Corporate Privacy Policy (Global)

Master List Ref	Release Date	Review Date	Next Review Date
PL-ISMS-ENT-012	January, 2013	January, 2025	January, 2026
Version: 2.1	**Process Owner** IRM	**Reviewed by** Associate Director - IRM	**Approved by** SVP - IRM

Content

1. Introduction

Firstsource Solutions Limited ("FSL","us", "we") is a business process management company providing services in the banking and financial services, customer services, telecom and media, and healthcare sectors.

FSL is committed to ensuring that personal data is collected and processed fairly, lawfully and in a transparent manner as per the requirements of applicable privacy legislations.

Personal data is any information (including opinions and intentions) which relates to an identified or identifiable natural person.

This Privacy Policy (hereinafter referred to as "Policy") sets forth the general principles which underlie FSL's specific practices for collecting, using, disclosing, storing, retaining, disposing, accessing, transferring, or otherwise processing personal data.

2. Purpose

This Policy sets forth the expected behaviors of FSL personnel and third parties in relation to the collection, use, disclosure, storage, retention, disposal, access, transfer, and any other processing of personal data.

FSL's leadership is fully committed to ensuring continued and effective implementation of this Policy and expects all FSL employees and third parties to share in this commitment. Any breach of this Policy will be taken seriously and may result in disciplinary action.

3. Scope

This Policy covers the processing of personal data of employees (including current and past employees, full time, and part time employees, on contract personnel, consultants, interns, and other such individuals), clients, suppliers, business partners and other identifiable individuals by an FSL entity on behalf of FSL entity, as applicable.

Where FSL processes personal data on behalf of its clients, FSL shall follow appropriate policies and practices agreed with its clients for the safe handling of personal data.

This Policy is applicable to all employees of FSL, subsidiaries and joint ventures where FSL has a controlling interest, as well as business partners who process personal data on FSL's behalf.

This Policy covers processing of personal data in electronic form (including but not limited to electronic mail and documents created with word processing software) or where it is held in manual files that are structured in a way that allows ready access to information about individuals.

Any processing of personal by a FSL entity will be governed by the applicable privacy regulation/s. If certain regions have specific regulatory requirements, those requirements will take precedence over this Policy.[1]

In case of conflict between this Policy and the Data Protection Policy and Procedure, the stricter of the two shall prevail.

(Please refer Appendix 1– Data protection legislations considered). Country and industry-specific laws and regulations shall take precedence over this Policy.

4. Definition of Key Terms

Below is a brief description of key terms that regularly come into play with Data Protection:

Term	Definition
Anonymization/Dissociation	Data amended in such a way that no individual can be identified from the data (whether directly or indirectly) by any means. As per Mexico's Federal Data Privacy Law (FDPL), dissociation is the procedure by which personal data cannot be associated with the owner or allow, due to its structure, content or degree of disaggregation, its identification
Biometric Data	Personal Data resulting from specific technical processing relating to the physical, physiological,

[1] The documents pertaining to specific requirements in the USA are referenced in Appendix 5.

Term	Definition
	or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.
Blocking[2]	The identification and conservation of personal data once the purpose for which they were collected has been fulfilled, with the sole purpose of determining possible responsibilities in relation to their treatment, until the legal or contractual prescription period of these. During said period, personal data may not be processed and after this, it will be cancelled in the corresponding database.
Consent	Any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. As per Mexico's FDPL, expression of the will of the data owner by which data processing is enabled. Further, tacit/implied consent is valid for processing personal data.
Database[3]	The ordered set of personal data referring to an identified or identifiable person.

