**A. Employee Training & Data Privacy Risk Culture**

**Description:** Information on the organization's initiatives for training employees on data privacy and fostering a culture of awareness.

**KeyPoints:**

1. **Significance of employee awareness in preventing data breaches. - Regular training programs for employees.**

* Why is it important?

Human error is the leading cause of data breaches.

Employees are the first line of defense against cyber threats.

Raising awareness helps mitigate risks from insider threats.

* How to do it?

Conduct regular cybersecurity training programs.

Equip employees with knowledge on phishing, passwords, safe browsing, etc.

Emphasize best practices for data protection.

Keep up-to-date with the latest threats.

* Benefits:

Reduces the risk of data breaches.

Creates a stronger cybersecurity environment.

1. **Resources for staying informed about data protection.**

Government Agencies Websites: For example: in the United States, the Federal Trade Commission (FTC) and the Cybersecurity and Infrastructure Security Agency (CISA) offer guidance and tools for businesses and individuals.

Industry Associations: Examples include the International Association of Privacy Professionals (IAPP) for privacy professionals, the Information Systems Security Association (ISSA), and the Cloud Security Alliance (CSA).

Cybersecurity Blogs and Websites: Numerous blogs and websites specialize in cybersecurity news, trends, and analysis. Examples include Krebs on Security, The Hacker News, Dark Reading, and SecurityWeek.

Online Courses and Webinars: Platforms like Coursera, Udemy, and LinkedIn Learning offer online courses and webinars on data protection, cybersecurity, and compliance topics.

Professional Conferences and Events: Attending cybersecurity conferences, workshops, and webinars can provide valuable insights into the latest trends and best practices. Events like RSA Conference, Black Hat, and DEF CON offer opportunities to learn from industry experts and network with peers.

1. **Reporting mechanisms for potential data privacy issues.**

Internal Department or Data Management: Organizations can establish an internal department or specialized team where employees can report issues related to data privacy through internal email or online reporting systems.

Internal Reporting System: Internal reporting systems such as internal email, electronic forms, or online applications are deployed by organizations to allow employees to report issues discreetly and securely.

Direct Contact with Management: Employees can directly contact their managers or senior staff if they encounter issues related to data privacy, either through one-on-one meetings or email communication.

External Reporting Systems or Services: Integrated external reporting systems or services allow employees to report issues anonymously or non-anonymously.

Regulatory Agencies and Legal Channels: If the issue cannot be resolved internally, employees may contact relevant regulatory agencies or legal entities such as privacy protection agencies or trade commissions.

Anonymous Reporting System: Organizations provide anonymous reporting systems where employees can report issues without revealing their identities.

**FAQs:**

1. **How often are employees trained on data privacy?**

HSBC have not trained for employees on data privacy, currently we are researching about data privacy and in the next time we will train for my employees early.

1. **What resources are available for staying informed?**

**There are many resources available to stay updated on data privacy in Vietnam:**

**Official sources:**

* **Ministry of Information and Communications**
* **Portal of the Ministry of Information and Communications**
* **Legal documents on personal data security**

**Unofficial sources:**

* **Vietnam Information Security Association (VNISA)**
* **National Cyber Security Monitoring Center** (NCSC)

1. **How can employees report data privacy issues?**

* Internal Department or Data Management
* Direct Contact with Management
* External Reporting Systems or Services

1. **What role do employees play in preventing breaches?**

Banks play a critical role in a nation's economy. HSBC is a multinational bank, therefore HSBC's data must be strictly protected. Employees play a very important role in preventing data breaches within an organization. They act as the first line of defense against various cyber threats and can significantly reduce the risk of successful attacks through their actions and awareness.

Overall, a well-informed and vigilant workforce is critical for an organization's data security posture. By actively participating in these preventative measures, employees can significantly contribute to reducing the risk of data breaches and protecting sensitive information.

1. **Are there consequences for policy violations?**

There are consequences for policy violations. The severity of the consequences depends on:

* The severity of the violation
* The frequency of the violation
* The organization's policies

General consequences:

* Verbal warnings
* Written warnings
* Suspension
* Termination

Specific consequences:

* Depend on the policy violated

Factors that influence:

* Previous disciplinary record
* Employee's intent
* Impact of the violation

**B. Data Subject Rights**

**Description:** Explanation of the rights that individuals have regarding their personal data, including access, correction, deletion, and data portability.

