Australian
Chamber of
Commerce
Vietnam

AUSCHAM
VIETNAM

White Paper

Decree 13/2023/ND-CP on Personal Data Protection
An AusCham Members Guide

JANUARY 2024

AusCham Advocacy White Paper

INDEX

Hiệp Hội Doanh Nghiệp Úc tại Việt Nam

AUSCHAMVN.ORG

Ho Chi Minh City
3F, Sonatus Building
15 Le Thanh Ton, Ben Nghe Ward
District 1, HCMC, Vietnam
T: +84 (0) 28 7100 1909
E: office@auschamvn.org

Hanoi
6F, Spaces Belvedere
28A Tran Hung Dao
Hoan Kiem District, Ha Noi, Vietnam
T: +84 (0) 24 7101 4054
E: auschamhanoi@auschamvn.org

AUSCHAM VIETNAM

AusCham Advocacy White Paper

Decree 13/2023/ND-CP on Personal Data Protection
An AusCham Members Guide

Abstract

On 01 July 2023, Decree No. 13/2023/ND-CP (**Decree 13**), the first-ever Personal Data Protection Decree (**PDPD**) of Vietnam, officially took effect. This landmark legal instrument integrates all of Vietnam's disparate data protection legislation, with the potential to bring them closer to the EU's General Data Protection Regulation (**GDPR**) requirements and is expected to have a profound impact on both local and foreign-invested companies doing business in and with Vietnam. Thus, compliance with this new regulation is mandated for all entities in any kind onshore or offshore situation that proceed with Vietnamese individuals' information, including Members of AusCham Vietnam.

As the PDPD continues to be a magnet for public attention, AusCham is taking a closer look at its key provisions and some initial implications for AusCham Members as below.

General overview

The development of a decree on personal data protection was launched by the Government of Vietnam since 2019. After 04 years of various drafts, discussions and public comments, the final version of the Decree was officially approved and issued on 17 April 2023, which demonstrates the cautious approach of Vietnamese government in this regard.

Decree 13 took immediate effect on 01 July 2023 without any transition period. A grace period of 02 years is only applicable to micro enterprise, SME[1] and start-up[2], excluding business that directly engage in the business of personal data processing.

Decree 13 establishes a comprehensive framework for the collection, use, storage, and processing of personal data by outlining various principles and regulations that organizations and individuals must adhere to when handling personal data. For individuals, this Decree also details specific rights, such as the right to access, correct and delete their personal information, as well as the right to object to the processing of their data for certain purposes.

Overall, Decree 13 provides a legal framework for the responsible and ethical handling of personal data in Vietnam. It seeks to balance the needs of organizations to collect and use data for legitimate purposes with the rights and privacy of individuals.

[1] According to Article 4 of Law on Provision of Assistance for Small and Medium Enterprises, an SME is either a micro-enterprise, small enterprise or medium-sized enterprise having the annual average number of employees who participate in social insurance is not greater than 200 and satisfying one of the following criteria:

a) The total capital is not greater than 100 billion dong;

b) The enterprise's revenue of the previous year is not greater than 300 billion dong.

[2] According to Article 3.2 of Law on Provision of Assistance for Small and Medium Enterprises, "start-up" is an SME that is established to implement its business ideas based on the exploitation of intellectual property, technology and new business models and is able to grow quickly.

Who needs to comply?

Decree 13 applies to all individuals and entities operating in Vietnam who engage in the provision, collection, or utilization of data for any purpose within the country (Article 1). This includes:

- Vietnamese agencies, organizations, and individuals;
- Foreign agencies, organizations, and individuals in Vietnam;
- Vietnamese agencies, organizations, and individuals operating abroad; and
- Foreign agencies, organizations, and individuals directly participating in or related to personal data processing activities in Vietnam.

Whilst Decree 13 has similar requirements in comparison with the EU's General Data Protection Regulation (**GDPR**), there are certain differences. Companies that have privacy management practices and policies in place that are either GDPR-compliant or compliant with other privacy laws are not automatically granted a free pass to compliance with Decree 13. Thus, it is critical for AusCham Members to review and audit their internal privacy management practices and policies to identify gaps and a corresponding action plan.

Key provisions

Definition of parties in handling personal data

Article 2 stipulates different roles of data handlers and their corresponding responsibilities.