[2] Definition of blocking as per Mexico's Federal data privacy law
[3] Definition of database as per Mexico's Federal data privacy law

Term	Definition
Data Controller/Personal Information Controller/Entity Responsible/Data Fiduciary[4]	This means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any Personal Data are or are to be processed. As per the United Kingdom's Data Protection Act, 2012 (DPA), any person on whom the obligation to process personal data is imposed by an enactment, for purposes and by means required by the enactment will also be considered as a data controller. As per Mexico's FDPL, person responsible means physical or legal person of a private nature who decides on the processing of personal data. As per Philippines DPA, 2012, Personal information controller refers to a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf. As per Digital Personal Data Protection Act 2023, a data fiduciary means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.
Data Processing Agreement	A legally binding contract that states the rights and obligations of each party concerning the protection of personal data.
Data Processor/ Personal Information Processor/ Processor[5]	In relation to personal data, means any person who processes the data on behalf of the data controller. For clients, Firstsource is a data processor, and we will only process data under

[4] For maintaining consistency, the term Controller is used in place of the above terms in this Policy.
[5] For maintaining consistency, the term Processor is used in place of the above terms in this Policy

Term	Definition
	the instruction of the client who will be the data controller. As per Philippines' DPA 2012, Personal information processor refers to any natural or juridical person qualified to act as such under this Act to whom a personal information controller may outsource the processing of personal data pertaining to a data subject.
Data Protection	The process of safeguarding personal data from unauthorized or unlawful disclosure, access, alteration, processing, transfer, or destruction.
Data Protection Authority	An independent public authority responsible for monitoring the application of the relevant data protection regulation set forth in national law.
Data Subject/Individual /Data Owner/Data Principal[6]	A natural person (living) individual whose Personal Data is processed by a data controller or processor. As per Digital Personal Data Protection Act 2023, Data Principal means the individual to whom the personal data relates and where such individual is— (i) a child, includes the parents or lawful guardian of such a child; (ii) a person with disability, includes her lawful guardian, acting on her behalf.
Encryption	The process of converting information or data into code, to prevent unauthorized access.
Non-Adequate Country	Non-Adequate Country means a country that under the applicable law is deemed not to provide an "adequate" level of data protection.
Personal Data/ Personal Information[7]	Any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be

[6] For maintaining consistency, the term data subject is used in place of the above terms in this Policy.
[7] For maintaining consistency, the term personal data is used in place of the above terms in this Policy

Term	Definition
	identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed.
Privileged Information[8]	Privileged information refers to any and all forms of data which under the Rules of Court and other pertinent laws constitute privileged communication.
Process/Treatment, Processed, Processing	The term "Processing of Personal Data" refers to any operation or set of operations which is performed on Personal Data or on sets of personal data, whether or not by automated means, such as the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction. As per Mexico's FDPL, treatment means obtaining, using, disclosing, or storing personal data, by any means. The use covers any action of access, management, use, transfer, or disposal of personal data.
Profiling	Any form of automated processing of personal data where personal data is used to evaluate

[8] Definition of privileged information as per Philippines' Data privacy Act, 2012.

Term	Definition
	specific or general characteristics relating to an identifiable natural person to analyze or predict certain aspects concerning the natural person's performance at work, economic situations, health, personal preferences, interests, reliability, behavior, location, or movement.
Pseudonymization	Data amended in such a way that no individual can be identified from the data (whether directly or indirectly) without a "key" that allows the data to be re-identified.
Special Categories of Personal Data / Sensitive Personal Data[9]	Personal Data revealing a Data Subjects racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership or the processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. As per Philippines' Data Privacy Act, 2012, apart from the above, the following data sets also fall within the definition of sensitive data: 1. Age 2. Color 3. Education 4. Committed or alleged offence, and any proceedings related to it 5. Documents issued by government agencies such as Social Security Number, Tax Identification number etc. 6. Specifically established by an executive order or an act of Congress to be kept classified

[9] For maintaining consistency, the term sensitive data is used in place of the above terms in this Policy.

Term	Definition
Standard Contractual Clauses (SCCs)	Standard contractual clauses (SCCs) are standardized and pre-approved model data protection clauses that serve as a tool for entities to comply with the requirements of the EU GDPR for transferring personal data to countries outside of the EEA (to non-adequate countries).
International Data transfer Agreement (IDTA)/IDTA Addendum	IDTA are standardized and pre-approved model data protection clauses that serve as a tool for entities to comply with the requirements of the UK GDPR for transferring personal data to countries outside of the UK (to non-adequate countries).

