政府

編號：13/2023/NĐ-CP

越南社會主義共和國

獨立－自由－幸福

河內市，2023 年 04 月 17 日

議定

個人資料保護

根據2015年06月19日《政府組織法》；於2019年11月22日修訂和補充若干條款之《政府組織法》和《地方政府組織法》；

根據2015年11月24日《民事法》；

根據2004年12月03日《國家安全法》

根據2018年06月12日《網路安全法》；

根據公安部部長的提議；

政府頒行個人資料保護議定

第一章

總則

第1條：調整範圍及適用對象

1. 本議定規定了對個人資料的保護及與個人資料保護相關之機關、組織和個人之責任。

2. 本議定適用於：

a) 越南機關、組織及個人；

b) 在越南之外國機關、組織及個人；

c) 在國外開展業務的越南機構、組織和個人

d) 直接參與或涉及越南個人資料處理活動的外國機構、組織和個人。

第2條：詞語解釋

在本議定中，下列術語的解釋如下：

1. 個人資料是以符號、文字、數字、圖像、聲音等形式存在於電子存儲介質上，與特定個人相關聯或有助於識別特定個人的信息。個人資料包括基本個人資料及敏感個人資料。

2. 有助於識別特定個人的信息是透過個人活動與其他存儲資料、信息相結合而形成之信息，其可以識別特定個人。

3. 基本個人資料包括：

a) 姓氏，中間名及出生登記名字及其他名字（如有）；

b) 出生日期；死亡或失蹤日期；

c) 性別；

d) 出生地、出生登記地、常住地、暫住地、現居住地、籍貫、聯繫地址；

đ) 國籍；

e) 個人照片；

g) 電話號碼、身份證號碼、個人識別碼、護照號碼、駕照號碼、車牌號碼、個人納稅識別號碼、社會保險號碼、醫療保險卡號碼；

h) 婚姻狀況；

i) 親屬的相關信息（父母、子女）；

k) 有關個人數字賬戶的信息；反映網絡空間的活動及活動歷史記錄的個人資料；

l) 與特定人相關聯或有助於識別特定人的其他信息不屬於本條第4款所規定之範圍。

4. 敏感個人資料是指與個人隱私相關的個人資料，其一旦受到侵犯將直接影響到個人的合法權益，包括：

a) 政治觀點、宗教觀點；

b) 病歷中記載的健康狀況及隱私，不包括血型信息；

c) 有關民族、族裔血統的信息；

d) 有關個人所繼承或擁有的遺傳特徵之信息；

đ) 有關個人的身體屬性及生物特徵的信息；

e) 有關個人性生活或性取向的信息；

g) 由執法機構收集和存儲關於犯罪和違法行為的資料；

h) 信貸機構、外國銀行分行、支付中介服務機構及其他授權機構的客戶信息，包括：法律規定的客戶身份識別信息、賬戶信息、存款信息、存入資產信息、交易信息；作為信貸機構、銀行分行、支付中介服務機構擔保方的組織及個人信息；

i) 透過定位服務識別的個人位置數據；

k) 法律規定的其他個人資料屬於特殊類及需要採取必要的保密措施。

5. 個人資料保護是指依法預防、發現、阻止和處理與個人資料有關的違法行為之活動。

6. 資料的主體是個人資料所反映之個人。

7. 個人資料處理是影響個人資料的一項或多項活動，例如：收集、記錄、分析、確認、存儲、更正、披露、組合、訪問、輸出、撤回、編碼、解碼、複製、分享、傳輸、提供、轉交、刪除、銷毀個人資料或其他相關行為。

8. 資料主體的同意是指資料主體明確、自願、肯定地表示允許處理個人資料。

9. 個人資料管控方是決定個人資料處理目的及方式的組織、個人。

10. 個人資料處理方是指通過與資料管控方簽訂的合同或協議，代表資料管控方進行處理資料的組織、個人。

11. 個人資料管控及處理方是同時決定個人資料處理目的、方式並直接處理個人資料的組織、個人。

12. 第三方是除資料主體、個人資料管控方、個人資料處理方、個人資料管控及處理方之外有權處理個人資料的組織、個人。

13. 自動處理個人資料是透過電子方式執行個人資料處理的一種形式，以達到評估、分析、預測特定個人的活動，例如：習慣、偏好、興趣、置信度、行為、地點、趨勢、能力及其他情況。

14. 向境外轉移個人資料是指利用網絡空間、設備、電子手段或其他形式將越南公民的個人資料轉移至越南社會主義共和國境外的某個地點或利用越南社會主義共和國境外的某個地點處理越南公民的個人資料，包括：

a) 將越南公民的個人資料傳輸給境外組織、企業、管理部門的組織、企業、個人應當按照資料主體同意的目的進行處理；

b) 個人資料管控方、個人資料管控及處理方、個人資料處理方透過位於越南社會主義共和國境外的自動系統處理越南公民的個人資料應當按照資料主體同意的目的進行處理；

第3條：個人資料保護之原則

1. 個人資料應當依法處理。

2. 除非法律另有規定，資料主體對其個人資料的相關處理活動享有知情權。

3. 個人資料只能按照個人資料管控方、個人資料處理方、個人資料管控及處理方、第三方登記及指定的目的進行處理。

4. 個人資料的收集必須符合及僅限於需要處理的範圍和目的。除非法律另有規定，不得以任何形式買賣個人資料。

5. 個人資料應根據處理目的進行更新和補充。

6. 個人資料正處理過程中可以採取各種保護、保密措施，包括防止違反個人資料保護規定的行為以及防範丟失、損壞或因事故、使用技術措施造成的損失。

7. 除非法律另有規定，個人資料僅在適合資料處理目的的期限內存儲。

8. 資料管控方、個人資料管控及處理方有責任遵守本條第1至第7款所規定的資料處理原則，並需要證明其遵守該資料處理原則。

第4條：違反個人資料保護規定的處分

對於違反個人資料保護規定的機關、組織及個人，視情節輕重，可按照規定給予紀律處分、行政處分或刑事處理。

第5條：國家對個人資料保護的管理

政府統一個人資料保護的國家管理工作。

國家對個人資料保護管理的內容包括：

1. 報送國家主管機關頒布或者依據職權頒布法律文件並指導、組織實施個人資料保護的法律文件。

2. 制定並組織實施個人資料保護策略、政策、提案、項目、方案和計劃。

3. 按照法律規定向機關、組織和個人提供個人資料保護措施、流程和標準的指導。

4. 宣傳、教育個人資料保護法；佈告、傳播保護個人資料的知識和技能。

5. 建設、培訓及培養幹部、公務員、公職人員及被指派從事個人資料保護的專員。

6. 稽查、檢查個人資料保護法規的執行情況；依法處理投訴、舉報以及處理違反個人資料保護法的行為。

7. 向國家主管機關提供個人資料保護情況和個人資料保護法實施情況的統計、資訊及報告。

8. 保護個人資料的國際合作。

第6條：個人資料保護議定、相關法律及國際條約的適用

個人資料的保護按照越南社會主義共和國作為締約國之國際條約規定、相關法律及本議定的其他規定執行。

第7條：保護個人資料的國際合作

1. 建立國際合作機制以促進個人資料保護法的有效執行。

2. 參與他國保護個人資料的司法協助，包括通知、建議投訴、協助調查及信息交換，並以適當的保護措施來保護個人資料。

3. 舉辦會議、研討會、科學研究及促進保護個人資料的國際執法合作活動。

4. 舉辦雙邊和多邊會議，交流個人資料保護的法制建設和實踐經驗。

5. 個人資料保護的技術轉讓。

第8條：嚴厲禁止的行為

1. 違反個人資料保護法的規定進行處理個人資料。

2. 以創建危害越南社會主義共和國的信息、資料為目的進行處理個人資料。

3. 以創建影響國家安全、社會秩序安全以及其他組織和個人合法權益的信息、資料為目的進行處理個人資料。

4. 阻礙主管機關的個人資料保護活動。

5. 利用個人資料保護活動進行違法行為。

第二章

個人資料保護活動

第1節：資料主體的權利及義務

第9條：資料主體的權利

1. 知情權

除非法律另有規定，資料主體對其個人資料的處理活動享有知情權。

2. 同意權

除本議定第17條規定的情況外，資料主體對其個人資料的處理享有同意和拒絕權。

3. 訪問權

除非法律另有規定，資料主體對其個人資料享有瀏覽、編輯或要求修改個人資料的訪問權。

4. 同意撤回權

除非法律另有規定，資料主體有權撤回其同意。

5. 資料刪除權

除非法律另有規定，資料主體有權刪除或要求刪除其個人資料。

6. 資料處理限制權

a) 除非法律另有規定，資料主體有權對其個人資料要求限制處理；

b) 除非法律另有規定，在資料主體提出請求後72個小時內對資料主體請求限制的所有個人資料進行限制處理。

7. 資料取得權

除非法律另有規定，資料主體有權要求個人資料管控方、個人資料管控及處理方提供其個人資料。

8. 資料處理反對權

a) 除非法律另有規定，資料主體有權反對個人資料管控方、個人資料管控及處理方處理其個人資料，以防止或限制個人資料的披露或用於廣告和營銷目的。

b) 除非法律另有規定，個人資料管控方、個人資料管控及處理方應當在收到資料主體的請求後於72個小時內滿足資料主體的請求。

9. 投訴、舉報、起訴權

資料主體有權依法投訴、舉報或起訴。

10. 損失索賠權

除非當事人另有約定或者法律另有規定，當發生違反個人資料保護規定的行為時，資料主體有權依法索賠損失。

11. 自衛權

資料主體有權依照《民事法》、其他有關法律及本議定的規定保護自己，或者要求主管機構、組織依照《民事法》第11條規定實施保護民事權利的措施。

第10條：資料主體的義務

1. 保護自己的個人資料；要求其他相關組織和個人保護其個人資料。

2. 尊重、保護他人的個人資料。

3. 在同意允許處理個人資料時提供完整且準確的個人資料。

4. 參與個人資料保護技能的宣傳和傳播。

5. 遵守個人資料保護法的規定，參與防治個人資料保護法違法行為。

第2節：個人資料處理過程中的個人資料保護

第11條：資料主體的同意

1. 除非法律另有規定，資料主體的同意適用於個人資料處理程序的所有活動。

2. 僅在資料主體自願且完全了解以下內容時，資料主體的同意才有效：

a) 被處理的個人資料類型；

b) 處理個人資料的目的；

c) 被允許處理個人資料的組織、個人；

d) 資料主體的權利和義務。

3. 資料主體必須明確表達同意，具體是以書面形式、語音、勾選同意框、發送同意短訊、選擇同意的技術設置或者透過其他可明確表達的行為。

4. 資料主體的同意必須與目的相符。當存在多種目的時，個人資料管控方、個人資料管控及處理方應列出各項目的，供資料主體對一項或多項所述目的給予同意。

5. 資料主體的同意必須以可以打印、書面複製的格式表達，包括電子或可驗證的格式。

6. 資料主體的沉默或不回應不被視為同意。

7. 資料主體可以給予部分或有條件的同意。

8. 對於敏感個人資料的處理，必須告知資料主體所處理的資料屬於敏感個人資料。

9. 資料主體的同意一直生效直至資料主體另有決定或主管當局提出書面要求時為止。

10. 如果發生爭議，證明資料主體同意的責任由個人資料管控方、個人資料管控及處理方承擔。

11. 在資料主體已知悉並根據本條第3款規定予以同意的情況下，經依照《民事法》的規定授權的組織和個人可代表資料主體以配合個人資料管控方、個人資料管控及處理方進行個人資料處理的相關程序；對法律另有規定者除外。

