsourcing Standards" and ensure to implement security measures such as data masking, encryption, password protected etc. “Personal Information Handling Outsourcing Standards outline how organizations must manage, protect, and control personal data when outsourcing its processing to third-party vendors”.

5. PII controllers will inform to Data Governance Committee and Data Principal in case any personal data gets breached and follow the Information Security Incident Process flow (refer HMSI Data Governance Policy for reporting incident).

4.3 Consent

1. If required by applicable laws, regulations, or industry standards the Company shall obtain the agreement of the person to whom the Personal Information belongs with respect to the purpose of its use. Where such an agreement is not required by applicable laws, regulations, or industry standards, the Company shall give notice to the person to whom the Personal Information belongs.

2. At the time of collecting the personal data or information, the Company shall provide an option to the provider of the information to not to provide the data or information sought to be collected.

3. Notwithstanding Paragraph 1 of this section, the Company need not obtain agreement or give notice to the person to whom Personal Information belongs under the following circumstances.

4. If the collection or use of the person’s Personal Information is necessary for the completion of a contract or business arrangement with that person, and the person has agreed in advance to such collection or use.

5. If it is necessary to collect or use the Personal Information due to legal requirements.

6. If required by the State for providing benefits to the individual,

7. To respond to a medical emergency,

8. During employment related,

9. Necessary for reasonable purposes such as prevention of fraud, mergers and acquisitions, recovery of debt etc.

10. In case of child (age below 18 years) personal data, company shall implement appropriate mechanism to verify child age and must obtain explicit consent from parent / legal guardian.

11. HMSI will determine when and how consent is to be obtained and will ensure below points while taking consent:
    - Free
    - Informed
    - Specific
    - Clear
    - Capable of being withdrawn (consent is sought before processing)
    - Determine what makes consent 'explicit'.
    - Keep records of consent

4.4 Processing of Personal Data/ Information

1. By visiting the website /Portals/ Applications/ Mobile Apps / Social Media accounts of HMSI and by providing personally identifiable, the person providing such information understands and consents to the collection, use, processing, transfer and disclosure of your personally identifiable information in accordance with this Privacy Policy. Such consent shall be deemed to include consent to transfer of the personally identifiable information to locations that may have different levels of privacy protection than in India.

2. Considering the nature, scope and purpose of processing personal data, necessary security safeguards shall be implemented to prevent misuse, unauthorized access, modification or destruction of personal data.

3. HMSI will process personal data by its operations covering following:
    - Fair and reasonable processing
    - Purpose limitation
    - Collection limitation
    - Lawful processing
    - Notice
    - Data quality
    - Data storage limitation
    - Accountability

4. HMSI shall limit the processing of PII to the minimum that is relevant, adequate and necessary for the identified purposes.

5. The personal data may be processed without obtaining consent if such processing is necessary for such reasonable purposes as may be specified by regulations, after taking into consideration:
   - The interest of the data fiduciary in processing for that purpose.
   - Whether the data fiduciary can reasonably be expected to obtain the consent of the data principal.
   - Any public interest in processing for that purpose.
   - The effect of the processing activity on the rights of the data principal.
   - The reasonable expectations of the data principal having regard to the context of the processing.

   The reasonable expectations:
   - prevention and detection of any unlawful activity including fraud.
   - whistle blowing.
   - mergers and acquisitions.
   - network and information security.
   - credit scoring; checking for suppliers.
   - recovery of debt.
   - processing of publicly available personal data.
   - the operation of search engines.

6. HMSI may process the personal data of a Data Principal if the Data Principal has voluntarily provided such data and has not informed the Data Fiduciary of any objection or withdrawal of consent regarding its use.

7. HMSI shall keep records of data processing practices. These records must include details of the regular reviews of the security safeguards.

8. HMSI shall have a written contract with PII processor that it uses and shall ensure that their contracts with PII processors address the implementation of the appropriate controls in PIMS SOA.