5. Objectives

The objectives of this Policy are to:

- Ensure that processing of personal and sensitive personal data by or on behalf of FSL complies with the data protection principles and follows the lawful basis for processing, as per the applicable data protection laws.
- Make all the stakeholders aware about the processes that need to be followed for collection, usage, disclosure/transfer, retention, archival and disposal of personal data.

6. Governance

Leadership of FSL is committed to ensuring and upholding data privacy principles as well as compliance requirements of applicable data privacy laws.

To demonstrate commitment to data protection, and to enhance the effectiveness of compliance efforts, FSL shall establish a Data Privacy Team (DPT). The DPT shall operate with independence and shall be headed by the Data Protection Officer (DPO). The DPO shall be a suitably skilled individual who has been granted all necessary authority. The DPO shall report to FSL's senior leadership.

7. Policy statements

7.1 Data protection principles

FSL's processing of personal data shall be governed by the following principles:

- **Principle 1: Lawfulness, Fairness and Transparency:**

  Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. This means, FSL shall inform the data subject what processing will occur (transparency), the processing shall match the description given to the data subject (fairness), and it shall be as per the permitted lawful bases specified in the applicable data protection regulation (lawfulness).

- **Principle 2: Purpose Limitation:**

  Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means FSL shall specify exactly what the personal data collected will be used for and limit the processing of that personal data to only what is necessary to meet the specified purpose.

- **Principle 3: Data Minimization:**

  Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. This means FSL shall not collect or otherwise process any personal data which is beyond the specified purposes.

- **Principle 4: Accuracy:**

  Personal data shall be accurate and, kept up to date to the extent practically possible.

- **Principle 5: Storage Limitation:**

  Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed (subject to regulatory requirements). This means FSL shall, wherever possible, store personal data in a way that limits or prevents identification of the data subject when no longer required for the processing purpose.

- **Principle 6: Integrity & Confidentiality:**

  Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing, and against accidental loss, destruction, or damage. This means that FSL shall use appropriate technical and organizational measures to ensure the integrity and confidentiality of personal data is maintained throughout the data processing lifecycle.

- **Principle 7: Accountability:**

The data controller shall be responsible for and be able to demonstrate compliance. This means FSL shall demonstrate that the six data protection principles (outlined above) are met for all personal data for which it is responsible.

7.2 Data Collection

Data Sources

Personal data shall be collected only from the data subject unless one of the following apply:

- The nature of the business purpose necessitates collection of the personal data from other persons or bodies.
- The collection is required to be carried out under emergency circumstances to protect the vital interests of the data subject or to prevent serious loss or injury to another person.

7.2.1 Consent

FSL shall obtain personal data only by lawful and fair means and, where appropriate with the knowledge and consent of the individual concerned. Where a need exists to request and receive the consent of an individual prior to the collection, use or disclosure of their personal data, FSL shall seek such consent.

The data subjects shall be given option to withdraw or revoke their consent by writing to the Data Protection Officer (DPO) at dataprivacy@firstsource.com. The data subject shall be duly informed of their right to revoke or withdraw consent.

7.2.1.1 Geography-specific requirements for consent

I. Mexico

FSL shall ensure the following while obtaining consent for processing personal data of data subjects of Mexico: -

- As per Mexico's Federal Data Privacy Law (FDPL), consent is the only lawful basis for processing personal data of data subjects of Mexico.
- For processing sensitive or financial personal data, FSL shall obtain explicit consent from data subjects such as employees, vendors, clients, prospects and any such other category of data subjects in Mexico before processing such data.

- For transferring personal data outside the borders of Mexico, explicit consent shall be obtained.

For processing personal data (excluding sensitive/financial personal data), providing a privacy notice with information regarding data processing suffices the requirement for tacit consent (which is required for processing non-sensitive data), provided that the privacy notice is not opposed by the data subject.

II. Philippines

FSL shall ensure the following while obtaining consent for processing personal data of data subjects of Philippines: -

- Provide provision to allow agent (specifically authorized) to give consent on behalf of the data subject
- For processing privileged information and/or sensitive data of data subjects of Philippines, consent shall be obtained, prior to processing such data.
- For transferring personal data outside the borders of Philippines, explicit consent shall be obtained.