**KeyPoints:**

1. **Overview of data subject rights.**

Based on Decree [13/2023/ND-CP](https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Nghi-dinh-13-2023-ND-CP-bao-ve-du-lieu-ca-nhan-465185.aspx), the rights of data subjects in Vietnam:

1. Right to be Informed

Data subjects have the right to be informed about the processing of their personal data, unless otherwise provided by law.

2. Right to Consent

Data subjects have the right to consent to or refuse the processing of their personal data, except as provided in Article 17 of this Decree.

3. Right to Access

Data subjects have the right to access, review, or request the correction of their personal data, unless otherwise provided by law.

4. Right to Withdraw Consent

Data subjects have the right to withdraw their consent, except as otherwise provided by law.

5. Right to Erasure of Data

Data subjects have the right to be erased or to request the erasure of their personal data, except as otherwise provided by law.

6. Right to Restriction of Data Processing

a) Data subjects may request the restriction of the processing of their personal data, except as otherwise provided by law;

b) Restriction of data processing shall be carried out within 72 hours after the data subject's request, for all personal data requested to be restricted by the data subject, except as otherwise provided by law.

7. Right to Data Portability

Data subjects may request that the Data Controller, the Controller, and the processor provide them with their own personal data, except as otherwise provided by law.

8. Right to Object to Data Processing

a) Data subjects have the right to object to the Data Controller, the Controller, and the processor processing their personal data to prevent or restrict the disclosure of personal data or use for advertising or marketing purposes, except as otherwise provided by law;

b) The Data Controller, the Controller, and the processor shall comply with the data subject's request within 72 hours after receiving the request, except as otherwise provided by law.

9. Right to Complaint, Denunciation, Lawsuit

Data subjects have the right to complaint, denunciation, or lawsuit according to the law.

10. Right to Compensation for Damage

Data subjects have the right to demand compensation for damages as provided by law in case of violation of the provisions on protection of their personal data, except as otherwise agreed by the parties or provided by law.

11. Right to Self-Protection

Data subjects have the right to self-protection as provided by the Civil Code, other relevant laws, and this Decree, or to request competent authorities or organizations to implement civil rights protection measures as provided in Article 11 of the Civil Code.

1. **Process for requesting access and correction.**

1. Preparation:

Identify the organization that holds your personal data.

Determine the information you want to access or edit.

Prepare the required documents:

ID card/Citizen identification card or passport

Request for access/edit of personal data (downloadable from the organization's website or handwritten)

2. Submitting the request:

Methods:

* In person at the organization's headquarters
* By mail
* By email
* Through the organization's electronic portal (if available)

Content of the request:

* Reason for requesting access/edit
* Specific information about the data you want to access/edit
* Desired format of the data (if applicable)
* Your contact information

3. Verification:

The organization may require you to provide additional information to verify your identity and access rights.

4. Processing time:

The organization has 72 working hours from received your request and respond to your request.

5. Receiving the results:

Access:

The organization will provide you with a copy of your personal data.

Format: paper, electronic file, or other suitable form.

Editing:

The organization will edit your personal data according to your request.

The organization may require you to provide additional information to verify the accuracy of the data.

6. Complaint:

If you are not satisfied with the organization's handling of your request, you can file a complaint with the state management agency for personal data protection.

1. **Handling requests for data deletion.**

5 Cases Where Data Subjects Can Request Personal Data Deletion

According to Clause 1, Article 16 of Decree 13/2023/ND-CP, data subjects can request the Data Controller and Data Processor to delete their personal data in the following cases:

(1) They deem it no longer necessary for the purpose of collection and agree to accept the potential damages that may occur when requesting data deletion.

(2) They withdraw their consent.

(3) They object to the data processing and the Data Controller and Data Processor do not have legitimate grounds to continue processing.

(4) The personal data is processed for purposes other than those for which consent was given, or the processing of personal data violates legal regulations.

(5) The personal data must be deleted according to legal regulations.

Similar to data editing, data deletion is performed within 72 hours after receiving a request from the data subject, for all personal data collected by the Data Controller and Data Processor, unless otherwise provided by law.

1. **Ensuring data portability for data subjects.**

Article 3 of Decree [13/2023/ND-CP](https://datafiles.chinhphu.vn/cpp/files/vbpq/2023/4/13nd.signed.pdf) on principles of personal data protection:

Personal data collected must be appropriate and limited to the scope and purpose of the processing.

Personal data may not be bought or sold in any form, except as otherwise provided by law.