Personal Data Controller means an organization or individual that decides on the purpose and means of personal data processing. The Personal Data Controller is responsible for notifying and cooperating with the competent authorities in case of personal data breaches. The Personal Data Controller is ultimately accountable to the data subject and bears the burden of proving prior consent is obtained for all processing activities.

Personal Data Processor means an organization or individual that performs the processing of the data on behalf of a Personal Data Controller under a contract or agreement with such Personal Data Controller. While the Data Controller holds primary responsibility for personal data processing, the Data Processor plays a critical role in ensuring the proper handling and protection of the data on behalf of the Personal Data Controller.

Personal Data Controller cum Processor means an organization or individual that decides on the purpose and means of processing and simultaneously and directly performs the personal data processing. This hybrid role needs to comply with the obligations of both Data Controller and Data Processor.

Third Party means an organization or individual other than the Data Subject, Personal Data Controller, Personal Data Processor and Personal Data Controller and Processor that is authorized to process personal data. This definition can be broadly referred to other persons involved in personal data handling, such as payment service providers, telecommunication service providers, etc.

Classification of Personal Data

Also, according to Article 2, personal data refers to any information that is expressed in the form of symbol, text, digit, image, sound or in similar forms in electronic environment that is associated with a particular natural person or helps identify a particular natural person. Personal data is classified as basic personal data and sensitive personal data.

Basic Personal Data includes usual identification information e.g., name, date of birth, date of death, contact details, marital status and family relationship, ethnicity, personal image, gender, personal identification numbers (citizen identification number, passport, tax code, social/medical insurance code, driving license number, vehicle plate number) but also including blood type, digital accounts and data reflecting individuals' activity history on cyberspace.

Sensitive Personal Data is defined as personal data associated with an individual's privacy and when violated will directly affect the individual's legitimate rights and interests and includes political and religious views, health conditions (except blood type), biometric data, genetic data, sexual orientation, criminal records, customer data of credit institutions, intermediate payment services, geographic location and other types of sensitive personal data as stipulated by Vietnamese laws.

Principles for the Processing of Personal Data

Article 3 stipulates principles for processing personal data.

Closely modeled on those under the GDPR, these eight basic tenets include: (i) the processing is in accordance with the law (lawfulness); (ii) data subjects must be informed of every activity involving the processing (transparency); (iii) personal data shall be processed only for the purposes registered and announced in relation to the processing (purpose limitation); (iv) personal data collected must be relevant and

confined to the extent and purposes of the processing (data minimization); (v) personal data must be updated and supplemented in accordance with the processing's purposes (accuracy); (vi) personal data must be subject to protection and security measures during the processing (integrity, confidentiality and security); (vii) personal data shall be kept only for a term appropriate with the processing's purposes (storage limitation); and (viii) the Controller and Controller-Processor must comply with the above principles and demonstrate their compliance (accountability).

The above principles are extremely important to keep in mind, as they will play a key role in guiding businesses' compliance procedures.

Prohibited Acts

There are certain prohibited activities in terms of handling personal data (Article 8), specifically:

(i) Processing personal data contrary to the law on personal data protection;

(ii) Processing personal data to create information and data to fight against the State of the Socialist Republic of Vietnam;

(iii) Processing personal data to create information and data that affect the national security, social order and safety, and legitimate rights and interests of other organizations and individuals;

(iv) Obstructing the personal data protection by competent agencies;

(v) Taking advantage of the personal data protection activities to violate the law.

Measures to protect personal data protection

The PDPD sets out that every party processing personal data must apply managerial and technical measures to protect personal data (Article 26 to 28). However, it does not indicate which management and technical measures could be considered sufficient. Measure for personal data protection shall include management and technical measures taken by organizations and/or individuals in relation to personal data processing or by competent state agencies.

In terms of basic personal data, Article 27 of Decree 13 requires organizations and/or individuals to: (i) develop and promulgate the regulations on personal data protection, specifying the tasks to be completed in accordance with the Decree; (ii) encourage the application of standards for personal data protection appropriate to the fields, industries and activities in relations to the personal data processing; (iii) check the systems, facilities and equipment serving the personal data processing for network security before the processing, permanent deletion or destruction of devices containing personal data.

The protection measures for sensitive personal data appear to be a bit stricter. More specifically, the protection of sensitive personal data would necessitate (i) all of the managerial and technical measures required for the protection of basic personal data, plus (ii) the appointment of a Data Protection Officer (**DPO**) and an internal personal Data Protection Department (**DPD**) (information on the DPD and the DPO should be notified to the authority), and (iii) notification to data subjects that their sensitive personal data is processed except in specified cases.