III. Australia

Australian Privacy Principles (APP) –
There are 13 Australian Privacy Principles and they govern standards, rights and obligations around:

- the collection, use and disclosure of personal information
- an organisation or agency's governance and accountability
- integrity and correction of personal information
- the rights of individuals to access their personal information.

The 13 Australia Privacy Principles are

1) Open and Transparent management of Personal Information
2) Anonymity and Pseudonymity
3) Collection of solicited personal information
4) Dealing with unsolicited personal information
5) Notification of the collection of personal information
6) Use or disclosure of personal information
7) Direct Marketing
8) Cross-border disclosure of personal information
9) Adoption, use or disclosure of government related identifiers

10) Quality of Personal Information
11) Security of personal information
12) Access to personal information
13) Correction of personal information

When processing data outside of Australia, businesses must adhere to the Australian Privacy Principles (APPs) which mandate taking "reasonable steps" to ensure that overseas recipients of personal information do not breach these principles, meaning they must protect the data to the same standard as if it were processed within Australia; essentially making the organization accountable for how the data is handled even when it is transferred overseas.

APP-8 - Cross-border disclosure of personal information

The Privacy Act permits international transfers of personal information without further requirements where the country of the recipient has a law or binding rules that has the effect of protecting the personal information in a way that, overall, is at least substantially similar to the way in which the APPs protect the information; and there are mechanisms under which the data subject can take action to enforce the protection of the law or binding rules.

Firstsource to ensure the following are adhered:

a) APP entity to ensure that an overseas recipient will handle an individual's personal information in accordance with the APPs, and makes the APP entity accountable if the overseas recipient mishandles the information.
b) Before an APP entity discloses personal information about an individual to an overseas recipient, the entity must take reasonable steps to ensure that the recipient does not breach the APPs in relation to that information. Where an entity discloses personal information to an overseas recipient, it is accountable for an act or practice of the overseas recipient that would breach the APPs
c) When an APP entity discloses personal information to an overseas recipient it will also need to comply with APP 6. That is, it must only disclose the personal information for the primary purpose for which it was collected unless an exception to that principle applies.

7.2.2 Notice

FSL shall, where required by applicable law, contract, or where it considers that it is reasonably appropriate to do so, provide data subjects with information as to the purpose of the processing of their personal data and other relevant processing details.

- FSL shall provide a privacy notice to data subjects in the following manner: -

a. To employees - at the time of onboarding or along with employment agreement
b. To candidates - at the time of collecting their CV (Curriculum Vitae), Resume, cover letter and other such documents containing personal data.
c. To customers - at the time of entering stakeholder details in CRM
d. To service providers - at the time of onboarding the vendors
e. Visitors to office premises - at the time they provide their details for visitors' log
f. Marketing prospects - at the time of collection of data (for both offline and online)

- FSL shall also provide a privacy notice to the data subjects in case any new purpose is identified for processing personal data before such information is used for new purposes.
- FSL's website shall include a 'Privacy Policy' and 'Cookie Policy' which shall inform the website's visitors about the processing of their personal data in relation to their activities while accessing the website. Additionally, the website shall obtain visitors' consent on the deployment of cookies as applicable.

7.2.3 Geography-specific requirements for notice

I. India

FSL shall provide the data subjects the option to request privacy notice specified in any of the languages specified in the eighth schedule of the Constitution of India.

7.3 Data use

7.3.1 Data processing

FSL shall process personal data when at least one of the following requirements are met:

- The data subject has given consent to the processing of his or her personal data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering a contract.
- Processing is necessary for compliance with a legal obligation to which the data controller is subject.
- Processing is necessary to protect the vital interests of the data subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller.

- Processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject).
- Processing personal data, but not sensitive personal data is necessary for employment purposes.