第12條：撤回同意

1. 撤回同意並不影響資料處理在撤回同意前的合法性。

2. 資料主體的撤回同意必須以可以打印、書面複製的格式表達，包括電子或可驗證的格式。

3. 在收到資料主體撤回同意的請求後，個人資料管控方、個人資料管控及處理方應通知資料主體撤回同意時可能產生的後果和損害。

4. 資料管控方、資料處理方、資料管控及處理方、第三方在執行本條第2款規定後，必須停止並要求相關組織和個人停止處理已撤回同意的資料主體的資料。

第13條：個人資料處理的通知

1. 在進行個人資料處理活動之前應發出一次通知。

2. 向資料主體發出有關個人資料處理的通知內容：

a) 處理目的；

b) 與本條第2款a點所規定之處理目的相關的個人資料類型；

c) 處理方式；

d) 與本條第2款a點所規定之處理目的相關的其他組織、個人的資訊；

đ) 可能發生的不良後果及損害；

e) 資料處理的開始時間和結束時間。

3. 對資料主體的通知必須以可以打印、書面複製的格式表達，包括電子或可驗證的格式。

4. 個人資料管控方、個人資料管控及處理方在下列情況下無需執行本條第1款規定：

a) 資料主體在同意予以個人資料管控方、個人資料管控及處理方按照本議定第9條規定進行收集個人資料之前，已知曉並完全同意本條第1款及第2款規定的內容；

b) 個人資料由國家主管機關依法處理，以服務國家機關的運作。

第14條：提供個人資料

1. 資料主體有權要求個人資料管控方、個人資料管控及處理方提供其個人資料。

2. 個人資料管控方、個人資料管控及處理方：

a) 經資料主體的同意後可以向其他組織、個人提供個人資料，法律另有規定除外；

b) 在資料主體同意允許代表及授權的情況下，代表資料主體向其他組織或個人提供資料主體的個人資料，法律另有規定除外；

3. 資料主體的個人資料之提供由個人資料管控方、個人資料管控及處理方在資料主體提出請求後於72個小時內執行，法律另有規定除外。

4. 個人資料管控方、個人資料管控及處理方在下列情況下不提供個人資料：

a) 對國防、國家安全、社會秩序和安全造成危害；

b) 資料主體的個人資料之提供可能會影響他人的安全、身體或心理健康；

c) 資料主體不同意提供、不允許代表或授權接收個人資料。

5. 要求提供個人資料的形式：

a) 資料主體直接或授權他人前往個人資料管控方、個人資料管控及處理方之總部要求提供個人資料。

請求接收者有責任指導提出請求的組織、個人按《個人資料提供申請表》填寫內容。

如果提出請求的組織、個人是文盲或殘疾人，無法撰寫請求，則請求接收者有責任幫助填寫《個人資料提供申請表》的內容。

b) 依照本議定附錄的第1號、2號表格填寫內容並透過電子網絡、郵政服務、傳真向個人資料管控方、個人資料管控及處理方發送《個人資料提供申請表》。

6.《個人資料提供申請表》必須以越南語提交，包括以下主要內容：

a) 姓氏、名字；居所、地址；請求提出者的身份證號碼、公民身份證號碼或護照號碼；傳真、電話號碼、電子郵箱地址（如有）；

b) 對所要求提供的個人資料註明文件、檔案、資料的名稱；

c) 個人資料的提供形式；

d) 要求提供個人資料的理由、目的。

7. 如果要求提供本條第2款所規定的個人資料則必須附上有關的個人、組織的書面同意。

8. 接收個人資料的提供請求

a) 個人資料管控方、個人資料管控及處理方負責接收提供個人資料的請求，並根據請求監控個人資料的提供過程和清單；

b) 如果所請求的個人資料不屬於其權限範圍，收到請求的個人資料管控方、個人資料管控及處理方必須通知並對提出請求的組織或個人引導至主管機關或明確告知無法提供個人資料。

9. 處理個人資料的提供請求

在接收到合格的個人資料提供請求後，個人資料管控方、個人資料管控及處理方負責提供個人資料，並通知提供個人資料的期限、地點、形式；打印、複印、拍照及透過郵政服務發送信息和傳真（如有）的實際費用以及付款方式和期限；按照本條規定的順序和程序提供個人資料。

第15條：個人資料的修改

1. 資料主體：

a) 有權訪問以查閱、修改其已同意允許個人資料管控方、個人資料管控及處理方收集的個人資料，法律另有規定除外；

b) 如果因技術原因或其他原因無法直接修改，資料主體可要求個人資料管控方、個人資料管控及處理方修改其個人資料。

2. 個人資料管控方、個人資料管控及處理方在獲得資料主體同意後應盡快修改資料主體的個人資料或者按照專門法的規定進行修改。如果無法進行，則必須在收到資料主體的個人資料修改請求後於72個小時內通知資料主體。

3. 個人資料處理方、第三方在獲得個人資料管控方、個人資料管控及處理方的書面同意及明確知道資料主體已同意後，可以修改資料主體的個人資料。

第16條：個人資料的存儲、刪除及銷毀

1. 在下列情況下，資料主體可以要求個人資料管控方、個人資料管控及處理方刪除其個人資料：

a) 對已同意的收集目的不再認為是必要並接受要求刪除資料可能造成的損害；

b) 撤回同意；

c) 反對資料的處理且個人資料管控方、個人資料管控及處理方沒有充分的理由繼續處理；

d) 未按照約定目的處理個人資料或違法處理個人資料；

đ) 個人資料必須依法刪除。

2. 資料主體的請求在下列情況下不適用於資料的刪除；

a) 法律規定不允許刪除資料；

b) 由國家主管機關以服務國家機關依法運作為目的進行處理的個人資料；

c) 已依法公開的個人資料；

d) 依照法律規定以服務於法律、科研、統計目的來處理的個人資料；

đ) 在國防、國家安全、社會秩序與安全、重大災害、危險的流行病等緊急情況下；當存在威脅安全和國防的風險但未達到宣佈緊急狀態的程度時；防治騷亂、恐怖主義、打擊犯罪分子和違法行為；

e) 應對威脅資料主體或其他個人生命、健康或安全的緊急情況。

3. 如果進行企業分立、拆分、合併、整合或者解散則應當依法轉移個人資料。

4. 如果進行機關、組織、行政單位分立、拆分、合併及國有企業重組、轉換所有制形式則應當依法轉移個人資料。

5. 在資料主體對個人資料管控方、個人資料管控及處理方所收集之全部資料提出請求後應在72個小時內執行資料的刪除，法律另有規定除外。

6. 個人資料管控方、個人資料管控及處理方、個人資料處理方、第三方應以適合其活動的形式存儲個人資料並依法採取個人資料的保護措施。

7. 個人資料管控方、個人資料管控及處理方、個人資料處理方、第三方在下列情況可永久刪除資料：

a) 資料處理不當或已完成經資料主體同意的個人資料處理目的；

b) 個人資料管控方、個人資料管控及處理方、個人資料處理方、第三方的運營不再需要存儲個人資料；

c) 個人資料管控方、個人資料管控及處理方、個人資料處理方、第三方依法解散或不再運營或宣佈破產或被強制終止經營。

第17條：在不需要資料主體同意的情況下處理個人資料

1. 在發生緊急情況時，需要立即處理相關個人資料以保護資料主體或他人的生命和健康。個人資料管控方、個人資料處理方、個人資料管控及處理方、第三方負責證明該情況。

2. 依法公開個人資料。

3. 國家主管機關在國防、國家安全、社會秩序與安全、重大災害、危險的流行病等緊急情況下進行的資料處理；當存在威脅安全和國防的風險但未達到宣佈緊急狀態的程度時；防治騷亂、恐怖主義、打擊犯罪分子和違法行為。

4. 依法履行資料主體與有關機關、組織和個人的合同義務。

5. 依照專門法的規定，為國家機關的活動服務。

第18條：處理在公共場所以錄音、錄像活動獲得的個人資料

主管機關和組織為了維護國家安全、社會秩序與安全、法律規定的組織和個人的合法權益，可以在不需要獲得主體同意的情況下在公共場所進行錄音、錄像及處理透過錄音、錄像活動所獲得的個人資料。在進行錄音、錄像時，主管機關有責任告知當事人了解其被錄音、錄像的情況，法律另有規定除外。

第19條：處理被宣佈為失蹤者、死亡者的個人資料

1. 除了本議定第17條及第18條所規定的情況，處理與被宣佈為失蹤者、死亡者個人資料相關的個人資料時必須獲得其配偶或成年子女的同意，如果上述人等不存在則必須獲得被宣佈為失蹤者、死亡者父母的同意。

2 . 本條第1款所述人等均不存在則視為不同意。

第20條：處理兒童的個人資料

1. 兒童個人資料的處理始終遵循保護兒童權利和最大利益的原則。

2. 除了本議定第17條所規定的情況，處理年滿7周歲及以上年齡的兒童個人資料時必須獲得兒童的同意以及依法徵得其父母或監護人的同意。個人資料管控方、個人資料處理方、個人資料管控及處理方、第三方必須在進行處理兒童個人資料前核實兒童的年齡。

3. 在下列情況下，停止處理兒童個人資料，永久刪除或銷毀兒童個人資料：

a) 資料處理不當或已完成經資料主體同意的個人資料處理目的，法律另有規定除外；

b) 兒童的父母或監護人撤回其允許處理兒童個人資料的同意，法律另有規定除外；

c) 當有充分的依據證明個人資料的處理影響兒童的合法權益時應當配合主管機關的要求，法律另有規定除外。

第21條：營銷服務、介紹廣告產品業務中的個人資料保護

1. 經營營銷服務、介紹廣告產品的組織和個人，僅在徵得資料主體同意的情況下才可以將透過其業務活動所收集的客戶之個人資料用於營銷服務、介紹廣告產品的業務。

2. 在營銷服務、介紹廣告產品業務中處理客戶的個人資料必須在客戶清楚了解產品介紹的內容、方式、形式及頻率的基礎上徵得客戶的同意。

3. 經營營銷服務、介紹廣告產品的組織和個人有責任證明所推介產品的客戶個人資料的使用符合本條第1和第2款的規定。

第22條：違法收集、轉交、買賣個人資料

1. 個人資料處理的相關組織和個人必須採取個人資料保護措施以防止其服務系統、設備非法收集個人資料的情況。

2. 未經資料主體同意而設置軟件系統、技術措施或者組織收集、轉交、買賣個人資料的活動屬於違法行為。

第23條：關於違反個人資料保護規定的通知

1. 如果發現違反個人資料保護規定的行為，個人資料管控方、個人資料管控及處理方應當在發生本議定附錄第3號表單所載之違規行為後的72個小時內通知公安部（網絡安全及防治高科技犯罪分子局）。對於72個小時後的通知，必須附上延遲通知的原因。