Consent of the data subject

Prior consent requirements

The PDPD maintains a consent-centric approach, requiring the permission of a data subject for the data processing of their personal data, including both basic and sensitive personal data (Article 11). Personal data processing means one or more operations that affect personal data, such as: collecting, recording, analyzing, verifying, storing, editing, publishing, combination, access, retrieval, recovery, encryption, decryption, duplication, sharing, transmission, provision, transfer, deletion, destruction of personal data or other relevant operations.

AusCham highlights that personal data processing includes processing activities of internal staff data also.

Consent must be voluntarily and based on the data subject's full understanding of (i) the purpose of the personal data processing; (ii) the type of personal data to be processed; (iii) the entities authorized to process personal data; and (iv) the data subject's rights.

The consent shall be made for a single purpose. Upon multiple purposes, the Personal Data Controller and Personal Data Controller cum Processor shall list the purposes for the data subjects to give consent to one or more of the stated purposes.

Consent must be expressed clearly and specifically in writing, by voice, by ticking the consent box, by text message, by selecting consent technical settings, or via another action which demonstrates the same. Moreover, consent must be expressed in a format that can be printed out or reproduced in writing, including in electronic or verifiable formats.

Default setting, pre-ticked boxes, general terms and conditions or silence or non-response will not be considered as consent.

As mentioned above, with regard to the processing of sensitive personal data, the data subjects shall be informed that the data to be processed is sensitive personal data.

Withdrawal of consent

The individual has the right to withdraw his or her consent at any time (Article 12). The withdrawal of consent shall be expressed in a format that can be printed and/or reproduced in writing, including in electronic or verifiable formats. Upon receipt of the data subject's request for withdrawal of consent, the Personal Data Controller and/or the Personal Data Controller cum Processor shall notify the data subject of possible consequences and damage upon withdrawal of consent.

Exemption

Regardless of the foregoing, Article 17 states that the processing of personal data without consent is permissible in the following circumstances:

- In urgent cases where it is necessary to immediately process relevant personal data to protect the life or health of the data subject or others;
- Where the public disclosure of personal data is in accordance with the law;
- When the processing of data is done by competent state agencies in the event of a state of emergency on national defense, security, social order and safety, major disaster, or dangerous epidemic; or when there is a risk that threatens security and national defense but not to the extent where it is necessary to declare a state of emergency; or to prevent and combat riots, terrorism, crimes and violations of the law;
- To fulfill the contractual obligations of the data subject with relevant agencies, organizations and individuals as prescribed by law; or
- To serve the activities of state agencies as prescribed by sector-specific laws.

Notification before processing personal data

One notification shall be given before the personal data processing (Article 13). The notification shall cover: (i) purpose of the processing; (ii) type of personal data to be processed; (iii) method of processing; (iv) information on other organizations and/or individuals who are relevant to the processing purposes; (v) potential and unwanted consequences and/or damage; (vi) starting time and ending time of the data processing.

The notification to be given to the data subject shall be made in a format that can be printed and/or reproduced in writing, including in electronic or verifiable formats.

The Personal Data Controller and Personal Data Controller and Processor shall not be required to comply with the above rules in the following cases:

- The data subject has acknowledged and given consent to all of the contents
  specified in clauses 1 and 2 of this Article before authorizing the Personal Data
  Controller and Personal Data Controller and Processor to collect his/her personal data in accordance with Article 9 hereof;
- The personal data is subject to the processing by a competent state agency for the operation of the state agency in accordance with the law.

There might be an overlap between rules on prior consent of data subject (Article 11) and notification before processing personal data (Article 13). However, as the Decree indicates those requirements in two separate Articles, it is recommended for AusCham Members to conduct both types of activities.

Data Protection Impact Assessment Dossier ("DPIA Dossier")

Article 24 stipulates that Controllers/Processors/Controller-Processors (regardless of the type) must establish and keep available a DPIA Dossier. One copy of the DPIA Dossier must be submitted to the Department of Cybersecurity and Hi-Tech Crime Prevention ("A05"), an authority under the Ministry of Public Security of Vietnam ("MPS") within 60 days from the date of processing of personal data. AusCham notes that definition of "processing activities" under Article 2 is broad, including collection of personal data, which the vast majority of AusCham Members are involved in, at least in terms of collecting information of the staff.