9. HMSI shall record transfers/ disclosures of PII to or from third parties and ensure cooperation with those parties to support future requests related to obligations to the PII principals.

4.5 Sensitive Personal Information of Persons who are Not Associates/ Employees or Business Partners

1. In general, HMSI shall not collect or use the following types of information with respect to persons who are not Associates/Employees or business partners:

   - Passwords
   - Financial Information such as Banks Accounts, credit cards, debit cards and other payment instrument details
   - Sexual Orientation
   - Biometric information
   - official identifier
   - genetic data
   - transgender or intersex status
   - Matters concerning the faith, caste or religious beliefs of a person
   - Race, ethnicity, family status, physical or mental disorders, and criminal history, except to the extent required or permitted by law

2. Matters concerning execution of the right to organize, collectively bargain and any other group movement by workers

3. Matters concerning political participation or beliefs of a person; and

4. The matters concerning health and medical treatment, and sex life.

4.6 Transfer of Personal Information

1. If required by applicable laws, regulations, or industry standards, HMSI collects or uses Personal Information and intends or transfer it across international boundaries except where the Central Government restricts such transfer to specific countries. It will notify and obtain the agreement of the person who owns the information.

2. HMSI may transfer customer personal data to another authorized dealer or service network (a "Successor Dealer") if the dealer from whom data was originally collected ceases to operate, is terminated, resigns, or is replaced.
   Such transfer is carried out to ensure continuity of services, fulfilment of warranty and safety obligations, customer support, and other legitimate business purposes.

HMSI remains the Data Fiduciary and continues to determine the purpose and means of processing your personal data. The Successor Dealer acts strictly as a Data Processor on behalf of HMSI and is bound by confidentiality, data protection, and security obligations.
Customers retain all their rights under applicable law, including the right to access, correct, update, or request erasure of their personal data, as well as the right to raise grievances via HMSI's designated grievance mechanism or Data Protection Officer.

3. HMSI may transfer Personal Data to any other Honda Company or third party within or out of India subject to the condition that no personal data shall be transferred to any entity that is not duly authorized by HMSI, and all transfers shall take place through secure, approved systems in compliance with the Digital Personal Data Protection Act, 2023.

Chapter 5: Requests by Owners of Personal Information

5.1 Obligation to Data Principal

1. HMSI shall determine and document their legal, regulatory and business obligations to data principals related to processing of their PII and provide the means to meet these obligations.

2. HMSI shall determine and document the information to be provided to data principals regarding the processing of their PII and the timing of such a provision.

3. HMSI shall Implement mechanism to exercise data principal rights to ensure following:
   - The right to confirmation and access
   - The right to correction
   - The right to be forgotten and withdraw/ deletion
   - The right to object PII processing
   - The right to Nominate (manage their data on behalf in case of death & incapability)

5.2 Requests for Disclosure of Personal Information

1. With respect to Personal Information collected or used by HMSI, HMSI shall be prepared, if required by local laws and regulations and upon request by the person to whom the Personal Information belongs, to disclose the following:

   - The kind of Personal Information collected or used and, to the extent possible, the sources of such Personal Information.
   - The identity of any third parties, if any, to whom the Personal Information has been disclosed, and the reason(s) for such disclosure.
   - If the person has a right to request correction, deletion, or suspension including right to restrict or prevent the continuing disclosure of his personal information.
   - under local laws or regulations, the disclosure shall so state; and
   - Any other information required by law.

2. The appropriate form of disclosure requests and of the disclosures themselves, including the security requirements necessary to verify the identity of a person requesting disclosure, shall be decided by the HMSI Confidentiality Committee.

3. The Division Head shall have ultimate responsibility for determining whether a disclosure request for Personal Information has been appropriately made.

4. In addition, if the disclosure meets any of the following criteria, the HMSI Data Governance Committee shall determine whether disclosure is appropriate:

   - If disclosure may threaten the life, body, property, or other right or interest of the person to whom the Personal Information belongs or a third party; and
   - If disclosure would violate applicable laws or regulations.