2. 個人資料處理方當發現違反個人資料保護規定的行為後，必須盡快通知個人資料管控方。

3. 違反個人資料保護規定的通知內容：

a) 描述違反個人資料保護規定的性質，包括：時間、地點、行為、組織、個人、個人資料類型以及涉及的資料數量；

b) 指派保護資料的人員或負責保護個人資料的組織、個人的聯繫方式；

c) 描述違反個人資料保護規定可能造成的後果和損害；

d) 描述為解決和減少由違反個人資料保護規定引起的危害而採取的措施。

4. 如果本條第3款所規定的內容無法悉數通知則可以進行分批、分階段通知。

5. 個人資料管控方、個人資料管控及處理方必須對個人資料保護規定之違反行為的發生作出書面確認，並配合公安部（網絡安全及防治高科技犯罪分子局）處理違規行為。

6. 組織和個人當發現下列情況，應通報公安部（網絡安全及防治高科技犯罪分子局）：

a) 發現個人資料方面的違法行為；

b) 個人資料的處理目的不當，與資料主體和個人資料管控方、個人資料管控及處理方之間的原始約定不符或違反法律規定；

c) 資料主體的權利得不到保障或沒有正確落實；

d) 法律所規定的其他情況。

第3節：影響評估及向境外轉移個人資料

第24條：評估個人資料處理的影響

1. 個人資料管控方、個人資料管控及處理方應從開始處理個人資料時建立並貯存其處理個人資料的影響評估檔案。

個人資料管控方、個人資料管控及處理方的個人資料處理影響評估檔案包括：

a) 個人資料管控方、個人資料管控及處理方的資訊及聯繫方式；

b) 被指定執行個人資料保護任務的組織以及個人資料管控方、個人資料管控及處理方的個人資料保護官的姓名和聯繫方式;

c) 處理個人資料的目的；

d) 所處理的個人資料類型；

đ) 接收個人資料的組織和個人，包括越南境外的組織和個人；

e) 向境外轉移個人資料的情況；

g) 個人資料處理時間；刪除或銷毀個人資料的預計時間（如有）；

h) 所採用的個人資料保護措施的說明；

i) 評估個人資料處理的影響；後果、可能發生的不必要損害、減少或消除此類風險和損害的措施。

2. 個人資料處理方在與個人資料管控方履行合約時，應當建立並貯存個人資料處理的影響評估檔案。個人資料處理方的個人資料處理影響評估檔案包括：

a) 個人資料處理方的資訊和聯繫方式；

b) 被指定執行個人資料處理的組織以及個人資料處理方的個人資料處理人員的姓名和聯繫方式；

c) 依照與個人資料管控方簽訂的合約進行個人資料的處理活動及類型的描述；

d) 個人資料處理時間；刪除或銷毀個人資料的預計時間（如有）；

đ) 向境外轉移個人資料的情況；

e) 所採用的個人資料保護措施的一般說明；

g) 後果、可能發生的不必要損害、減少或消除此類風險和損害的措施。

3. 本條第1款和第2款所規定的個人資料處理影響評估檔案應當以個人資料管控方、個人資料管控及處理方或個人資料處理方的合法有效文件為建立依據。

4. 個人資料處理影響檔案應始終可用以服務公安部的檢查、評估活動以及在進行處理個人資料之日起60天內向公安部（網絡安全和防治高科技犯罪分子局）寄送1份依照本議定附錄第4號表單的原件。

5. 如果檔案不完整且符合規定，公安部（網絡安全和防治高科技犯罪分子局）將進行評估及要求個人資料管控方、個人資料管控及處理方、個人資料處理方完善個人資料處理影響評估檔案。

6. 個人資料管控方、個人資料管控及處理方、個人資料處理方應在已寄送至公安部（網絡安全和防治高科技犯罪分子局）的檔案內容（依照本議定附錄的第5號表單）發生變化時，對個人資料處理影響評估檔案進行更新、補充。

第25條：向境外轉移個人資料

1. 越南公民的個人資料在跨境資料轉移方已建立了向境外轉移個人資料之影響評估檔案並執行本條第3、4和5款規定程序的情況下可以向境外轉移。跨境資料轉移方包括個人資料管控方、個人資料管控及處理方、個人資料處理方、第三方。

2. 向境外轉移個人資料之影響評估檔案包括：

a) 越南公民個人資料的資料轉移方及資料接收方的資訊及聯繫方式；

b) 有關轉移和接收越南公民個人資料的資料轉移方之組織、負責人姓名和聯繫方式；

c) 描述並解釋越南公民的個人資料經轉移至境外後的資料處理活動之目的；

d) 描述並闡明轉移至境外的個人資料類型；

đ) 描述並明確表達遵守本議定的個人資料保護規定、詳細說明所採用的個人資料保護措施；

e) 評估個人資料處理的影響程度；可能產生的後果、不必要的損害；減少或消除此類風險或損害的措施；

g) 在資料主體充分了解出現問題或請求時的反饋、投訴機制的基礎上徵得本議定第11條規定的資料主體的同意。

h) 在轉移和接收越南公民個人資料的組織、個人之間應存在對處理個人資料具有表達約束和責任的書面文件。

3. 向境外轉移個人資料的影響評估檔案必須始終可用以服務公安部的檢查、評估活動。

向境外轉移資料的當事方應當自進行處理個人資料之日起60天內向公安部（網絡安全和防治高科技犯罪分子局）寄送1份依照本議定附錄第6號表單的正本檔案。

4. 在資料轉移成功後，資料轉移方應當將資料轉移的情況及負責的單位和個人之聯繫方式以書面形式通報至公安部（網絡安全和防治高科技犯罪分子局）。

5. 如果檔案不完整且符合規定，公安部（網絡安全和防治高科技犯罪分子局）將進行評估及要求向境外轉移資料的當事方完善向境外轉移個人資料影響評估檔案。

6. 向境外轉移資料的當事方應在已寄送至公安部（網絡安全和防治高科技犯罪分子局）的檔案內容（依照本議定附錄的第5號表單）發生變化時，對向境外轉移個人資料影響評估檔案進行更新、補充。向境外轉移資料的當事方完善檔案的期限為自要求之日起的10天內。

7. 根據具體情況，公安部決定對個人資料的境外轉移進行檢查的次數為1次/年。發現本議定所規定的違反個人資料保護法行為或發生越南公民個人資料的洩露、丟失事故的情況除外。

8. 在下列情況下，公安部決定要求向境外轉移資料的當事方停止向境外轉移個人資料：

a) 當發現所轉移的個人資料用於侵犯越南社會主義共和國的利益和國家安全的活動時；

b) 向境外轉移資料的當事方不遵守本條第5、第6款的規定；

c) 發生越南公民個人資料的洩露、丟失事故 。

第4節：個人資料保護的保障措施及條件

第26條：保護個人資料的措施

1. 個人資料保護措施適用於個人資料處理的開始以及整個處理過程。

2. 個人資料的保護措施包括：

a) 由參與個人資料處理的組織、個人執行的管理措施；

b) 由參與個人資料處理的組織、個人執行的技術措施

c) 由國家主管管理機關依照本議定和相關法律規定採取的措施；

d) 由國家主管機關執行的調查、訴訟措施；

đ) 法律規定的其他措施。

第27條：保護基本個人資料

1. 採用本議定第26條第2款所規定的措施。

2. 制定和發佈個人資料保護條例，明確需要依照本議定規定執行的事項。

3. 鼓勵採用適合個人資料處理相關領域、行業和活動的個人資料保護標準。

4. 在對存儲個人資料的設備進行處理、永久刪除或銷毀之前，應對服務於個人資料處理的系統、工具和設備進行網絡安全的檢查。

第28條：保護敏感個人資料

1. 採用本議定第26條第2款及第27條所規定的措施。

2. 指定具有個人資料保護職能的部門，指定個人資料保護負責人，並與保護個人資料的專門機構交換負責個人資料保護的部門、個人的資訊。如果個人資料管控方、個人資料管控和處理方、資料處理方、第三方是個人則進行交換執行人的個人信息。