Form No. 04 of Decree 13 provides a sample of DPIA. See Appendix 1 for Vietnamese version and Appendix 2 for English version for reference. Please note that A05 accepts submissions in Vietnamese only.

Form No. 05 of Decree 13 is used for updating and supplementing the submitted DPIA. See Appendix 3 for Vietnamese version and Appendix 4 for English version for reference. Please note that A05 accepts submissions in Vietnamese only.

Cross-Border Transfer of Personal Data

Definition

Decree 13 defines cross-border transfer of personal data as any activity involving the use of cyberspace, electronic equipment, electronic means or other forms to transfer personal data of Vietnamese citizens to a location outside the territory of the Socialist Republic of Vietnam or use of a location outside the territory of the Socialist Republic of Vietnam to process a Vietnamese citizen's personal data of, including:

- Organizations, enterprises or individuals transferring personal data of Vietnamese citizens to organizations, enterprises or management bodies located overseas for processing in accordance with the purposes consented by the data subjects;
- Processing of personal data of Vietnamese citizens by use of automated systems located outside the territory of the Socialist Republic of Vietnam by the Personal Data Controller, Personal Data Controller and Processor or Personal Data Processor in accordance with the purposes consented by the data subjects.

Required Acts

The 'transferor' of personal data must first create a Dossier of Impact Assessment for the Cross-Border Transfer of Personal Data ("TIA Dossier") before transferring personal data out of Vietnam. The TIA Dossier must include: (i) information and contact details of the transferor and receiver; (ii) full name and contact details of the organization and/or individual in charge of the transferor; (iii) description and explanation of the objectives of the personal data processing following the transfer; (iv) description and clarification on the type of personal data to be transferred; (v) description and explanation on the compliance with the regulations under the PDPD, detailing the applied measures for personal data protection; (vi) assessment on the impact of the processing, as well as the potential and unwanted consequences and/or damages, and measures to minimize or

eliminate such consequences and/or damages; (vii) consent from the data subject; and (viii) documents pertaining to the binding responsibilities of personal data processing between the transferor and transferee.

The TIA Dossier must be always made available for the inspection and evaluation by the authority. In addition, the transferor must submit one original copy of the TIA Dossier to the Department of Cybersecurity and Hi-Tech Crime Prevention ("A05"), an authority under the Ministry of Public Security of Vietnam ("MPS") within 60 days from the date of the personal data processing.

In terms of reporting, the PDPD adopts an ex-post management approach, requiring the transferor to notify and submit to the A05 the information on the transfer, as well as the contact details of the responsible organization and individuals in writing upon the successful completion of the transfer. The A05 will review the TIA Dossier and may request that the transferor complete the dossier if it is found to be incomplete or does not comply with the PDPD standards.

In addition, it is worth noting that the MPS has the power to halt cross-border data transfers if (i) the data is used for activities that violate the interests and national security of Vietnam; (ii) the transferor fails to complete or update the TIA Dossier; or (iii) the personal data of Vietnamese citizens is disclosed or lost. The first criterion is very broad and vague.

Form No. 06 of Decree 13 provides a sample of TIA. See Appendix 5 for Vietnamese version and Appendix 6 for English version for reference. Please note that A05 accepts submissions in Vietnamese only.

Form No. 05 of Decree 13 is used for updating and supplementing the submitted TIA. See Appendix 3 for Vietnamese version and Appendix 4 for English version for reference. Please note that A05 accepts submissions in Vietnamese only.

Proposed Compliance Actions

1. Identify your role in data handling procedures, e.g., whether you are the Personal Data Controller, Personal Data Processor, Personal Data Controller cum Processor, or Third Party; and your possible corresponding obligations.

2. Identify the type of personal data you are handling with, e.g. whether the data is basic or sensitive. In case you are handling sensitive personal data, assign a Data Protection Officer ("DPO") and an internal personal data protection department ("DPD").

3. Develop or review your personal data management system to:

- Examine if the existing personal data management system (practice, policies, training and system log, etc.) is in compliance with Decree 13 requirements;
- In case you do not hve an existing data management system, or your existing data management system does not comply with Decree 13 requirements, develop an internal personal data management regulation, which at least contains:

(i) a data categorization for different types of personal data;

(ii) rules and procedures for handling personal data, which includes proposed actions in points 4, 5, 6, 7, 8, and 9 below and distinguishes the management system for each type of personal data (e.g. basic and sensitive);

(iii) rights and responsibilities of related parties in handling personal data;

(iv) rules and processes in case of personal data breaches, and

(v) remediation protocols.