5. If a disclosure request was not appropriately made or the HMSI Confidentiality Committee determines that disclosure is inappropriate for the reasons listed in the preceding Paragraph, the Company shall timely notify the person to whom the Personal Information belongs of the denial and the reason for it.

5.3 Correction

1. HMSI will take reasonable steps to correct personal information to ensure that, having regard to a purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading, if either:
   - is satisfied that it needs to be corrected; or
   - an individual request that their personal information be corrected.

2. Data Principal can follow below method for correction in their personal information as collected by HMSI:
   - In writing by sending an email on grievance officer email id.
   - Posting a letter on grievance officer address.
   - By accessing and managing consent preferences through the Dedicated Preference Centre or Consent Preference Management links embedded on HMSI's websites or digital platforms, where such functionality is enabled.

5.4 Right to Withdraw Consent:

1. HMSI will provide the right to withdraw consent mechanism to data principal to withdraw his/ her consent at any time by notifying the same to HMSI though any of methods as mentioned in section 5.3 Correction.

2. Data principal can withdraw his consent from the processing of any personal data without disclosing any valid reason, however, all legal consequences for the effect of such withdrawal shall be the borne by such data principal.

3. HMSI will ensure provision of HMSI's goods or services, or performance of a contract is not conditional on consent to processing any personal data that is not necessary for that purpose.

5.5 Retention or Erase or Deletion or Suspension of Use

1. If required by applicable laws or regulations, HMSI shall implement a method for the person to whom the Personal Information belongs to request deletion or suspension of use of the Personal Information when the following criteria are met:

    - If the Personal Information is no longer necessary for the purpose for which it was collected or used; If the agreement to process the data is canceled, the valid period of agreement to keep the data has expired and there is not any legal ground to process the data; and
    - If the person to whom the Personal Information belongs objects to its further collection or use on legal grounds.

2. HMSI may choose to retain or continue the use of Personal Information that has been requested for deletion or suspension, if retention or continued use would:

    - Be necessary to protect the public good, whether for health and safety or other reasons.
    - Serve the purpose of historical, statistical, or scientific research.
    - Be necessary to maintain compliance with applicable statutes or regulations.
    - The retention shall be in accordance with the HMSI Data Governance Policy.

3. The use of Personal Information shall be restricted in the following situations:

    - While the Personal Information is being corrected, if the person to whom the Personal Information belongs has made a valid request for correction.
    - When HMSI does not need the Personal Information for business purposes, but it is being preserved as evidence.
    - If the person to whom the information belongs objects to deletion of Personal Information because the method of processing is illegal and the person to whom the information belongs requests HMSI to restrict its use until the validity of the processing method is established.

4. HMSI will not use or disclose personal information for a purpose other than the primary purpose of collection, unless:

    - The secondary purpose is related to the primary purpose, and the individual would reasonably expect the organization to use or disclose the information for the secondary purpose.

- the individual has consented to the use or disclosure.
- the organization reasonably believes that the use or disclosure is necessary to lessen or prevent a serious and imminent threat to an individual's life, health or safety; or a serious threat to public health or safety.
- the organization uses or discloses the personal information in investigating a suspicion of unlawful activity or in reporting its concerns to relevant persons or authorities; or
- the use or disclosure is required.
- authorized by or under law.

5. HMSI shall take necessary steps to notify all relevant entities or individuals to whom such personal data may have been disclosed regarding the relevant correction, completion, updating or erasure, particularly where such action may have an impact on the rights and interests of the data principal or on decisions made regarding them.

5.6 Designation of contact for requests related to Personal Information

HMSI Data Governance Committee shall establish a contact for inquiries related to personal information, including requests for deletion/ withdrawn, correction, or suspension of use and prominently display that contact information to the public.

5.7 Grievance Officer

1. HMSI has designated a Grievance Officer to address the grievances of its information providers including those of customers, associates (employees), or business partners.