3. 除本議定第13條第4款、第17條及第18條規定的情況外，應向資料主體通知資料主體的敏感個人資料已被處理。

第29條：個人資料保護的專門機構和國家個人資料保護門戶網站

1. 個人資料保護的專門機構是公安部 – 網絡安全和防治高科技犯罪分子局，負責協助公安部執行個人資料保護的國家管理工作。

2. 國家個人資料保護門戶網站：

a) 提供黨對個人資料保護的方針、路徑、政策資訊及國家對個人資料保護的法律資訊；

b) 宣傳和傳播有關個人資料保護的政策和法律；

c) 更新個人資料保護的資訊和情況；

d) 通過網絡空間接收有關個人資料保護活動的資訊、檔案和資料；

đ) 提供有關參與個人資料保護的機關、組織、個人的工作結果評估資訊；

e) 接收違反個人資料保護規定的通知；

g) 依法對侵犯個人資料的風險和行為進行警示及協助警示；

h) 依法處理違反個人資料保護的行為；

i) 依照個人資料保護法進行其他活動。

第30條：個人資料保護活動的保障條件

1. 保護個人資料的隊伍：

a) 從事個人資料保護的專門隊伍應在個人資料保護的專門機關設立；

b) 機關、組織、企業應指定具有個人資料保護職能的部門和人員以確保個人資料保護法規的實施；

c) 依號召參與個人資料保護的組織和個人；

d) 公安部制定具體的方案和計劃以發展個人資料保護的人力資源。

2. 機關、組織和個人有責任宣傳和傳播知識和技能，提高機關、組織和個人的個人資料保護意識。

3. 確保個人資料保護專門機構的設施和運營條件。

第31條：確保個人資料保護活動的資金

1. 實施個人資料保護的資金來源包括國家預算；國內外機關、組織和個人的支持；來自提供個人資料保護服務的收入；國際援助以及其他合法的收入來源。

2. 國家機關的個人資料保護經費由國家預算保障，並納入國家年度預算概算。國家預算資金的管理和使用必須遵守國家預算法。

3. 組織、企業的個人資料保護經費由組織、企業自行安排及按照規定落實。

第三章

機關、組織和個人的責任

第32條：公安部的責任

1. 協助政府對個人資料保護進行國家統一管理。

2. 指導和實施個人資料保護活動，保護資料主體的權利免受違反個人資料保護法行為的侵害，提出頒布個人資料保護標準和適用的建議。

3. 建立、管理和運營國家個人資料保護門戶網站。

4. 評估有關機構、組織和個人的個人資料保護工作結果。

5. 根據本議定的規定接收有關個人資料保護的檔案、表單和資訊。

6. 推動個人資料保護領域的創新措施和研究，開展個人資料保護的國際合作。

7. 依法稽查、檢查、處理投訴、舉報、處理違反個人資料保護規定的行為。

第33條：信息與傳媒部的責任

1. 指導媒體機構、通訊社、管理領域所屬組織和企業依照本議定的規定保護個人資料。

2. 根據被分配的職責任務，制定、指導和實施個人資料保護措施，保障信息通信活動中個人資料的網絡信息安全。

3. 配合公安部稽查、檢查和處理個人資料保護違法行為。

第34條：國防部的責任

按照法律規定和被分配的職責任務，對隸屬國防部的機構、組織和個人進行管理、稽查、檢查、監督、處理違規行為以及採用個人資料保護規定。

第35條：科學技術部的責任

1. 配合公安部制定個人資料保護標準以及適用個人資料保護標準的建議。

2. 與公安部就個人資料保護措施進行研究、交流，以適應科學、科技的發展情況。

第36條：各部委、部級機構、政府所屬機關的責任

1. 依照個人資料保護法的規定，對保護個人資料的管理部門及領域實施國家管理。

2. 制定並落實本議定的個人資料保護內容和任務。

3. 在制定、落實各部委的任務中對個人資料保護規定進行補充。

4. 依照現行的分級管理預算法規為個人資料保護活動分配資金。

5. 發佈符合個人資料保護規定的開放資料名錄

第37條：各省、直轄市人民委員會的責任

1. 依照個人資料保護法的規定，對保護個人資料的管理部門及領域實施國家管理。

2. 落實本議定有關個人資料保護的規定。

3. 依照現行的分級管理預算法規為個人資料保護活動分配資金。

4. 發佈符合個人資料保護規定的開放資料名錄

第38條：個人資料管控方的責任

1. 實施組織和技術措施以及適當的安全、保密措施，以證明資料處理活動已按照個人資料保護法的規定進行，並根據需要對這些措施進行檢查和更新。

2. 記錄並存儲個人資料處理過程的系統日誌。

3. 發出違反本議定第23條規定的個人資料保護條例的通知。

4. 選擇明確與任務相符的個人資料處理方並僅與具有適當保護措施的個人資料處理方合作。

5. 確保本議定第九條所規定的資料主體的權利。

6. 個人資料管控方就個人資料處理過程造成的損害對資料主體負責。

7. 在個人資料保護活動方面配合公安部及國家主管機關，為查處違反個人資料保護法行為提供資訊。

第39條：個人資料處理方的責任

1. 僅在與個人資料管控方簽訂資料處理合同或協議後才能接收個人資料。

2. 根據與個人資料管控方簽訂的合同或協議處理個人資料。

3. 全面落實本議定及其他相關法律文件規定的個人資料保護措施。

4. 個人資料處理方就個人資料處理過程造成的損害對資料主體負責。

5. 在資料處理完成後，刪除、向個人資料管控方返還所有個人資料。

6. 在個人資料保護活動方面配合公安部及國家主管機關，為查處違反個人資料保護法行為提供資訊。

第40條：資料管控及處理方的責任

全面遵守有關個人資料管控方和個人資料處理方職責的規定。

第41條：第三方的責任

全面遵守本議定所規定的個人資料處理責任規定。

第42條：相關組織和個人的責任

1. 採取保護自己個人資料的措施，並對所提供的個人資料的準確性負責。

2. 遵守本議定有關個人資料保護的規定。

3. 及時通知公安部有關個人資料保護活動的違規行為。

4. 配合公安部處理有關個人資料保護活動的違法行為。

第四章

執行條款

第43條：執行效力

1. 本議定自2023年07月01日起生效。

2. 微型企業、小型企業、中型企業和初創企業有權選擇在企業成立之日起的前兩年內免除指定個人資料保護的個人、部門的規定。

3. 直接從事個人資料處理活動的微型企業、小型企業、中型企業、初創企業不適用本條第二款的規定。

第44條：執行責任

1. 公安部部長督促、檢查、指導本議定的實施。

2. 部長、部級機關負責人、政府所屬機關負責人；省、直轄市人民委員會主席負責執行本議定。

收件處：
- 黨中央書記委員會；
- 總理、各政府副總理；
- 各部委、部級機關、政府所屬機關；
- 各省、直轄市人民議會、人民委員會；
- 中央辦公室及各黨委；
- 總書記辦公室；
- 國家主席辦公室；
- 國會的民族議會及委員會；
- 國會辦公室；
- 最高人民檢察院；
- 最高人民法院；
- 國家審計；
- 國家政策監察委員會；
- 社會政策銀行；
- 越南發展銀行；
- 越南祖國陣線中央委員會；
- 各團體的中央機關；
- 政府辦公室：主任、副主任、總理助理、電子信息門戶網站總經理、各司、局、直屬單位、公報；
- 存檔：文書、行政程序控制局(2b)TM.

代表政府
代替總理簽署
副總理
（已簽名蓋章）

陳留光

~ 恒利翻譯，謹供參考 ~

CHÍNH PHỦ **--------**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc** **----------**
Số: 13/2023/NĐ-CP	*Hà Nội, ngày 17 tháng 4 năm 2023*

NGHỊ ĐỊNH

BẢO VỆ DỮ LIỆU CÁ NHÂN

Căn cứ Luật Tổ chức Chính phủ ngày 19 tháng 6 năm 2015; Luật sửa đổi, bổ sung một số điều của Luật Tổ chức Chính phủ và Luật Tổ chức chính quyền địa phương ngày 22 tháng 11 năm 2019;

Căn cứ Bộ luật Dân sự ngày 24 tháng 11 năm 2015;

Căn cứ Luật An ninh quốc gia ngày 03 tháng 12 năm 2004;

Căn cứ Luật An ninh mạng ngày 12 tháng 6 năm 2018;

Theo đề nghị của Bộ trưởng Bộ Công an;

Chính phủ ban hành Nghị định bảo vệ dữ liệu cá nhân.

Chương I

NHỮNG QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh và đối tượng áp dụng

1. Nghị định này quy định về bảo vệ dữ liệu cá nhân và trách nhiệm bảo vệ dữ liệu cá nhân của cơ quan, tổ chức, cá nhân có liên quan.

2. Nghị định này áp dụng đối với:

a) Cơ quan, tổ chức, cá nhân Việt Nam;

b) Cơ quan, tổ chức, cá nhân nước ngoài tại Việt Nam;

c) Cơ quan, tổ chức, cá nhân Việt Nam hoạt động tại nước ngoài;

d) Cơ quan, tổ chức, cá nhân nước ngoài trực tiếp tham gia hoặc có liên quan đến hoạt động xử lý dữ liệu cá nhân tại Việt Nam.

Điều 2. Giải thích từ ngữ

Trong Nghị định này, các từ ngữ dưới đây được hiểu như sau:

1. Dữ liệu cá nhân là thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự trên môi trường điện tử gắn liền với một con người cụ thể hoặc giúp xác định một con người cụ thể. Dữ liệu cá nhân bao gồm dữ liệu cá nhân cơ bản và dữ liệu cá nhân nhạy cảm.

2. Thông tin giúp xác định một con người cụ thể là thông tin hình thành từ hoạt động của cá nhân mà khi kết hợp với các dữ liệu, thông tin lưu trữ khác có thể xác định một con người cụ thể.

3. Dữ liệu cá nhân cơ bản bao gồm:

a) Họ, chữ đệm và tên khai sinh, tên gọi khác (nếu có);

b) Ngày, tháng, năm sinh; ngày, tháng, năm chết hoặc mất tích;

c) Giới tính;

d) Nơi sinh, nơi đăng ký khai sinh, nơi thường trú, nơi tạm trú, nơi ở hiện tại, quê quán, địa chỉ liên hệ;

đ) Quốc tịch;

e) Hình ảnh của cá nhân;

g) Số điện thoại, số chứng minh nhân dân, số định danh cá nhân, số hộ chiếu, số giấy phép lái xe, số biển số xe, số mã số thuế cá nhân, số bảo hiểm xã hội, số thẻ bảo hiểm y tế;

h) Tình trạng hôn nhân;

i) Thông tin về mối quan hệ gia đình (cha mẹ, con cái);

k) Thông tin về tài khoản số của cá nhân; dữ liệu cá nhân phản ánh hoạt động, lịch sử hoạt động trên không gian mạng;

l) Các thông tin khác gắn liền với một con người cụ thể hoặc giúp xác định một con người cụ thể không thuộc quy định tại khoản 4 Điều này.

4. Dữ liệu cá nhân nhạy cảm là dữ liệu cá nhân gắn liền với quyền riêng tư của cá nhân mà khi bị xâm phạm sẽ gây ảnh hưởng trực tiếp tới quyền và lợi ích hợp pháp của cá nhân gồm:

a) Quan điểm chính trị, quan điểm tôn giáo;

b) Tình trạng sức khỏe và đời tư được ghi trong hồ sơ bệnh án, không bao gồm thông tin về nhóm máu;

c) Thông tin liên quan đến nguồn gốc chủng tộc, nguồn gốc dân tộc;

d) Thông tin về đặc điểm di truyền được thừa hưởng hoặc có được của cá nhân;

đ) Thông tin về thuộc tính vật lý, đặc điểm sinh học riêng của cá nhân;

e) Thông tin về đời sống tình dục, xu hướng tình dục của cá nhân;

g) Dữ liệu về tội phạm, hành vi phạm tội được thu thập, lưu trữ bởi các cơ quan thực thi pháp luật;

h) Thông tin khách hàng của tổ chức tín dụng, chi nhánh ngân hàng nước ngoài, tổ chức cung ứng dịch vụ trung gian thanh toán, các tổ chức được phép khác, gồm: thông tin định danh khách hàng theo quy định của pháp luật, thông tin về tài khoản, thông tin về tiền gửi, thông tin về tài sản gửi, thông tin về giao dịch, thông tin về tổ chức, cá nhân là bên bảo đảm tại tổ chức tín dụng, chi nhánh ngân hàng, tổ chức cung ứng dịch vụ trung gian thanh toán;

i) Dữ liệu về vị trí của cá nhân được xác định qua dịch vụ định vị;

k) Dữ liệu cá nhân khác được pháp luật quy định là đặc thù và cần có biện pháp bảo mật cần thiết.

5. Bảo vệ dữ liệu cá nhân là hoạt động phòng ngừa, phát hiện, ngăn chặn, xử lý hành vi vi phạm liên quan đến dữ liệu cá nhân theo quy định của pháp luật.

6. Chủ thể dữ liệu là cá nhân được dữ liệu cá nhân phản ánh.

7. Xử lý dữ liệu cá nhân là một hoặc nhiều hoạt động tác động tới dữ liệu cá nhân, như: thu thập, ghi, phân tích, xác nhận, lưu trữ, chỉnh sửa, công khai, kết hợp, truy cập, truy xuất, thu hồi, mã hóa, giải mã, sao chép, chia sẻ, truyền đưa, cung cấp, chuyển giao, xóa, hủy dữ liệu cá nhân hoặc các hành động khác có liên quan.

8. Sự đồng ý của chủ thể dữ liệu là việc thể hiện rõ ràng, tự nguyện, khẳng định việc cho phép xử lý dữ liệu cá nhân của chủ thể dữ liệu.

9. Bên Kiểm soát dữ liệu cá nhân là tổ chức, cá nhân quyết định mục đích và phương tiện xử lý dữ liệu cá nhân.

10. Bên Xử lý dữ liệu cá nhân là tổ chức, cá nhân thực hiện việc xử lý dữ liệu thay mặt cho Bên Kiểm soát dữ liệu, thông qua một hợp đồng hoặc thỏa thuận với Bên Kiểm soát dữ liệu.

11. Bên Kiểm soát và xử lý dữ liệu cá nhân là tổ chức, cá nhân đồng thời quyết định mục đích, phương tiện và trực tiếp xử lý dữ liệu cá nhân.

12. Bên thứ ba là tổ chức, cá nhân ngoài Chủ thể dữ liệu, Bên Kiểm soát dữ liệu cá nhân, Bên Xử lý dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân được phép xử lý dữ liệu cá nhân.

13. Xử lý dữ liệu cá nhân tự động là hình thức xử lý dữ liệu cá nhân được thực hiện bằng phương tiện điện tử nhằm đánh giá, phân tích, dự đoán hoạt động của một con người cụ thể, như: thói quen, sở thích, mức độ tin cậy, hành vi, địa điểm, xu hướng, năng lực và các trường hợp khác.

14. Chuyển dữ liệu cá nhân ra nước ngoài là hoạt động sử dụng không gian mạng, thiết bị, phương tiện điện tử hoặc các hình thức khác chuyển dữ liệu cá nhân của công dân Việt Nam tới một địa điểm nằm ngoài lãnh thổ của nước Cộng hòa xã hội chủ nghĩa Việt Nam hoặc sử dụng một địa điểm nằm ngoài lãnh thổ của nước Cộng hòa xã hội chủ nghĩa Việt Nam để xử lý dữ liệu cá nhân của công dân Việt Nam, bao gồm:

a) Tổ chức, doanh nghiệp, cá nhân chuyển dữ liệu cá nhân của công dân Việt Nam cho tổ chức, doanh nghiệp, bộ phận quản lý ở nước ngoài để xử lý phù hợp với mục đích đã được chủ thể dữ liệu đồng ý;

b) Xử lý dữ liệu cá nhân của công dân Việt Nam bằng các hệ thống tự động nằm ngoài lãnh thổ của nước Cộng hòa xã hội chủ nghĩa Việt Nam của Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân, Bên Xử lý dữ liệu cá nhân phù hợp với mục đích đã được chủ thể dữ liệu đồng ý.

Điều 3. Nguyên tắc bảo vệ dữ liệu cá nhân

1. Dữ liệu cá nhân được xử lý theo quy định của pháp luật.

2. Chủ thể dữ liệu được biết về hoạt động liên quan tới xử lý dữ liệu cá nhân của mình, trừ trường hợp luật có quy định khác.

3. Dữ liệu cá nhân chỉ được xử lý đúng với mục đích đã được Bên Kiểm soát dữ liệu cá nhân, Bên Xử lý dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân, Bên thứ ba đăng ký, tuyên bố về xử lý dữ liệu cá nhân.

4. Dữ liệu cá nhân thu thập phải phù hợp và giới hạn trong phạm vi, mục đích cần xử lý. Dữ liệu cá nhân không được mua, bán dưới mọi hình thức, trừ trường hợp luật có quy định khác.