If the purposes of processing personal data change over time or data is to be used for a new purpose which was not originally anticipated, the processing shall only be performed if:

- The new purpose is compatible with the original purpose; or
- FSL obtains the data subject's specific consent for the new purpose.
- In order to determine whether a new purpose is compatible with the original purpose, FSL shall obtain guidance and approval from the DPO and take into account:
- Any link between the purpose for which the personal data was collected and the reasons for intended further processing.
- The context in which the personal data has been collected, in particular regarding the relationship between data subject and the data controller/ data processor.
- The nature of the personal data, in particular whether sensitive personal data are being processed.
- The possible consequences of the intended further processing for the data subject.
- The existence of appropriate safeguards pertaining to further processing, which may include measures such as encryption, anonymization or pseudonymization.

7.3.2 Sensitive personal data

FSL shall avoid the processing of sensitive personal data where it is not required for the purposes for which the data is collected (or subsequently processed). Where sensitive personal data is required to be processed, FSL shall limit access to appropriate persons.

7.3.2.3 Geography-specific requirements for processing sensitive data

I. Mexico

As per FDPL, for processing sensitive and financial data, FSL shall obtain explicit consent of the data subjects and record the same.

II. Philippines

As per DPA, for processing sensitive data, FSL shall obtain explicit consent of the data subjects.

7.3.3 Data retention

- Personal data shall not be retained by FSL for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further processed.
- The length of time for which personal data is to be retained shall be determined by considering the applicable legal and contractual requirements, both minimum and maximum, that influence the retention periods.

7.3.4 Data disposal

- Personal data shall be deleted, destroyed, or anonymized as soon as it has been confirmed that there is no longer a need to retain it or if it is in violation of any of the data protection principles.
- Personal data disposal shall follow FSL's data disposal process to ensure the safe disposal of personal data and avoid unauthorized retrieval.

7.3.5 Direct marketing

FSL shall not send promotional or direct marketing material to a data subject (for example, through digital channels such as email and the Internet or conventional channels including but not limited to fax, email, SMS, and MMS) without first obtaining their consent.

The data subject shall be informed at the point of first contact that they have the right to withdraw consent, at any stage, from having their data processed for marketing purposes. If the data subject withdraws consent to processing of their personal data, the minimum required details to identify the data subject shall be kept on a suppression list with a record of their opt-out decision, rather than being completely deleted.

Further, FSL shall not disguise or conceal its identity in any direct marketing communication and shall provide the contact details of the DPO so that the data subject may send a request to opt-out or unsubscribe from such communication.

7.4 Record maintenance

For the purpose of demonstrating accountability, appropriate records related to processing personal data shall be maintained, including but not limited to the following:-

- Record of processing activities (RoPAs) shall be maintained and shall be reviewed and updated on a periodic basis.
- Inventory of personal data shall be reviewed and updated on a regular basis.
- Data Flow Diagram (DFD) shall be reviewed and updated on a regular basis.

- Data breach record shall be maintained for all the data privacy breaches as well as incidents.
- Data Protection Impact Assessment (DPIA) shall be carried out on a periodic basis for applicable processes/applications to ensure risks to personal data are identified and managed.
- Legitimate Interest Assessment (LIA) shall be carried out on a periodic basis for processes where legitimate interest is relied upon as a lawful basis of processing.
- Consent request and withdrawal forms shall be maintained to ensure and demonstrate that data subject has consented to or opted-out of processing their personal data.
- Data subject rights management templates shall be maintained for all data subject requests received by FSL.
- Privacy by Design (PbD) assessments shall be maintained for FSL's applications and processes processing personal data.
- Privacy audits' results and mitigation plan to ensure that the privacy related requirements are reviewed on a regular basis.

7.5 Data security

FSL shall ensure robust safeguards are in place to protect personal data by ensuring the following to protect personal data:-

- Ensure that the data resides behind firewall with access restricted to authorized personnel.
- Prevent persons entitled to use data processing systems from accessing personal data beyond their needs and authorization.
- Ensure that in the case where processing is carried out by another entity on our behalf, the data is processed only in accordance with the data processing addendums and the agreed contractual obligations.
- Ensure confidential waste bins are made available to all areas processing sensitive data.
- Ensure applicable controls as per standards -ISMS, PCI DSS and HITRUST are reviewed on a regular basis.
- Ensure that there is a defined password policy which is enforced at an organizational level.
- Ensure data security and privacy trainings as well as refresher trainings for employees are conducted on a regular basis.
- Ensure role-based access control are provided to application and supporting infrastructure.