2. HMSI shall publish the contact details of such Grievance Officer on their website.

3. The grievances so raised before the Grievance Officer appointed by HMSI shall be redressed within a month of the filing of such grievance.

4. Providing information and advice on matters relating to fulfilling obligations under the applicable laws.

5. Monitoring personal data processing activities to ensure that such processing does not violate the provisions of Law.

6. Providing advice on carrying out the data protection impact assessments and carry out its review.

Contact Information:

In case of any complaint or grievance, User may contact the following: **Grievance Officer**

Honda Motorcycle & Scooter India Pvt. Ltd.
Plot No. - 01, Sector – 03, IMT Manesar, Gurgaon - 122050
Email: persinfo.grievance@honda.hmsi.in
Emails received on persinfo.grievance@honda.hmsi.in other than context of Privacy Policy will not be entertained. Please use other sections like Reach us, FAQ section or customer care number for product related queries/ other complaints.

Note: All email as received on persinfo.grievance@honda.hmsi.in, need to be documented for future reference.
All third-party associates can raise any concern pertaining to personal data and forward such concerns / emails to relevant reporting managers.

For Grievance Reporting and Response Process, refer Annexure A.

Chapter 6: Action in case Personal Information Leakages

6.1 Reasonable Security Practices & Procedures to be Followed

1. HMSI shall have and implement reasonable security practices and standards for personal data information.

2. HMSI shall take reasonable technical and organizational precautions and implement certain security safeguards to prevent the loss, misuse, unlawfully accessed, modification, destroyed or alteration of any personal data/information stored with them.

3. HMSI shall store all the personal information provided to them on a secure (Data encryption, password and firewall protection) servers.

4. All electronic and financial transactions entered through the website / Portals/ Applications/ Mobile Apps of HMSI will be protected by encryption technology.

5. The information providers shall acknowledge that the transaction of information over the internet is inherently insecure and HMSI cannot guarantee the security of data sent to them over the internet. HMSI shall subject PII transmitted over a data transmission network to appropriate controls designed to ensure that the data reaches its intended destination.

6. The security safeguard shall be periodically reviewed in such manner as may be specified by applicable laws and appropriate measures shall be taken accordingly.

6.2 Response to a Leakage Involving Personal Information

In the event of a leakage or loss of Personal Information, in addition to following the processes described in HMSI Data Governance Policy Section 3.7 Violations, the Chief Privacy Officer of the Company (or the HMSI Data Governance Committee as appropriate) shall evaluate the scope of the leakage or loss, the identity of persons affected by the leakage or loss, the appropriate notice(s) to be given, and shall effect such notice(s).

In addition, the Chief Privacy Officer shall report any such incident to the Risk Management Officer and the Chief Compliance Officer.

6.3 Consequences of Breach of Personal Data

1. Any unauthorized access of the computer system (or any personally sensitive information therein) by any individual, associate (employee) or partner, shall be punishable as per the applicable laws, rules & regulations.

2. Any unauthorized downloading, extraction, copying of data or any unauthorized introduction of computer virus of contaminants shall also be covered under the consequences.

3. If any individual, associate (employee) or partner conducts any mode of hacking with the intention or knowledge of causing wrongful loss or damage to any person, the person who accessed such information shall be punishable in accordance with the applicable laws, rules & regulations.

4. Any individual, associate (employee) or partner who wrongly causes any computer resource to be either destroyed, deleted, altered or diminishes its value, shall also be liable to be prosecuted in accordance with the applicable laws, rules & regulations.

5. Any unauthorized access or attempt to secure access of any protected computer system or network by the government, shall also attract criminal proceedings which would be initiated by HMSI.

6. Any unauthorized access of data stored in a Protected System in contravention of any law by any individual, associate (employee) or partner.

7. Shall make the person who accessed such data liable for punishment in accordance with the applicable laws, rules & regulations.