5. Dữ liệu cá nhân được cập nhật, bổ sung phù hợp với mục đích xử lý.

6. Dữ liệu cá nhân được áp dụng các biện pháp bảo vệ, bảo mật trong quá trình xử lý, bao gồm cả việc bảo vệ trước các hành vi vi phạm quy định về bảo vệ dữ liệu cá nhân và phòng, chống sự mất mát, phá hủy hoặc thiệt hại do sự cố, sử dụng các biện pháp kỹ thuật.

7. Dữ liệu cá nhân chỉ được lưu trữ trong khoảng thời gian phù hợp với mục đích xử lý dữ liệu, trừ trường hợp pháp luật có quy định khác.

8. Bên Kiểm soát dữ liệu, Bên Kiểm soát và xử lý dữ liệu cá nhân phải chịu trách nhiệm tuân thủ các nguyên tắc xử lý dữ liệu được quy định từ khoản 1 tới khoản 7 Điều này và chứng minh sự tuân thủ của mình với các nguyên tắc xử lý dữ liệu đó.

Điều 4. Xử lý vi phạm quy định bảo vệ dữ liệu cá nhân

Cơ quan, tổ chức, cá nhân vi phạm quy định bảo vệ dữ liệu cá nhân tùy theo mức độ có thể bị xử lý kỷ luật, xử phạt vi phạm hành chính, xử lý hình sự theo quy định.

Điều 5. Quản lý nhà nước về bảo vệ dữ liệu cá nhân

Chính phủ thống nhất quản lý nhà nước về bảo vệ dữ liệu cá nhân.

Nội dung quản lý nhà nước về bảo vệ dữ liệu cá nhân gồm:

1. Trình cơ quan nhà nước có thẩm quyền ban hành hoặc ban hành theo thẩm quyền văn bản quy phạm pháp luật và chỉ đạo, tổ chức thực hiện văn bản quy phạm pháp luật về bảo vệ dữ liệu cá nhân.

2. Xây dựng và tổ chức thực hiện chiến lược, chính sách, đề án, dự án, chương trình, kế hoạch về bảo vệ dữ liệu cá nhân.

3. Hướng dẫn cơ quan, tổ chức, cá nhân về biện pháp, quy trình, tiêu chuẩn bảo vệ dữ liệu cá nhân theo quy định của pháp luật.

4. Tuyên truyền, giáo dục pháp luật về bảo vệ dữ liệu cá nhân; truyền thông, phổ biến kiến thức, kỹ năng bảo vệ dữ liệu cá nhân.

5. Xây dựng, đào tạo, bồi dưỡng cán bộ, công chức, viên chức và người được giao làm công tác bảo vệ dữ liệu cá nhân.

6. Thanh tra, kiểm tra việc thực hiện quy định của pháp luật về bảo vệ dữ liệu cá nhân; giải quyết khiếu nại, tố cáo và xử lý vi phạm pháp luật về bảo vệ dữ liệu cá nhân theo quy định của pháp luật.

7. Thống kê, thông tin, báo cáo về tình hình bảo vệ dữ liệu cá nhân và việc thực hiện pháp luật về bảo vệ dữ liệu cá nhân cho cơ quan nhà nước có thẩm quyền.

8. Hợp tác quốc tế về bảo vệ dữ liệu cá nhân.

Điều 6. Áp dụng Nghị định bảo vệ dữ liệu cá nhân, các luật liên quan và Điều ước quốc tế

Việc bảo vệ dữ liệu cá nhân được thực hiện theo quy định các điều ước quốc tế mà nước Cộng hòa xã hội chủ nghĩa Việt Nam là thành viên, các quy định khác của Luật có liên quan và Nghị định này.

Điều 7. Hợp tác quốc tế về bảo vệ dữ liệu cá nhân

1. Xây dựng cơ chế hợp tác quốc tế để tạo điều kiện cho việc thực thi có hiệu quả pháp luật về bảo vệ dữ liệu cá nhân.

2. Tham gia tương trợ tư pháp về bảo vệ dữ liệu cá nhân của các quốc gia khác, bao gồm thông báo, đề nghị khiếu nại, trợ giúp điều tra và trao đổi thông tin, với các biện pháp bảo vệ thích hợp để bảo vệ dữ liệu cá nhân.

3. Tổ chức các hội nghị, hội thảo, nghiên cứu khoa học và thúc đẩy các hoạt động hợp tác quốc tế trong việc thực thi pháp luật để bảo vệ dữ liệu cá nhân.

4. Tổ chức các cuộc gặp song phương, đa phương, trao đổi kinh nghiệm xây dựng pháp luật và thực tiễn bảo vệ dữ liệu cá nhân.

5. Chuyển giao công nghệ phục vụ bảo vệ dữ liệu cá nhân.

Điều 8. Hành vi bị nghiêm cấm

1. Xử lý dữ liệu cá nhân trái với quy định của pháp luật về bảo vệ dữ liệu cá nhân.

2. Xử lý dữ liệu cá nhân để tạo ra thông tin, dữ liệu nhằm chống lại Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam.

3. Xử lý dữ liệu cá nhân để tạo ra thông tin, dữ liệu gây ảnh hưởng tới an ninh quốc gia, trật tự an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân khác.

4. Cản trở hoạt động bảo vệ dữ liệu cá nhân của cơ quan có thẩm quyền.

5. Lợi dụng hoạt động bảo vệ dữ liệu cá nhân để vi phạm pháp luật.

Chương II

HOẠT ĐỘNG BẢO VỆ DỮ LIỆU CÁ NHÂN

Mục 1. QUYỀN VÀ NGHĨA VỤ CỦA CHỦ THỂ DỮ LIỆU

Điều 9. Quyền của chủ thể dữ liệu

1. Quyền được biết

Chủ thể dữ liệu được biết về hoạt động xử lý dữ liệu cá nhân của mình, trừ trường hợp luật có quy định khác.

2. Quyền đồng ý

Chủ thể dữ liệu được đồng ý hoặc không đồng ý cho phép xử lý dữ liệu cá nhân của mình, trừ trường hợp quy định tại Điều 17 Nghị định này.

3. Quyền truy cập

Chủ thể dữ liệu được truy cập để xem, chỉnh sửa hoặc yêu cầu chỉnh sửa dữ liệu cá nhân của mình, trừ trường hợp luật có quy định khác.

4. Quyền rút lại sự đồng ý

Chủ thể dữ liệu được quyền rút lại sự đồng ý của mình, trừ trường hợp luật có quy định khác.

5. Quyền xóa dữ liệu

Chủ thể dữ liệu được xóa hoặc yêu cầu xóa dữ liệu cá nhân của mình, trừ trường hợp luật có quy định khác.

6. Quyền hạn chế xử lý dữ liệu

a) Chủ thể dữ liệu được yêu cầu hạn chế xử lý dữ liệu cá nhân của mình, trừ trường hợp luật có quy định khác;

b) Việc hạn chế xử lý dữ liệu được thực hiện trong 72 giờ sau khi có yêu cầu của chủ thể dữ liệu, với toàn bộ dữ liệu cá nhân mà chủ thể dữ liệu yêu cầu hạn chế, trừ trường hợp luật có quy định khác.

7. Quyền cung cấp dữ liệu

Chủ thể dữ liệu được yêu cầu Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân cung cấp cho bản thân dữ liệu cá nhân của mình, trừ trường hợp luật có quy định khác.

8. Quyền phản đối xử lý dữ liệu

a) Chủ thể dữ liệu được phản đối Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân xử lý dữ liệu cá nhân của mình nhằm ngăn chặn hoặc hạn chế tiết lộ dữ liệu cá nhân hoặc sử dụng cho mục đích quảng cáo, tiếp thị, trừ trường hợp luật có quy định khác;

b) Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân thực hiện yêu cầu của chủ thể dữ liệu trong 72 giờ sau khi nhận được yêu cầu, trừ trường hợp luật có quy định khác.

9. Quyền khiếu nại, tố cáo, khởi kiện

Chủ thể dữ liệu có quyền khiếu nại, tố cáo hoặc khởi kiện theo quy định của pháp luật.

10. Quyền yêu cầu bồi thường thiệt hại

Chủ thể dữ liệu có quyền yêu cầu bồi thường thiệt hại theo quy định của pháp luật khi xảy ra vi phạm quy định về bảo vệ dữ liệu cá nhân của mình, trừ trường hợp các bên có thỏa thuận khác hoặc luật có quy định khác.

11. Quyền tự bảo vệ

Chủ thể dữ liệu có quyền tự bảo vệ theo quy định của Bộ luật Dân sự, luật khác có liên quan và Nghị định này, hoặc yêu cầu cơ quan, tổ chức có thẩm quyền thực hiện các phương thức bảo vệ quyền dân sự theo quy định tại Điều 11 Bộ luật Dân sự.

Điều 10. Nghĩa vụ của chủ thể dữ liệu

1. Tự bảo vệ dữ liệu cá nhân của mình; yêu cầu các tổ chức, cá nhân khác có liên quan bảo vệ dữ liệu cá nhân của mình.

2. Tôn trọng, bảo vệ dữ liệu cá nhân của người khác.

3. Cung cấp đầy đủ, chính xác dữ liệu cá nhân khi đồng ý cho phép xử lý dữ liệu cá nhân.

4. Tham gia tuyên truyền, phổ biến kỹ năng bảo vệ dữ liệu cá nhân.

5. Thực hiện quy định của pháp luật về bảo vệ dữ liệu cá nhân và tham gia phòng, chống các hành vi vi phạm quy định về bảo vệ dữ liệu cá nhân.

Mục 2. BẢO VỆ DỮ LIỆU CÁ NHÂN TRONG QUÁ TRÌNH XỬ LÝ DỮ LIỆU CÁ NHÂN

Điều 11. Sự đồng ý của chủ thể dữ liệu

1. Sự đồng ý của chủ thể dữ liệu được áp dụng đối với tất cả các hoạt động trong quy trình xử lý dữ liệu cá nhân, trừ trường hợp luật có quy định khác.

2. Sự đồng ý của chủ thể dữ liệu chỉ có hiệu lực khi chủ thể dữ liệu tự nguyện và biết rõ các nội dung sau:

a) Loại dữ liệu cá nhân được xử lý;

b) Mục đích xử lý dữ liệu cá nhân;

c) Tổ chức, cá nhân được xử lý dữ liệu cá nhân;

d) Các quyền, nghĩa vụ của chủ thể dữ liệu.

3. Sự đồng ý của chủ thể dữ liệu phải được thể hiện rõ ràng, cụ thể bằng văn bản, giọng nói, đánh dấu vào ô đồng ý, cú pháp đồng ý qua tin nhắn, chọn các thiết lập kỹ thuật đồng ý hoặc qua một hành động khác thể hiện được điều này.

4. Sự đồng ý phải được tiến hành cho cùng một mục đích. Khi có nhiều mục đích, Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân liệt kê các mục đích để chủ thể dữ liệu đồng ý với một hoặc nhiều mục đích nêu ra.

5. Sự đồng ý của chủ thể dữ liệu phải được thể hiện ở một định dạng có thể được in, sao chép bằng văn bản, bao gồm cả dưới dạng điện tử hoặc định dạng kiểm chứng được.

6. Sự im lặng hoặc không phản hồi của chủ thể dữ liệu không được coi là sự đồng ý.

7. Chủ thể dữ liệu có thể đồng ý một phần hoặc với điều kiện kèm theo.

8. Đối với xử lý dữ liệu cá nhân nhạy cảm, chủ thể dữ liệu phải được thông báo rằng dữ liệu cần xử lý là dữ liệu cá nhân nhạy cảm.

9. Sự đồng ý của chủ thể dữ liệu có hiệu lực cho tới khi chủ thể dữ liệu có quyết định khác hoặc khi cơ quan nhà nước có thẩm quyền yêu cầu bằng văn bản.