- Ensure users' logical access and physical access are deactivated in a timely manner post-termination.
- Ensure user access reconciliation is performed and corrective action is taken in case of any discrepancies.
- Ensure security patches and antivirus are updated on a periodic basis.

7.5.1 Privacy by design (PbD)

FSL shall apply Privacy by Design principles by applying strong privacy practices early and consistently to projects and business processes which involve personal data processing. The obligation to enforce privacy by default shall apply to the types of personal data collected, the extent of processing, the period of storage and the accessibility of the personal data.

7.6 Data protection impact assessment

Each business function of FSL shall ensure that where required as per the applicable privacy regulation, a Data Protection Impact Assessment (DPIA) is conducted, in consultation with the DPO, for any new and/or revised systems or processes for which it has responsibility. The subsequent findings of the DPIA shall then be submitted to the DPO for review and approval.

7.7 Legitimate Interest Assessment

Each business function of FSL shall ensure that where required as per the applicable privacy regulation, a Legitimate Interest Assessment (LIA) is conducted, in consultation with the DPO, for any existing or new and/or revised systems or processes where legitimate interest is relied upon as lawful basis for processing.

7.8 Data subject rights requests

FSL shall establish a process to enable and facilitate the data subject rights related to:-

- Right of Access: The data subject can request access to and request a copy of their personal data being processed by FSL.
- Right to Rectification: The data subject can request rectification of inaccurate personal data, or to have incomplete personal data completed.
- Right to be Forgotten / Right to Erasure: The right to be forgotten / right to erasure entitles the data subject to request the erasure of their personal data.

- Right to Object to Processing: The data subject can object (i.e., exercise their right to "opt-out") to the processing of their personal data particularly in relation to profiling or to marketing communications.
- Right to Restriction of Processing: The data subject can request this right where certain conditions apply to have a right to restrict the processing.
- Right of Portability: The data subject can request this right if they want the data, we hold about them to be transferred to another organisation.
- Right to Object to Automated Processing, including profiling: The data subject can request this right to object to subject to the legal effects of automated processing or profiling.
- Right to judicial review/complain: The data subject can request this right if FSL refuses their request under rights of access, a reason for refusal shall be communicated to the data subjects.

On receiving a request when a data subject exercises any of his or her rights, FSL shall respond to the requests within stipulated timelines as per the applicable data protection laws.

7.9 Data protection training

All FSL employees that have access to personal data shall have their responsibilities under this Policy outlined to them as part of their onboarding training. Additionally, FSL shall conduct refresher data protection training annually.

7.10 Cross-border Data Transfer

In order for FSL to carry out its operations effectively, there may be occasions when it is necessary to transfer personal data from one FSL entity to another or to share personal data with service providers that are located overseas, or to allow access to the personal data from an overseas location. Should this occur, the FSL entity sending / allowing access to the personal data shall remain responsible for ensuring protection for that personal data.

FSL shall handle the transfer of personal data between FSL entities, where the location of the recipient entity is a non-adequate country as per safeguards mentioned in applicable laws (such as obtaining consent, SCC, IDTA etc.). FSL shall transfer only the minimum required personal data and ensure adequate security measures for protection of personal data during the transfer.

7.11 Transfers to third parties

FSL shall only transfer personal data to or allow access by third parties through a Data

Processing Agreement (DPA), when it is assured that the information will be processed legitimately and protected appropriately by the recipient. These agreements shall clarify each party's responsibilities in respect to the personal data transferred. The third party shall establish procedures to meet the terms of their agreement with relevant FSL entity/subsidiary to protect personal data and demonstrate compliance with the data transfer requirements as per applicable data protection laws.

Personal data shall be disclosed to data processor (such as vendor and contractor) only for identified lawful purposes and after obtaining appropriate consent from the data subjects/ providing appropriate notice, as applicable, unless a law or regulation allows or requires otherwise. Where FSL is outsourcing services to a third party (including cloud computing services), FSL shall consider whether the outsourcing will entail any non-adequate country transfers of personal data.