8. Any individual, associate (employee) or partner who knowingly and intentionally discloses personal data and information without consent of the person concerned and in breach of a lawful contract shall have committed breach of confidentiality and piracy and shall be liable for punishment in accordance with the applicable laws, rules & regulations.

9. Any individual, associate (employee) or partner who has been entrusted with the personal data/information if dishonestly misappropriates such information or coverts it into his own property, or dishonestly uses or disposes off that personal data/information in violation of this Privacy Policy and the Indian Law in force shall have committed Criminal breach of trust and shall be liable to be prosecuted in accordance with the applicable laws, rules & regulations.

6.4 Penalties, Compensation and Offences

1. The Data Protection Board of India has the power to issue penalties up to INR 250 crore against DPDP Act 2023 upon failure to comply with its legal requirements.

2. While determining the amount of monetary penalty to be imposed, the Board shall consider following conditions, namely:

- The nature, gravity and duration of the breach
- The type and nature of the personal data affected
- Whether the person, as a result of the breach, has realized a gain or avoided any loss
- Whether the person took any action to mitigate the effects and consequences of the breach, and the timeliness and effectiveness of such action
- Whether the monetary penalty to be imposed is proportionate and effective having regard to the need to secure observance of and deter breach of the provisions of this Act
- The likely impact of the imposition of the monetary penalty on the person

3. Prevention of doing re-identification of data from de-identification data:

- Re-identifies personal data which has been de-identified (removing information from a database) by a data fiduciary or a data processor or
- Re-identifies and processes such personal data as mentioned in section (a),
- Without the consent of such data fiduciary or data processor, then such person shall be punishable with imprisonment for a term not exceeding three years or with a fine which may extend to two lakh rupees or both.

6.5 Choice of Sharing Information

Any person may choose to share Personally Identifiable Information with HMSI. However, any participation in using our HMSI Website/ Portals/ Applications/ Mobile Apps/ Social Media accounts and providing Personally Identifiable Information is completely voluntary. Anyone can choose to unsubscribe and opt-out to certain communications and access, or update and delete their contact information, by contacting us at the email address/number or address specified below.

6.6 Accessing and updating your information

HMSI shall give access to personal information held by it on request by the individual to which the information pertains to, except:

- in the case of personal information other than health information - providing access would pose a serious and imminent threat to the life or health of any individual; or
- in the case of health information - providing access would pose a serious threat to the life or health of any individual; or
- providing access would have an unreasonable impact upon the privacy of other individuals; or
- the request for access is frivolous or vexatious; or

- the information relates to existing or anticipated legal proceedings between the organization and the individual, and the information would not be accessible by the process of discovery in those proceedings; or
- providing access would reveal the intentions of the organization in relation to negotiations with the individual in such a way as to prejudice those negotiations; or
- providing access would be unlawful; or
- denying access is required or authorized by or under law; or
- providing access would be likely to prejudice an investigation of possible unlawful activity.
- providing access would be likely to prejudice:

a) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law; or
b) the enforcement of laws relating to the confiscation of the proceeds of crime; or
c) the protection of the public revenue; or
d) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or
e) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders; by or on behalf of an enforcement body; or
f) an enforcement body performing a lawful security function asks the organization not to provide access to the information on the basis that providing access would be likely to cause damage to the security of India.

6.7 Jurisdiction

The Privacy Policy shall be governed by the laws of India and the Courts in Gurgaon, Haryana shall have exclusive jurisdiction in respect of all matters arising out of, or concerning or incidental to this Privacy Policy.

HMSI shall identify and document the relevant basis for transfers of PII between jurisdictions.

6.8 Liability Disclaimer

1. The information, software, products, and services included in or available through this website may include inaccuracies or typographical errors. Changes are periodically made to this website and to the information therein.