4. Identify whether do you need to obtain consent from data subject? If yes, establish a mechanism to get consent from data subject. The form of consent must comply with the requirements of Decree 13 (Article 11). Make sure that the consent is capable of being printed or reproduced in writing, which can be in electronic format.

5. Establish a mechanism for data subjects to withdraw their consent (Article 12). Make sure to notify the data subject of the consequence or damage that has arisen from the withdrawal.

6. Identify whether do you need to notify the data subject before processing personal data? If yes, establish a mechanism to notify data subject before processing the data. Ensure the minimum requirements stipulated by Article 13.

7. Establish a mechanism to handle requests of data subject. Any request to restrict or objection to data processing will need to be addressed within 72 hours of the request.

8. Prepare and submit Data Protection Impact Assessment Dossier to the MPS within 60 days from the date of processing of personal data.

9. Prepare and submit Cross Border Transfers Impact Assessment Dossier to the MPS.

APPENDIX 1

Form No. 04 (Vietnamese)

Mẫu số 04

TÊN TỔ CHỨC **--------**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc** **----------**
Số:	*....., ngày.... Tháng... năm...*

THÔNG BÁO

GỬI HỒ SƠ ĐÁNH GIÁ TÁC ĐỘNG XỬ LÝ DỮ LIỆU CÁ NHÂN

Kính gửi: Bộ Công an

(Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao,

Bộ Công an)

Thực hiện quy định về bảo vệ dữ liệu cá nhân,.....[1] gửi Bộ Công an Hồ sơ đánh giá tác động xử lý dữ liệu cá nhân, như sau:

1. Thông tin về tổ chức, doanh nghiệp

- Tên tổ chức, doanh nghiệp:.....

- Địa chỉ trụ sở chính:.....

- Địa chỉ trụ sở giao dịch:.....

- Quyết định thành lập/Giấy chứng nhận đăng ký doanh nghiệp/Giấy chứng nhận đăng ký kinh doanh/Giấy chứng nhận đầu tư số:..... do.... cấp ngày... tháng... năm... tại...

- Điện thoại:..... Website.....

- Nhân sự chịu trách nhiệm bảo vệ dữ liệu cá nhân:.....

Họ và tên:.....

Chức danh:.....

Số điện thoại liên lạc (cố định và di động):.....

Email:.....

2. Hồ sơ đánh giá tác động xử lý dữ liệu cá nhân

1.....

2.....

3. Cam kết

(Tên cơ quan, tổ chức, doanh nghiệp) xin cam kết: Chịu trách nhiệm trước pháp luật về tính chính xác và tính hợp pháp của hồ sơ đánh giá tác động xử lý dữ liệu cá nhân và tài liệu kèm theo.

Nơi nhận:	**TM. TỔ CHỨC, DOANH NGHIỆP**
- Như trên;	*(Ký, ghi rõ họ tên, đóng dấu)*
...	

Ghi chú: 1. Tên tổ chức/doanh nghiệp

APPENDIX 2

Form No. 04 (English)

NAME OF ORGANIZATION **--------**	**SOCIALIST REPUBLIC OF VIETNAM** **Independence - Freedom - Happiness** **----------**
No.:	*....., [insert date]*

NOTICE
OF SUBMISSION OF THE DOSSIER FOR ASSESSMENT OF THE IMPACT OF PERSONAL DATA PROCESSING

Respectfully to: Ministry of Public Security
(Department of Cybersecurity and Hi-Tech Crime Prevention,
Ministry of Public Security)

Pursuant to the regulations on personal data protection,.....[1] would like to submit to the Ministry of Public Security a Dossier for Assessment of the Impact of Personal Data Processing, as follows:

1. Details of organization/enterprise

- Name of organization/enterprise: .....

- Head office address: .....

- Transaction office address:.....

- Decision on Establishment/Certificate of Enterprise Registration/Certificate of Business Registration/Certificate of Investment No.: ..... issued by ..... on [*insert date*] at ...

- Telephone:..... Website.....

- Staff in charge of personal data protection: .....

Full name:.....

Position: .....