7.12 Breach reporting

FSL shall establish robust personal data breach detection, investigation, and reporting procedures.

Any individual who suspects that a personal data breach has occurred due to the theft or exposure of personal data shall immediately notify the DPO providing a description of the breach.

FSL shall investigate all reported incidents to confirm whether a personal data breach has occurred. If a personal data breach is confirmed, FSL shall take necessary steps to minimize the risks to the rights of the data subjects. FSL shall keep a record of all breaches.

8. Changes to this Policy

We may amend this document from time to time. Please refer to the document on a regular basis.

9. Contact Us

In case of any questions or concerns about this Privacy Policy, or your dealings with the personal data, you can contact dataprivacy@firstsource.com for clarifications.

10. Appendices

10.1 Appendix 1 – Data protection legislation considered

Below is the list of data protection laws that have been taken into consideration in developing this Policy:

1. United Kingdom's Data Protection Act (DPA), 2018
2. United Kingdom's General Data Protection Regulation (GDPR), 2022
3. Mexico's Federal Law on Protection of Personal Data Held by Private Parties (FDPL), 2010
4. Philippines' Data Privacy Act (DPA) 2012
5. India's Digital Personal Data Protection Act, 2023

10.2 Appendix 2- Data Protection Authorities

Country	Data Protection Authority	Address
United Kingdom	Information Commissioner Office (ICO)	Information Commissioner's Office Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
Mexico	National Institute of Transparency for Access to Information and Personal Data Protection (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales) (INAI)	Insurgentes Sur 3211 Colonia Insurgentes Copilco, Coyoacán, Ciudad de México'
Philippines	National Privacy Commission (NPC)	5th Floor Delegation Building, PICC Complex, Vicente Sotto Avenue, Pasay City, Metro Manila 1307, or email us at dpo@privacy.gov.ph.

10.3 Appendix-3 - Exemption

As per Digital Personal Data Protection Act, 2023, this policy shall not apply to the following:

a. Processing of personal data of data principals outside India pursuant to any contract entered into with a foreign party

b. Necessary for a scheme of compromise or arrangement or merger or amalgamation of two or more companies

10.4 Appendix 4 – Associated documents

This Policy shall be read in conjunction with the following:-

- Privacy governance framework
- Data protection officer - Roles and responsibilities
- Privacy by design guidelines
- Data retention and disposal guidelines
- Personal data breach management procedure
- Data protection impact assessment guidelines and selection criteria templates
- Legitimate interest assessment guidelines
- Consent Management Guideline
- Cookie Policy
- Website Privacy Policy

10.5 Appendix 5 – USA specific documents

- Firstsource HIPAA Framework Policy v.10
- Firstsource HIPAA Awareness Policy Manual v.17
- Firstsource Healthcare Safeguarding Information Against Identity Theft v.6
- Firstsource Healthcare Record Retention Policy v.1
- Firstsource Group USA, Inc. CCPA Privacy Notice

Annexure A

Information Classification Details

Classification: Firstsource Restricted
Information Owner (IO): Head - Technology
Information Custodian (IC): IRM team
Authorization List (AL): All Employees, 3rd Parties, Existing/Prospective Clients,
Declassify on: Never

Annexure B

Changes since the Last Version (Version)

Date	Version Number	Changes made
24th Jan, 2013	v1.0 to v1.1	1. Section 6 (Reporting Privacy Breach) updated to include additional CSD contact number & e-mail address.
28th Jan, 2014	v1.1 to v1.2	1. Included UK Data Protection Act explicitly under section 2 (Firstsource Data Privacy Framework).
January 4, 2016	v1.2 to v1.3	1. Replaced InfoSec team with IRM team.
January 25, 2017	v1.3 to v1.4	1. Updated the new CSD number in section 6 (Reporting Privacy breach)
January 05, 2024	v1.4 to v2.0	1. Refreshed the data privacy policy to reflect the changed framework
January 20, 2025	V2.0 to v2.1	Added Australian Data Privacy Law under Geography specific requirements