2. HMSI makes no representations about the suitability, reliability, availability, timeliness, lack of viruses or other harmful components and accuracy of the information, software, products, services and related graphics contained within the website for any purpose. All such information, software, products, services and related graphics are provided "as is" without warranty of any kind. HMSI hereby disclaim all warranties and conditions regarding this information, software, products, services and related graphics, including all implied warranties and conditions of merchantability, fitness for a particular purpose, work man like effort, title and non-infringement.

3. HMSI shall not be responsible for unauthorized access to or alteration of any transmissions or data, any material sent or received or not sent or received, or any transactions entered into through HMSI's website. In no event shall HMSI and/or its suppliers be liable for any direct, indirect, punitive, incidental, special, consequential damages or any damages whatsoever including, without limitation, damages for loss of use, data or profits, arising out of or in any way connected with the use or performance of the this website/services, with the delay or inability to use the website/services, the provision of or failure to provide services, or for any information, software, products, services and related graphics obtained through this website/services, or otherwise arising out of the use of this website/services, whether based on contract, tort, negligence, strict liability or otherwise, even if HMSI or any of its suppliers has been advised of the possibility of damages. If customer are dissatisfied with any portion of this website/services, or with any of these terms of use, their sole and exclusive remedy is to discontinue using the website/services. HMSI makes no warranty that any service on this website will be uninterrupted, timely, secure or error-free.

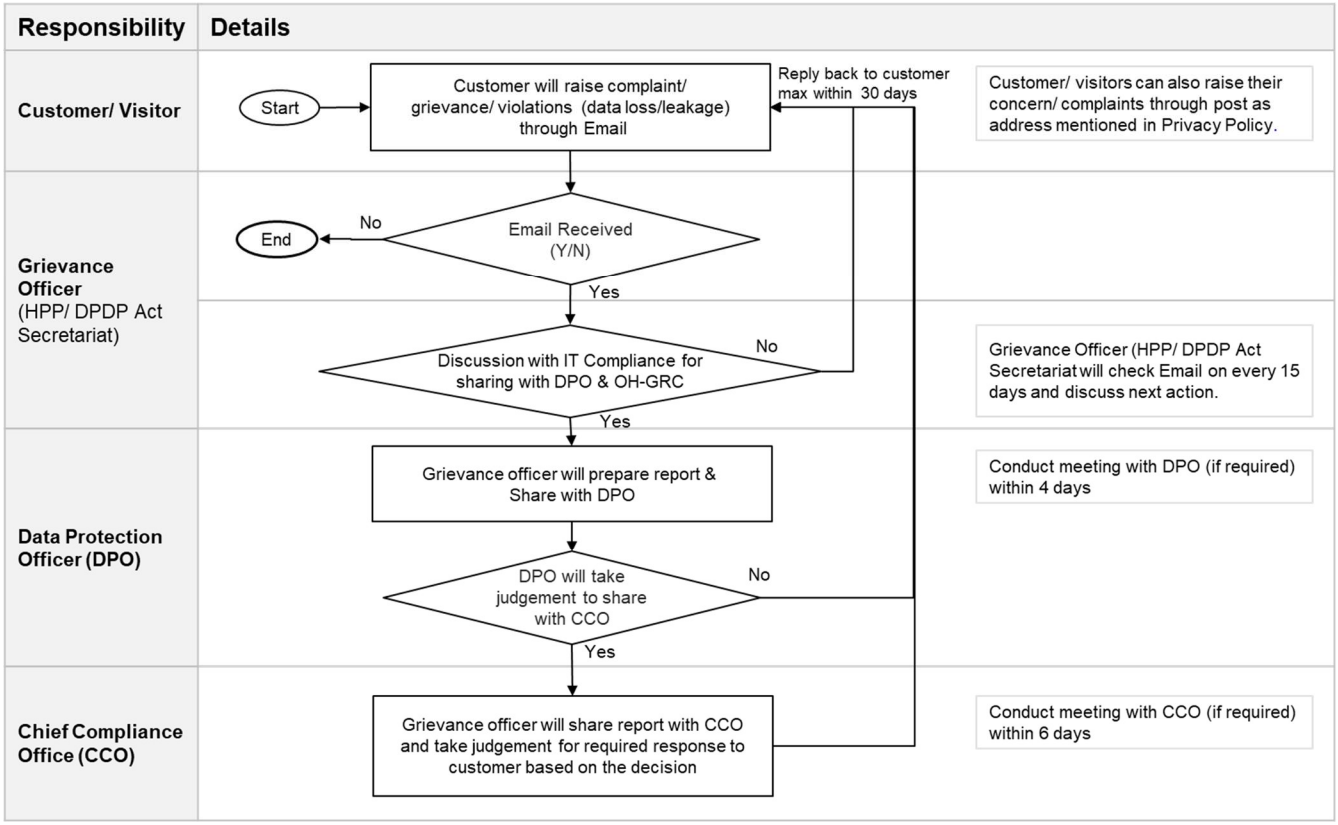
4. HMSI reserves the right to disclose any personal information about you or your use of the HMSI Site/ Services, including its contents, without your prior permission if HMSI has a good faith belief that such action is necessary to:
   a. conform to legal requirements or comply with legal process
   b. protect and defend the rights or property of HMSI or its affiliated companies
   c. enforce the terms or use