Contact telephone numbers (landline & mobile):.....

Email:.....

2. Dossier for Assessment of the Impact of Personal Data Processing

1. .....

2. .....

3. Undertakings

(Name of agency/organization/ enterprise) undertakes: To take responsibility before the law for the accuracy and legality of the Dossier for Assessment of the Impact of Personal Data Processing and the enclosures.

Recipients:

- As mentioned above;

....

ON BEHALF OF THE ORGANIZATION/ENTERPRISE

(Signature, full name, seal)

Note: 1. Name of enterprise/organization

APPENDIX 3

Form No. 05 (Vietnamese)

Mẫu số 05

TÊN TỔ CHỨC --------	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc** ----------
Số:	*....., ngày.... tháng... năm...*

THÔNG BÁO

THAY ĐỔI NỘI DUNG HỒ SƠ.....[1]

Kính gửi: Bộ Công an

(Qua Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao)

Thực hiện quy định về bảo vệ dữ liệu cá nhân,.....[2] gửi Bộ Công an Hồ sơ đánh giá tác động xử lý dữ liệu cá nhân, như sau:

1. Thông tin về tổ chức, doanh nghiệp

- Tên tổ chức, doanh nghiệp:.....

- Địa chỉ trụ sở chính:.....

- Địa chỉ trụ sở giao dịch:.....

- Quyết định thành lập/Giấy chứng nhận đăng ký doanh nghiệp/Giấy chứng nhận đăng ký kinh doanh/Giấy chứng nhận đầu tư số:..... do.... cấp ngày... tháng... năm... tại...

- Điện thoại:..... Website.....

- Nhân sự chịu trách nhiệm bảo vệ dữ liệu cá nhân:.....

Họ và tên:.....

Chức danh:.....

Số điện thoại liên lạc (cố định và di động):.....

Email:.....

2. Mô tả tóm tắt thay đổi nội dung hồ sơ

- Nội dung thay đổi:.....

- Lý do thay đổi:.....

3. Tài liệu kèm theo

1.....

2.....

4. Cam kết

(Tên cơ quan, tổ chức, doanh nghiệp) xin cam kết: Chịu trách nhiệm trước pháp luật về tính chính xác và tính hợp pháp của nội dung thay đổi và tài liệu kèm theo.

Nơi nhận:	**TM. TỔ CHỨC, DOANH NGHIỆP**
- Như trên;	*(Ký, ghi rõ họ tên, đóng dấu)*
...	

Ghi chú: 1. Tên Hồ sơ: Hồ sơ đánh giá tác động xử lý dữ liệu cá nhân hoặc Hồ sơ đánh giá tác động của Xử lý dữ liệu cá nhân xuyên biên giới.

1. Tên tổ chức/doanh nghiệp

APPENDIX 4

Form No. 05 (English)

NAME OF ORGANIZATION **--------**	**SOCIALIST REPUBLIC OF VIETNAM** **Independence - Freedom - Happiness** **----------**
No.:	*....., [insert date]*

NOTICE
OF CHANGES TO A DOSSIER.....[1]

Respectfully to: Ministry of Public Security
(Department of Cybersecurity and Hi-Tech Crime Prevention,
Ministry of Public Security)

Pursuant to the regulations on personal data protection,.....[2] would like to submit to the Ministry of Public Security a Dossier for Assessment of the Impact of Personal Data Processing, as follows:

1. Details of organization/enterprise

- Name of organization/enterprise: .....

- Head office address: .....

- Transaction office address:.....

- Decision on Establishment/Certificate of Enterprise Registration/Certificate of Business Registration/Certificate of Investment No.: ..... issued by ..... on [*insert date*] at ...

- Telephone:..... Website.....

- Staff in charge of personal data protection: .....

Full name:.....

Position: .....

Contact telephone numbers (landline & mobile):.....

Email:.....

2. Brief description of changes to the dossier

- Changed items:.....

- Reasons for changes: .....

3. Attached documents

3. Undertakings

(Name of agency/organization/ enterprise) undertakes: To take responsibility before the law for the accuracy and legality of the changed items and the enclosures.

Recipients:

- As mentioned above;

....

ON BEHALF OF THE ORGANIZATION/ENTERPRISE

(Signature, full name, seal)

Note: 1. Name of dossier: Dossier for Assessment of the Impact of Personal Data Processing or Dossier for Assessment of The Impact of Cross-Border Transfer of Personal Data.