10. Trong trường hợp có tranh chấp, trách nhiệm chứng minh sự đồng ý của chủ thể dữ liệu thuộc về Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân.

11. Thông qua việc ủy quyền theo quy định của Bộ luật Dân sự, tổ chức, cá nhân có thể thay mặt chủ thể dữ liệu thực hiện các thủ tục liên quan tới xử lý dữ liệu cá nhân của chủ thể dữ liệu với Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân trong trường hợp chủ thể dữ liệu đã biết rõ và đồng ý theo quy định tại khoản 3 Điều này, trừ trường hợp luật có quy định khác.

Điều 12. Rút lại sự đồng ý

1. Việc rút lại sự đồng ý không ảnh hưởng đến tính hợp pháp của việc xử lý dữ liệu đã được đồng ý trước khi rút lại sự đồng ý.

2. Việc rút lại sự đồng ý phải được thể hiện ở một định dạng có thể được in, sao chép bằng văn bản, bao gồm cả dưới dạng điện tử hoặc định dạng kiểm chứng được.

3. Khi nhận yêu cầu rút lại sự đồng ý của chủ thể dữ liệu, Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân thông báo cho chủ thể dữ liệu về hậu quả, thiệt hại có thể xảy ra khi rút lại sự đồng ý.

4. Sau khi thực hiện quy định tại khoản 2 Điều này, Bên Kiểm soát dữ liệu, Bên Xử lý dữ liệu, Bên

Kiểm soát và xử lý dữ liệu, Bên thứ ba phải ngừng và yêu cầu các tổ chức, cá nhân có liên quan ngừng xử lý dữ liệu của chủ thể dữ liệu đã rút lại sự đồng ý.

Điều 13. Thông báo xử lý dữ liệu cá nhân

1. Việc thông báo được thực hiện một lần trước khi tiến hành đối với hoạt động xử lý dữ liệu cá nhân.

2. Nội dung thông báo cho chủ thể dữ liệu về xử lý dữ liệu cá nhân:

a) Mục đích xử lý;

b) Loại dữ liệu cá nhân được sử dụng có liên quan tới mục đích xử lý quy định tại điểm a khoản 2 Điều này;

c) Cách thức xử lý;

d) Thông tin về các tổ chức, cá nhân khác có liên quan tới mục đích xử lý quy định tại điểm a khoản 2 Điều này;

đ) Hậu quả, thiệt hại không mong muốn có khả năng xảy ra;

e) Thời gian bắt đầu, thời gian kết thúc xử lý dữ liệu.

3. Việc thông báo cho chủ thể dữ liệu phải được thể hiện ở một định dạng có thể được in, sao chép bằng văn bản, bao gồm cả dưới dạng điện tử hoặc định dạng kiểm chứng được.

4. Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân không cần thực hiện quy định tại khoản 1 Điều này trong các trường hợp sau:

a) Chủ thể dữ liệu đã biết rõ và đồng ý toàn bộ với nội dung quy định tại khoản 1 và khoản 2 Điều này trước khi đồng ý cho Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân tiến hành thu thập dữ liệu cá nhân, phù hợp với các quy định tại Điều 9 Nghị định này;

b) Dữ liệu cá nhân được xử lý bởi cơ quan nhà nước có thẩm quyền với mục đích phục vụ hoạt động của cơ quan nhà nước theo quy định của pháp luật.

Điều 14. Cung cấp dữ liệu cá nhân

1. Chủ thể dữ liệu được yêu cầu Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân cung cấp cho bản thân dữ liệu cá nhân của mình.

2. Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân:

a) Được cung cấp dữ liệu cá nhân của chủ thể dữ liệu cho tổ chức, cá nhân khác khi có sự đồng ý của chủ thể dữ liệu, trừ trường hợp pháp luật có quy định khác;

b) Thay mặt chủ thể dữ liệu cung cấp dữ liệu cá nhân của chủ thể dữ liệu cho tổ chức hoặc cá nhân khác khi chủ thể dữ liệu đồng ý cho phép đại diện và ủy quyền, trừ trường hợp pháp luật có quy định khác.

3. Việc cung cấp dữ liệu cá nhân của chủ thể dữ liệu được Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân thực hiện trong 72 giờ sau khi có yêu cầu của chủ thể dữ liệu, trừ trường hợp luật có quy định khác.

4. Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân không cung cấp dữ liệu cá nhân trong trường hợp:

a) Gây tổn hại tới quốc phòng, an ninh quốc gia, trật tự an toàn xã hội;

b) Việc cung cấp dữ liệu cá nhân của chủ thể dữ liệu có thể ảnh hưởng tới sự an toàn, sức khỏe thể chất hoặc tinh thần của người khác;

c) Chủ thể dữ liệu không đồng ý cung cấp, cho phép đại diện hoặc ủy quyền nhận dữ liệu cá nhân.

5. Hình thức yêu cầu cung cấp dữ liệu cá nhân:

a) Chủ thể dữ liệu trực tiếp hoặc ủy quyền cho người khác đến trụ sở Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân yêu cầu cung cấp dữ liệu cá nhân.

Người tiếp nhận yêu cầu có trách nhiệm hướng dẫn tổ chức, cá nhân yêu cầu điền các nội dung vào Phiếu yêu cầu cung cấp dữ liệu cá nhân.

Trường hợp tổ chức, cá nhân yêu cầu cung cấp thông tin không biết chữ hoặc bị khuyết tật không thể viết yêu cầu thì người tiếp nhận yêu cầu cung cấp thông tin có trách nhiệm giúp điền các nội dung vào Phiếu yêu cầu cung cấp dữ liệu cá nhân;

b) Gửi Phiếu yêu cầu cung cấp dữ liệu cá nhân theo Mẫu số 01, 02 tại Phụ lục của Nghị định này qua mạng điện tử, dịch vụ bưu chính, fax đến Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân.

6. Phiếu yêu cầu cung cấp dữ liệu cá nhân phải được thể hiện bằng tiếng Việt gồm các nội dung chính sau đây:

a) Họ, tên; nơi cư trú, địa chỉ; số chứng minh nhân dân, thẻ căn cước công dân hoặc số hộ chiếu của người yêu cầu; số fax, điện thoại, địa chỉ thư điện tử (nếu có);

b) Dữ liệu cá nhân được yêu cầu cung cấp, trong đó chỉ rõ tên văn bản, hồ sơ, tài liệu;

c) Hình thức cung cấp dữ liệu cá nhân;

d) Lý do, mục đích yêu cầu cung cấp dữ liệu cá nhân.

7. Trường hợp yêu cầu cung cấp dữ liệu cá nhân quy định tại khoản 2 Điều này thì phải kèm theo văn bản đồng ý của cá nhân, tổ chức liên quan.

8. Tiếp nhận yêu cầu cung cấp dữ liệu cá nhân

a) Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân có trách nhiệm tiếp nhận yêu cầu cung cấp dữ liệu cá nhân và theo dõi quá trình, danh sách cung cấp dữ liệu cá nhân theo yêu cầu;

b) Trường hợp dữ liệu cá nhân được yêu cầu không thuộc thẩm quyền thì Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân nhận được yêu cầu phải thông báo và hướng dẫn tổ chức, cá nhân yêu cầu đến cơ quan có thẩm quyền hoặc thông báo rõ ràng việc không thể cung cấp dữ liệu cá nhân.

9. Giải quyết yêu cầu cung cấp dữ liệu cá nhân

Khi nhận được yêu cầu cung cấp dữ liệu cá nhân hợp lệ, Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân có trách nhiệm cung cấp dữ liệu cá nhân thông báo về thời hạn, địa điểm, hình thức cung cấp dữ liệu cá nhân; chi phí thực tế để in, sao, chụp, gửi thông tin qua dịch vụ bưu chính, fax (nếu có) và phương thức, thời hạn thanh toán; thực hiện việc cung cấp dữ liệu cá nhân theo trình tự, thủ tục quy định tại Điều này.

Điều 15. Chỉnh sửa dữ liệu cá nhân

1. Chủ thể dữ liệu:

a) Được truy cập để xem, chỉnh sửa dữ liệu cá nhân của mình sau khi đã được Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân thu thập theo sự đồng ý, trừ trường hợp luật có quy định khác;

b) Trường hợp không thể chỉnh sửa trực tiếp vì lý do kỹ thuật hoặc vì lý do khác, chủ thể dữ liệu yêu cầu Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân chỉnh sửa dữ liệu cá nhân của mình.

2. Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân chỉnh sửa dữ liệu cá nhân của chủ thể dữ liệu sau khi được chủ thể dữ liệu cá nhân đồng ý ngay khi có thể hoặc theo quy định của pháp luật chuyên ngành. Trường hợp không thể thực hiện thì thông báo tới chủ thể dữ liệu sau 72

giờ kể khi nhận được yêu cầu chỉnh sửa dữ liệu cá nhân của chủ thể dữ liệu.

3. Bên Xử lý dữ liệu cá nhân, Bên thứ ba được chỉnh sửa dữ liệu cá nhân của chủ thể dữ liệu sau khi được Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân đồng ý bằng văn bản và biết rõ rằng đã có sự đồng ý của chủ thể dữ liệu.

Điều 16. Lưu trữ, xóa, hủy dữ liệu cá nhân

1. Chủ thể dữ liệu được yêu cầu Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân xóa dữ liệu cá nhân của mình trong các trường hợp sau:

a) Nhận thấy không còn cần thiết cho mục đích thu thập đã đồng ý và chấp nhận các thiệt hại có thể xảy ra khi yêu cầu xóa dữ liệu;

b) Rút lại sự đồng ý;

c) Phản đối việc xử lý dữ liệu và Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân không có lý do chính đáng để tiếp tục xử lý;

d) Dữ liệu cá nhân được xử lý không đúng với mục đích đã đồng ý hoặc việc xử lý dữ liệu cá nhân là vi phạm quy định của pháp luật;

đ) Dữ liệu cá nhân phải xóa theo quy định của pháp luật.

2. Việc xóa dữ liệu sẽ không áp dụng khi có đề nghị của chủ thể dữ liệu trong các trường hợp:

a) Pháp luật quy định không cho phép xóa dữ liệu;

b) Dữ liệu cá nhân được xử lý bởi cơ quan nhà nước có thẩm quyền với mục đích phục vụ hoạt động của cơ quan nhà nước theo quy định của pháp luật;

c) Dữ liệu cá nhân đã được công khai theo quy định của pháp luật;

d) Dữ liệu cá nhân được xử lý nhằm phục vụ yêu cầu pháp lý, nghiên cứu khoa học, thống kê theo quy định của pháp luật;

đ) Trong trường hợp tình trạng khẩn cấp về quốc phòng, an ninh quốc gia, trật tự an toàn xã hội, thảm họa lớn, dịch bệnh nguy hiểm; khi có nguy cơ đe dọa an ninh, quốc phòng nhưng chưa đến mức ban bố tình trạng khẩn cấp; phòng, chống bạo loạn, khủng bố, phòng, chống tội phạm và vi phạm pháp luật;

e) Ứng phó với tình huống khẩn cấp đe dọa đến tính mạng, sức khỏe hoặc sự an toàn của chủ thể dữ liệu hoặc cá nhân khác.

3. Trường hợp doanh nghiệp chia, tách, sáp nhập, hợp nhất, giải thể thì dữ liệu cá nhân được chuyển giao theo quy định của pháp luật.

4. Trường hợp chia, tách, sáp nhập cơ quan, tổ chức, đơn vị hành chính và tổ chức lại, chuyển đổi hình thức sở hữu doanh nghiệp nhà nước thì dữ liệu cá nhân được chuyển giao theo quy định của pháp luật.

5. Việc xóa dữ liệu được thực hiện trong 72 giờ sau khi có yêu cầu của chủ thể dữ liệu với toàn bộ dữ liệu cá nhân mà Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân thu thập được, trừ trường hợp pháp luật có quy định khác.

6. Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân, Bên Xử lý dữ liệu cá nhân, Bên thứ ba lưu trữ dữ liệu cá nhân theo hình thức phù hợp với hoạt động của mình và có biện pháp bảo vệ dữ liệu cá nhân theo quy định của pháp luật.

7. Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân, Bên Xử lý dữ liệu cá nhân, Bên thứ ba xóa không thể khôi phục trong trường hợp:

a) Xử lý dữ liệu không đúng mục đích hoặc đã hoàn thành mục đích xử lý dữ liệu cá nhân được chủ thể dữ liệu đồng ý;

b) Việc lưu trữ dữ liệu cá nhân không còn cần thiết với hoạt động của Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân, Bên Xử lý dữ liệu cá nhân, Bên thứ ba;

c) Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân, Bên Xử lý dữ liệu cá nhân, Bên thứ ba bị giải thể hoặc không còn hoạt động hoặc tuyên bố phá sản hoặc bị chấm dứt hoạt động kinh doanh theo quy định của pháp luật.

Điều 17. Xử lý dữ liệu cá nhân trong trường hợp không cần sự đồng ý của chủ thể dữ liệu

1. Trong trường hợp khẩn cấp, cần xử lý ngay dữ liệu cá nhân có liên quan để bảo vệ tính mạng, sức khỏe của chủ thể dữ liệu hoặc người khác. Bên Kiểm soát dữ liệu cá nhân, Bên Xử lý dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân, Bên thứ ba có trách nhiệm chứng minh trường hợp này.

2. Việc công khai dữ liệu cá nhân theo quy định của luật.

3. Việc xử lý dữ liệu của cơ quan nhà nước có thẩm quyền trong trường hợp tình trạng khẩn cấp về quốc phòng, an ninh quốc gia, trật tự an toàn xã hội, thảm họa lớn, dịch bệnh nguy hiểm; khi có nguy cơ đe dọa an ninh, quốc phòng nhưng chưa đến mức ban bố tình trạng khẩn cấp; phòng, chống bạo loạn, khủng bố, phòng, chống tội phạm và vi phạm pháp luật theo quy định của luật.

4. Để thực hiện nghĩa vụ theo hợp đồng của chủ thể dữ liệu với cơ quan, tổ chức, cá nhân có liên quan theo quy định của luật.

5. Phục vụ hoạt động của cơ quan nhà nước đã được quy định theo luật chuyên ngành.

Điều 18. Xử lý dữ liệu cá nhân thu được từ hoạt động ghi âm, ghi hình tại nơi công cộng

Cơ quan, tổ chức có thẩm quyền được ghi âm, ghi hình và xử lý dữ liệu cá nhân thu được từ hoạt động ghi âm, ghi hình tại nơi công cộng với mục đích bảo vệ an ninh quốc gia, trật tự an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân theo quy định của pháp luật mà không cần có sự đồng ý của chủ thể. Khi thực hiện việc ghi âm, ghi hình, cơ quan, tổ chức có thẩm quyền có trách nhiệm thông báo để chủ thể hiểu được mình đang bị ghi âm, ghi hình, trừ trường hợp pháp luật có quy định khác.

Điều 19. Xử lý dữ liệu cá nhân của người bị tuyên bố mất tích, đã chết

1. Việc xử lý dữ liệu cá nhân liên quan đến dữ liệu cá nhân của người bị tuyên bố mất tích, người đã chết phải được sự đồng ý của vợ, chồng hoặc con thành niên của người đó, trường hợp không có những người này thì phải được sự đồng ý của cha, mẹ của người bị tuyên bố mất tích, người đã chết, trừ trường hợp quy định tại Điều 17 và Điều 18 Nghị định này.

2. Trường hợp không có tất cả những người được nêu tại khoản 1 Điều này thì được coi là không có sự đồng ý.

Điều 20. Xử lý dữ liệu cá nhân của trẻ em

1. Xử lý dữ liệu cá nhân của trẻ em luôn được thực hiện theo nguyên tắc bảo vệ các quyền và vì lợi ích tốt nhất của trẻ em.

2. Việc xử lý dữ liệu cá nhân của trẻ em phải có sự đồng ý của trẻ em trong trường hợp trẻ em từ đủ 7 tuổi trở lên và có sự đồng ý của cha, mẹ hoặc người giám hộ theo quy định, trừ trường hợp quy định tại Điều 17 Nghị định này. Bên Kiểm soát dữ liệu cá nhân, Bên Xử lý dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân, Bên thứ ba phải xác minh tuổi của trẻ em trước khi xử lý dữ liệu cá nhân của trẻ em.

3. Ngừng xử lý dữ liệu cá nhân của trẻ em, xóa không thể khôi phục hoặc hủy dữ liệu cá nhân của trẻ em trong trường hợp:

a) Xử lý dữ liệu không đúng mục đích hoặc đã hoàn thành mục đích xử lý dữ liệu cá nhân được chủ thể dữ liệu đồng ý, trừ trường hợp pháp luật có quy định khác;

b) Cha, mẹ hoặc người giám hộ của trẻ em rút lại sự đồng ý cho phép xử lý dữ liệu cá nhân của trẻ em, trừ trường hợp pháp luật có quy định khác;

c) Theo yêu cầu của cơ quan chức năng có thẩm quyền khi có đủ căn cứ chứng minh việc xử lý dữ liệu cá nhân gây ảnh hưởng tới quyền và lợi ích hợp pháp của trẻ em, trừ trường hợp pháp luật có quy định khác.

Điều 21. Bảo vệ dữ liệu cá nhân trong kinh doanh dịch vụ tiếp thị, giới thiệu sản phẩm quảng cáo

1. Tổ chức, cá nhân kinh doanh dịch vụ tiếp thị, giới thiệu sản phẩm quảng cáo chỉ được sử dụng dữ liệu cá nhân của khách hàng được thu thập qua hoạt động kinh doanh của mình để kinh doanh dịch vụ tiếp thị, giới thiệu sản phẩm quảng cáo khi có sự đồng ý của chủ thể dữ liệu.

2. Việc xử lý dữ liệu cá nhân của khách hàng để kinh doanh dịch vụ tiếp thị, giới thiệu sản phẩm quảng cáo phải được sự đồng ý của khách hàng, trên cơ sở khách hàng biết rõ nội dung, phương thức, hình thức, tần suất giới thiệu sản phẩm.

3. Tổ chức, cá nhân kinh doanh dịch vụ tiếp thị, giới thiệu sản phẩm quảng cáo có trách nhiệm chứng minh việc sử dụng dữ liệu cá nhân của khách hàng được giới thiệu sản phẩm đúng với quy định tại khoản 1 và khoản 2 Điều này.

Điều 22. Thu thập, chuyển giao, mua, bán trái phép dữ liệu cá nhân

1. Tổ chức, cá nhân có liên quan tới xử lý dữ liệu cá nhân phải áp dụng các biện pháp bảo vệ dữ liệu cá nhân để ngăn chặn tình trạng thu thập dữ liệu cá nhân trái phép từ hệ thống, trang thiết bị dịch vụ của mình.

2. Việc thiết lập các hệ thống phần mềm, biện pháp kỹ thuật hoặc tổ chức các hoạt động thu thập, chuyển giao, mua, bán dữ liệu cá nhân không có sự đồng ý của chủ thể dữ liệu là vi phạm pháp luật.

Điều 23. Thông báo vi phạm quy định về bảo vệ dữ liệu cá nhân

1. Trường hợp phát hiện xảy ra vi phạm quy định bảo vệ dữ liệu cá nhân, Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân thông báo cho Bộ Công an (Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) chậm nhất 72 giờ sau khi xảy ra hành vi vi phạm theo Mẫu số 03 tại Phụ lục của Nghị định này. Trường hợp thông báo sau 72 giờ thì phải kèm theo lý do thông báo chậm, muộn.

2. Bên Xử lý dữ liệu cá nhân phải thông báo cho Bên Kiểm soát dữ liệu cá nhân một cách nhanh nhất có thể sau khi nhận thấy có sự vi phạm quy định về bảo vệ dữ liệu cá nhân.

3. Nội dung thông báo vi phạm quy định về bảo vệ dữ liệu cá nhân:

a) Mô tả tính chất của việc vi phạm quy định bảo vệ dữ liệu cá nhân, bao gồm: thời gian, địa điểm, hành vi, tổ chức, cá nhân, các loại dữ liệu cá nhân và số lượng dữ liệu liên quan;

b) Chi tiết liên lạc của nhân viên được giao nhiệm vụ bảo vệ dữ liệu hoặc tổ chức, cá nhân chịu trách nhiệm bảo vệ dữ liệu cá nhân;

c) Mô tả các hậu quả, thiệt hại có thể xảy ra của việc vi phạm quy định bảo vệ dữ liệu cá nhân;

d) Mô tả các biện pháp được đưa ra để giải quyết, giảm thiểu tác hại của hành vi vi phạm quy định bảo vệ dữ liệu cá nhân.

4. Trường hợp không thể thông báo đầy đủ các nội dung quy định tại khoản 3 Điều này, việc thông báo có thể được thực hiện theo từng đợt, từng giai đoạn.

5. Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân phải lập Biên bản xác nhận về việc xảy ra hành vi vi phạm quy định bảo vệ dữ liệu cá nhân, phối hợp với Bộ Công an (Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) xử lý hành vi vi phạm.

6. Tổ chức, cá nhân thông báo cho Bộ Công an (Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) khi phát hiện các trường hợp sau:

a) Phát hiện hành vi vi phạm pháp luật đối với dữ liệu cá nhân;

b) Dữ liệu cá nhân bị xử lý sai mục đích, không đúng thỏa thuận ban đầu giữa chủ thể dữ liệu và Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân hoặc vi phạm quy định của pháp luật;

c) Không bảo đảm quyền của chủ thể dữ liệu hoặc không được thực hiện đúng;

d) Trường hợp khác theo quy định của pháp luật.

Mục 3. ĐÁNH GIÁ TÁC ĐỘNG VÀ CHUYỂN DỮ LIỆU CÁ NHÂN RA NƯỚC NGOÀI

Điều 24. Đánh giá tác động xử lý dữ liệu cá nhân

1. Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân lập và lưu giữ Hồ sơ đánh giá tác động xử lý dữ liệu cá nhân của mình kể từ thời điểm bắt đầu xử lý dữ liệu cá nhân.

Hồ sơ đánh giá tác động xử lý dữ liệu cá nhân của Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân, bao gồm:

a) Thông tin và chi tiết liên lạc của Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân;

b) Họ tên, chi tiết liên lạc của tổ chức được phân công thực hiện nhiệm vụ bảo vệ dữ liệu cá nhân và nhân viên bảo vệ dữ liệu cá nhân của Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân;

c) Mục đích xử lý dữ liệu cá nhân;

d) Các loại dữ liệu cá nhân được xử lý;

đ) Tổ chức, cá nhân nhận dữ liệu cá nhân, bao gồm tổ chức, cá nhân ngoài lãnh thổ Việt Nam;

e) Trường hợp chuyển dữ liệu cá nhân ra nước ngoài;

g) Thời gian xử lý dữ liệu cá nhân; thời gian dự kiến để xóa, hủy dữ liệu cá nhân (nếu có);

h) Mô tả về các biện pháp bảo vệ dữ liệu cá nhân được áp dụng;

i) Đánh giá mức độ ảnh hưởng của việc xử lý dữ liệu cá nhân; hậu quả, thiệt hại không mong muốn có khả năng xảy ra, các biện pháp giảm thiểu hoặc loại bỏ nguy cơ, tác hại đó.