5. Nothing contained in this Policy is in derogation of HMSI's right to comply with governmental, court and law enforcement requests or requirements relating to your use of the HMSI Site/Services or information provided to or gathered by HMSI with respect to such use. If any part of this Policy is determined to be invalid or unenforceable pursuant to applicable law including, but not limited to, the warranty disclaimers and liability limitations set forth above, then the invalid or unenforceable provision will be deemed superseded by a valid, enforceable provision that most closely matches the intent of the original provision and the remainder of the Policy shall continue in effect.

Kandla Joshi
Mohit Bhola
Goji Sugita
Vimal Bansal

Annexure – A

Grievance Reporting and Response Process:



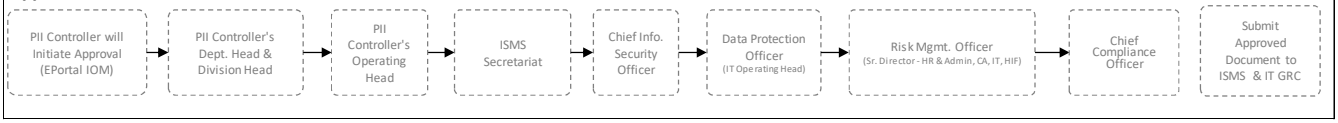
Kandla Joshi Mohit Bhola Goji Sugita Vimal Bansal

Annexure - B

Personal Data Notification/ Approval Process Flow:

Personal Data Collection Notification to Data Governance Committee				HMSI-IT -F2-15
PII Controller Details				
Emp. Code		Emp. Name		
Operation		Division / Department		
Designation		Location		
Purpose of Personal Data Collection				
Personal Data Collection Source				
Data Principal (Individuals whose personal data is being collected)				
☐ Employee ☐ Customer ☐ Supplier ☐ Dealer ☐ Other _____Please Specify				
Type of Personal Data				
☐ Name ☐ Contact No. ☐ Personal Mail ID ☐ Address ☐ Identity Proof _____Please Specify ☐ Other Details _____Please Specify				
Data Principal Consent Management				
Consent Implemented (Yes/ No)		If "Yes" - Attach Consent Form/ System screenshot as supporting document If "No" - Mention Consent Implementation target date		
Data Storage location (if multiple locations, kindly mention all)				
Personal Data Shared or Transferred Details				
Is Personal Data shared/ transferred (specify Operation/ Division/ Other Genpo detail)		If Personal Data shared/ transferred, specify data sharing/ transfer method (Email/ External Media/ Cloud/ Web transfer method/ FTP/ Other)		
Data Processor (processes personal data only on behalf personal data controller)				
Data Processor (Yes/ No)		If Data Processor Yes, specify Data Processor Name & attached signed agreement (with PII clause) as supporting document		
Declaration				
☐ I have understood and filled all above information correctly and attached the relevant documents.				