Article 22: Illegal collection, transfer, purchase, and sale of personal data:

The establishment of software systems, technical measures, or the organization of activities to collect, transfer, buy, or sell personal data without the consent of the data subject is a violation of the law.

Article 25: Transfer of personal data abroad:

Personal data of Vietnamese citizens may be transferred abroad in the following cases:

The Party transferring data abroad prepares a Personal Data Transfer Impact Assessment File and completes the procedures as prescribed in Clauses 3, 4, and 5 of this Article.

The Party transferring data abroad includes the Personal Data Controller, the Data Controller and Processor, the Data Processor, and the Third Party.

The Ministry of Public Security shall decide to request the Party transferring data abroad to stop transferring personal data abroad in the following cases:

When it is discovered that the transferred personal data is used for activities that violate the interests and national security of the Socialist Republic of Vietnam;

The Party transferring data abroad does not comply with the provisions of Clauses 5 and 6 of this Article;

An incident of disclosure or loss of personal data of Vietnamese citizens occurs.

**FAQs:**

1. **What rights do individuals have regarding their personal data?**

Some common rights:

* Right to access
* Right to rectification
* Right to erasure
* Restriction of processing
* Data portability
* Right to object
* Right to lodge a complaint

1. **How can individuals request access to their information?**

Request Process:

* Contacting the bank:

Individuals can directly contact the bank branch where they opened their account or through the customer service hotline.

Provide personal information to verify identity: ID card/CCCD, account number, contact information.

Fill out the personal information request form (according to the bank's form).

* Service fees:

Some banks may charge a fee for providing personal information.

1. **What is the process for correcting inaccurate data?**

The process for correcting inaccurate data in banks (Vietnam):

1. Identify inaccurate data:

* Review your account information, statements, and related documents.
* Determine which specific information is incorrect or incomplete.
* Gather supporting evidence such as ID cards, passports, or statements from relevant individuals.

2. Contact your bank:

* Find contact information through the bank's website, mobile app, or branch visits.
* Use various channels to contact them:
* Customer service hotline: Convenient and quick.
* Email: Send a detailed email with supporting documents attached.
* In-person visit: Discuss with a bank representative and provide necessary details.

3. Submit a formal request:

Use the data correction request form (if available) or write a written request.

Clearly specify in the request:

* Personal information: Full name, account number, and contact information.
* Data to be corrected: Clearly identify the specific information that needs correction.
* Reason for correction: Explain the reason and provide evidence.
* Desired correction: State the accurate information that needs to be replaced.

4. Follow up on the results:

* The bank may take several days or weeks to process the request.
* If you haven't received a response after 30 days, contact the bank again to inquire about the progress.

5. Appeal (optional):

* If your data correction request is denied, you have the right to appeal.
* Contact the bank's data protection officer or file a complaint with the State Bank of Vietnam (SBV).

Notes:

* Fees: Some banks may charge a small fee for data correction.
* Deadline: SBV requires banks to respond to data correction requests within 30 days.

1. **Can individuals request data deletion?**

The current legal framework in Vietnam regarding data deletion rights in the banking sector is still under development. While individuals do have certain rights to access, rectify, and restrict the processing of their personal data under Decree 13/NĐ-CP dated April 17, 2023 on personal data protection, the explicit right to request data deletion is not yet fully established in the context of banking institutions.

Limited right to deletion: Currently, Vietnamese law grants individuals the right to request "suspension of processing" and "erasure" of their personal data in specific situations. However, these situations are generally limited to:

* When the data is no longer necessary for the purpose for which it was collected
* When the individual withdraws their consent for processing
* When the data is processed illegally

Therefore, the right to data deletion in banks might not be as broad as in other sectors, and its application depends on the specific circumstances and the bank's internal policies.

Contact the bank: They might have internal procedures in place to address such requests, even if not explicitly mandated by law.

Express your request: Clearly explain your reasons for wanting your data deleted and provide any relevant details.

1. **How is data portability ensured?**

The current legal framework in Vietnam does not explicitly mention data portability in the context of banking institutions. While Decree 13/NĐ-CP dated April 17, 2023, on personal data protection outlines individual rights regarding personal data, data portability is not specifically addressed in this legislation.

Data access rights: Leverage existing data access rights under Decree 13/NĐ-CP to request your personal data from the bank. While not directly portable, you can receive the information in a structured format like a spreadsheet or CSV file, allowing for easier transfer to another service provider (if compatible).

Contacting the bank directly: It's worth contacting your bank directly to inquire about their policies and explore any potential options.