1. Name of organization/enterprise

APPENDIX 5

Form No. 06 (Vietnamese)

Mẫu số 06

TÊN TỔ CHỨC **--------**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc** **----------**
Số:	*....., ngày.... tháng... năm...*

HỒ SƠ ĐÁNH GIÁ TÁC ĐỘNG CHUYỂN DỮ LIỆU CÁ NHÂN RA NƯỚC NGOÀI

Kính gửi: Bộ Công an

(Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an)

Thực hiện quy định về bảo vệ dữ liệu cá nhân,.....[1] gửi Bộ Công an Hồ sơ đánh giá tác động chuyển dữ liệu cá nhân ra nước ngoài, như sau:

1. Thông tin về tổ chức, doanh nghiệp

- Tên tổ chức, doanh nghiệp:.....

- Địa chỉ trụ sở chính:.....

- Địa chỉ trụ sở giao dịch:.....

- Quyết định thành lập/Giấy chứng nhận đăng ký doanh nghiệp/Giấy chứng nhận đăng ký kinh doanh/Giấy chứng nhận đầu tư số:..... do.... cấp ngày... tháng... năm... tại...

- Điện thoại:..... Website.....

- Nhân sự chịu trách nhiệm bảo vệ dữ liệu cá nhân:.....

Họ và tên:.....

Chức danh:.....

Số điện thoại liên lạc (cố định và di động):.....

Email:.....

2. Hồ sơ đánh giá tác động chuyển dữ liệu cá nhân ra nước ngoài

1.....

2.....

3. Cam kết

(Tên cơ quan, tổ chức, doanh nghiệp) xin cam kết: Chịu trách nhiệm trước pháp luật về tính chính xác và tính hợp pháp của Hồ sơ đánh giá tác động chuyển dữ liệu cá nhân ra nước ngoài và tài liệu kèm theo.

Nơi nhận:	**TM. TỔ CHỨC, DOANH NGHIỆP**
- Như trên;	*(Ký, ghi rõ họ tên, đóng dấu)*
...	

APPENDIX 6

Form No. 06 (English)

NAME OF ORGANIZATION **--------**	**SOCIALIST REPUBLIC OF VIETNAM** **Independence - Freedom - Happiness** **----------**
No.:	*....., [insert date]*

NOTICE
OF SUBMISSION OF THE DOSSIER FOR ASSESSMENT OF THE IMPACT OF CROSS-BORDER TRANSFER OF PERSONAL DATA

Respectfully to: Ministry of Public Security
(Department of Cybersecurity and Hi-Tech Crime Prevention,
Ministry of Public Security)

Pursuant to the regulations on personal data protection, ... 1 would like to submit to the Ministry of Public Security a Dossier for Assessment of the Impact of Cross-border Transfer of Personal Data, as follows:

1. Details of organization/enterprise

- Name of organization/enterprise: .....

- Head office address: .....

- Transaction office address:.....

- Decision on Establishment/Certificate of Enterprise Registration/Certificate of Business Registration/Certificate of Investment No.: ..... issued by ..... on [*insert date*] at ...

- Telephone:..... Website.....

- Staff in charge of personal data protection: .....

Full name:.....

Position: .....

Contact telephone numbers (landline & mobile):.....

Email:.....

2. Dossier for Assessment of the Impact of Cross-border Transfer of Personal Data

1. .....

2. .....

3. Undertakings

(Name of agency/organization/ enterprise) undertakes: To take responsibility before the law for the accuracy and legality of the Dossier for Assessment of the Impact of Cross-border Transfer of Personal Data and the enclosures.

Recipients:

- As mentioned above;

....

ON BEHALF OF THE ORGANIZATION/ENTERPRISE

(Signature, full name, seal)

Note: 1. Name of enterprise/organization

Contact Us

This publication has been prepared for general guidance on matters of interest only. For further assistance, please contact AusCham Advocacy Officer at advocacy@auschamvn.org.

Tran Thi Lan Huong
Advocacy Officer
Read my Bio
advocacy@auschamvn.org

Disclaimer

The information provided by AusCham Vietnam is intended for general information purposes only. AusCham Vietnam does not provide advisory services and does not share this information in an advisory capacity. It is recommended that AusCham members seek professional advice tailored to their specific needs. In no event shall AusCham Vietnam be liable for any loss or damage arising from the use of this information.