Approval Flow



Kandla Joshi
Mohit Bhola
Goji Sugita
Vimal Bansal

Document Review

Policy Version	Revision Date	Nature of Change	Date Approved/ Applicability
1.0	29 May, 2020	Initial Release	29 May, 2020
2.0	12 Nov, 2021	Incorporate below change points based on Internal Audit & IT Act/ PDP (draft bill) assessment: • Article 1: Added Objective, Scope and Definitions as per PDP Bill • Article 2: Personal Information Mgmt. Organization – HCP reference added • Article 3: Data Protection Impact Assessment & audit section added • Article 4: Consent statement for child and Clause 4.1 (IA) added • Article 5: Retention Reference and Data Protection Officer Responsibility added	12 Nov, 2021
2.1	23 Apr, 2024	• Removed Honda Wing Logo • Added Date Approved/ Applicability in Document Change Approvals • Article 1 Section 1.4 “Definitions” updated – added below definition as per DPDP act ▪ Child ▪ Consent ▪ Prescribed ▪ Profiling ▪ Regulations • Article 1 Section 1.6 “Amendments to HMSI Privacy Policy” updated – Added policy frequency review as yearly • Article 2 Added Section 2.1 “Data Protection Officer” • Article 2 Updated Section 2.2 Update Chief Information Security Officer → Data Protection Officer • Article 3 Added Section 3.1 “Personal Data Inventory” • Article 5 Section 5.5 “Grievance” ▪ Update Grievance Officer or Data Protection Officer à Grievance Officer ▪ Updated HMSI Head Office address ▪ Updated Grievance Reporting and Response Process for incorporating DPO & CISO position in place of OH	10 May, 2024

Kandla Joshi
Mohit Bhola
Goji Sugita
Vimal Bansal

Policy Version	Revision Date	Nature of Change	Date Approved/ Applicability
3.0	20 Jan, 26	• Replace Article with Chapter • Updated Confidentiality → Data Governance • Section 1.3 Scope - Language updated • Section 1.4 Update definitions of Data Principal and Added below definitions: ▪ PII Controller ▪ Consent Manager ▪ Damage • Section 1.6 Amendment to Policy - Added Chief Compliance Office approval reference • Section 2.2 Chief Privacy Officer - Point No. 3, 5, 6 added • Section 3.1 Personal Data Secrecy added • Section 3.2 Personal Data Inventory - Reference of RoPA added • Section 3.3 Title renamed as "Data Protection Impact Assessment" and Language updated • Section 3.5 Training - Remove reference of training that business partner holds in contract • Section 3.8 Outsourced Management of PII to Business Partner - Point No. 6 added • Section 4.1 Collection - Point No. 3 updated & Point No. 5, 6 added • Section 4.2 Notification - Point No. 7 added and Merge amendment as sub-section 4.2.1 • Section 4.3 Consent - Point No. 11 added • Section 4.4 Processing of personal Data/ Information - Point No. 3 - 9 added • Section 4.6 Transfer of Personal Information - Point 2 & 3 Added • Section 5.1 Obligation of Data Principal Added • Section 5.3 Correction - Point No. 2 Updated • Section 5.4 Rights of Withdraw Consent added • Section 5.5 Retention or Erase or Deletion or Suspension of Use - Point No. 5 added • Section 5.7 Grievance Officer mail id updated • Section 6.4 Penalties, Compensation and Offences Added • Annexure B Merge amendment	01 Feb,26

Kandla Joshi
24e4f809-05bd-457e-85c7-448fc1399ac6
Mohit Bhola
881092a3-b31b-4763-8a45-7774664466535
Goji Sugita
9e9700017-0bfc-41dd-87b0-5c6065924d90
Vimal Bansal
3f8acc3b-cd12-4dbc-a348-b23cc84e47d6