2. Bên Xử lý dữ liệu cá nhân tiến hành lập và lưu giữ Hồ sơ đánh giá tác động xử lý dữ liệu cá nhân trong trường hợp thực hiện hợp đồng với Bên Kiểm soát dữ liệu cá nhân. Hồ sơ đánh giá tác động xử lý dữ liệu cá nhân của Bên Xử lý dữ liệu cá nhân, bao gồm:

a) Thông tin và chi tiết liên lạc của Bên Xử lý dữ liệu cá nhân;

b) Họ tên, chi tiết liên lạc của tổ chức được phân công thực hiện xử lý dữ liệu cá nhân và nhân viên thực hiện xử lý dữ liệu cá nhân của Bên Xử lý dữ liệu cá nhân;

c) Mô tả các hoạt động xử lý và các loại dữ liệu cá nhân được xử lý theo hợp đồng với Bên Kiểm soát dữ liệu cá nhân;

d) Thời gian xử lý dữ liệu cá nhân; thời gian dự kiến để xóa, hủy dữ liệu cá nhân (nếu có);

đ) Trường hợp chuyển dữ liệu cá nhân ra nước ngoài;

e) Mô tả chung về các biện pháp bảo vệ dữ liệu cá nhân được áp dụng;

g) Hậu quả, thiệt hại không mong muốn có khả năng xảy ra, các biện pháp giảm thiểu hoặc loại bỏ nguy cơ, tác hại đó.

3. Hồ sơ đánh giá tác động xử lý dữ liệu cá nhân quy định tại khoản 1 và khoản 2 Điều này được xác lập bằng văn bản có giá trị pháp lý của Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân hoặc Bên Xử lý dữ liệu cá nhân.

4. Hồ sơ đánh giá tác động xử lý dữ liệu cá nhân phải luôn có sẵn để phục vụ hoạt động kiểm tra, đánh

giá của Bộ Công an và gửi Bộ Công an (Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) 01 bản chính theo Mẫu số 04 tại Phụ lục của Nghị định này trong thời gian 60 ngày kể từ ngày tiến hành xử lý dữ liệu cá nhân.

5. Bộ Công an (Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) đánh giá, yêu cầu Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân, Bên Xử lý dữ liệu cá nhân hoàn thiện Hồ sơ đánh giá tác động xử lý dữ liệu cá nhân trong trường hợp hồ sơ chưa đầy đủ và đúng quy định.

6. Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân, Bên Xử lý dữ liệu cá nhân cập nhật, bổ sung Hồ sơ đánh giá tác động xử lý dữ liệu cá nhân khi có sự thay đổi về nội dung hồ sơ đã gửi cho Bộ Công an (Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) theo Mẫu số 05 tại Phụ lục của Nghị định này.

Điều 25. Chuyển dữ liệu cá nhân ra nước ngoài

1. Dữ liệu cá nhân của công dân Việt Nam được chuyển ra nước ngoài trong trường hợp Bên chuyển dữ liệu ra nước ngoài lập Hồ sơ đánh giá tác động chuyển dữ liệu cá nhân ra nước ngoài và thực hiện các thủ tục theo quy định tại khoản 3, 4 và 5 Điều này. Bên chuyển dữ liệu ra nước ngoài bao gồm Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân, Bên Xử lý dữ liệu cá nhân, Bên thứ ba.

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

a) Thông tin và chi tiết liên lạc của Bên chuyển dữ liệu và Bên tiếp nhận dữ liệu cá nhân của công dân Việt Nam;

b) Họ tên, chi tiết liên lạc của tổ chức, cá nhân phụ trách của Bên chuyển dữ liệu có liên quan tới việc chuyển và tiếp nhận dữ liệu cá nhân của công dân Việt Nam;

c) Mô tả và luận giải mục tiêu của các hoạt động xử lý dữ liệu cá nhân của Công dân Việt Nam sau khi được chuyển ra nước ngoài;

d) Mô tả và làm rõ loại dữ liệu cá nhân chuyển ra nước ngoài;

đ) Mô tả và nêu rõ sự tuân thủ quy định bảo vệ dữ liệu cá nhân tại Nghị định này, chi tiết các biện pháp bảo vệ dữ liệu cá nhân được áp dụng;

e) Đánh giá mức độ ảnh hưởng của việc xử lý dữ liệu cá nhân; hậu quả, thiệt hại không mong muốn có khả năng xảy ra, các biện pháp giảm thiểu hoặc loại bỏ nguy cơ, tác hại đó;

g) Sự đồng ý của chủ thể dữ liệu theo quy định tại Điều 11 Nghị định này trên cơ sở biết rõ cơ chế phản hồi, khiếu nại khi có sự cố hoặc yêu cầu phát sinh;

h) Có văn bản thể hiện sự ràng buộc, trách nhiệm giữa các tổ chức, cá nhân chuyển và nhận dữ liệu cá nhân của Công dân Việt Nam về việc xử lý dữ liệu cá nhân.

3. Hồ sơ đánh giá tác động chuyển dữ liệu cá nhân ra nước ngoài phải luôn có sẵn để phục vụ hoạt động kiểm tra, đánh giá của Bộ Công an.

Bên chuyển dữ liệu ra nước ngoài gửi 01 bản chính hồ sơ tới Bộ Công an (Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) theo Mẫu số 06 tại Phụ lục của Nghị định này trong thời gian 60 ngày kể từ ngày tiến hành xử lý dữ liệu cá nhân.

4. Bên chuyển dữ liệu thông báo gửi Bộ Công an (Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) thông tin về việc chuyển dữ liệu và chi tiết liên lạc của tổ chức, cá nhân phụ trách bằng văn bản sau khi việc chuyển dữ liệu diễn ra thành công.

5. Bộ Công an (Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) đánh giá, yêu cầu Bên chuyển dữ liệu ra nước ngoài hoàn thiện Hồ sơ đánh giá tác động chuyển dữ liệu cá nhân ra nước ngoài trong trường hợp hồ sơ chưa đầy đủ và đúng quy định.

6. Bên chuyển dữ liệu ra nước ngoài cập nhật, bổ sung Hồ sơ đánh giá tác động chuyển dữ liệu cá nhân ra nước ngoài khi có sự thay đổi về nội dung hồ sơ đã gửi cho Bộ Công an (Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) theo Mẫu số 05 tại Phụ lục của Nghị định này. Thời gian hoàn thiện hồ sơ dành cho Bên chuyển dữ liệu ra nước ngoài là 10 ngày kể từ ngày yêu cầu.

7. Căn cứ tình hình cụ thể, Bộ Công an quyết định việc kiểm tra chuyển dữ liệu cá nhân ra nước ngoài 01 lần/năm, trừ trường hợp phát hiện hành vi vi phạm quy định của pháp luật về bảo vệ dữ liệu cá nhân tại Nghị định này hoặc để xảy ra sự cố lộ, mất dữ liệu cá nhân của công dân Việt Nam.

8. Bộ Công an quyết định yêu cầu Bên chuyển dữ liệu ra nước ngoài ngừng chuyển dữ liệu cá nhân ra nước ngoài trong trường hợp:

a) Khi phát hiện dữ liệu cá nhân được chuyển được sử dụng vào hoạt động vi phạm lợi ích, an ninh quốc gia của nước Cộng hòa xã hội chủ nghĩa Việt Nam;

b) Bên chuyển dữ liệu ra nước ngoài không chấp hành quy định tại khoản 5, khoản 6 Điều này;

c) Để xảy ra sự cố lộ, mất dữ liệu cá nhân của công dân Việt Nam.

Mục 4. BIỆN PHÁP, ĐIỀU KIỆN BẢO ĐẢM BẢO VỆ DỮ LIỆU CÁ NHÂN

Điều 26. Biện pháp bảo vệ dữ liệu cá nhân

1. Biện pháp bảo vệ dữ liệu cá nhân được áp dụng ngay từ khi bắt đầu và trong suốt quá trình xử lý dữ liệu cá nhân.

2. Các biện pháp bảo vệ dữ liệu cá nhân, bao gồm:

a) Biện pháp quản lý do tổ chức, cá nhân có liên quan tới xử lý dữ liệu cá nhân thực hiện;

b) Biện pháp kỹ thuật do tổ chức, cá nhân có liên quan tới xử lý dữ liệu cá nhân thực hiện;

c) Biện pháp do cơ quan quản lý nhà nước có thẩm quyền thực hiện theo quy định của Nghị định này và pháp luật có liên quan;

d) Biện pháp điều tra, tố tụng do cơ quan nhà nước có thẩm quyền thực hiện;

đ) Các biện pháp khác theo quy định của pháp luật.

Điều 27. Bảo vệ dữ liệu cá nhân cơ bản

1. Áp dụng các biện pháp được quy định tại khoản 2 Điều 26 Nghị định này.

2. Xây dựng, ban hành các quy định về bảo vệ dữ liệu cá nhân, nêu rõ những việc cần thực hiện theo quy định của Nghị định này.

3. Khuyến khích áp dụng các tiêu chuẩn bảo vệ dữ liệu cá nhân phù hợp với lĩnh vực, ngành nghề, hoạt động có liên quan tới xử lý dữ liệu cá nhân.

4. Kiểm tra an ninh mạng đối với hệ thống và phương tiện, thiết bị phục vụ xử lý dữ liệu cá nhân trước khi xử lý, xóa không thể khôi phục được hoặc hủy các thiết bị chứa dữ liệu cá nhân.

Điều 28. Bảo vệ dữ liệu cá nhân nhạy cảm

1. Áp dụng các biện pháp được quy định tại khoản 2 Điều 26 và Điều 27 Nghị định này.

2. Chỉ định bộ phận có chức năng bảo vệ dữ liệu cá nhân, chỉ định nhân sự phụ trách bảo vệ dữ liệu cá nhân và trao đổi thông tin về bộ phận và cá nhân phụ trách bảo vệ dữ liệu cá nhân với Cơ quan chuyên trách bảo vệ dữ liệu cá nhân. Trường hợp Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân, Bên Xử lý dữ liệu, Bên thứ ba là cá nhân thì trao đổi thông tin của cá nhân thực hiện.

3. Thông báo cho chủ thể dữ liệu biết việc dữ liệu cá nhân nhạy cảm của chủ thể dữ liệu được xử lý, trừ trường hợp quy định tại khoản 4 Điều 13, Điều 17 và Điều 18 Nghị định này.

Điều 29. Cơ quan chuyên trách bảo vệ dữ liệu cá nhân và Cổng thông tin quốc gia về bảo vệ dữ liệu cá nhân

1. Cơ quan chuyên trách bảo vệ dữ liệu cá nhân là Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao - Bộ Công an, có trách nhiệm giúp Bộ Công an thực hiện quản lý nhà nước về bảo vệ dữ liệu cá nhân.

2. Cổng thông tin quốc gia về bảo vệ dữ liệu cá nhân:

a) Cung cấp thông tin về chủ trương, đường lối, chính sách của Đảng, pháp luật của Nhà nước về bảo vệ dữ liệu cá nhân;

b) Tuyên truyền, phổ biến chính sách, pháp luật về bảo vệ dữ liệu cá nhân;

c) Cập nhật thông tin, tình hình bảo vệ dữ liệu cá nhân;

d) Tiếp nhận thông tin, hồ sơ, dữ liệu về hoạt động bảo vệ dữ liệu cá nhân qua không gian mạng;

đ) Cung cấp thông tin về kết quả đánh giá công tác bảo vệ dữ liệu cá nhân của cơ quan, tổ chức, cá nhân có liên quan;

e) Tiếp nhận thông báo vi phạm quy định về bảo vệ dữ liệu cá nhân;

g) Cảnh báo, phối hợp cảnh báo về nguy cơ, hành vi xâm phạm dữ liệu cá nhân theo quy định của pháp luật;

h) Xử lý vi phạm về bảo vệ dữ liệu cá nhân theo quy định của pháp luật;

i) Thực hiện hoạt động khác theo quy định của pháp luật về bảo vệ dữ liệu cá nhân.

Điều 30. Điều kiện bảo đảm hoạt động bảo vệ dữ liệu cá nhân

1. Lực lượng bảo vệ dữ liệu cá nhân:

a) Lực lượng chuyên trách bảo vệ dữ liệu cá nhân được bố trí tại Cơ quan chuyên trách bảo vệ dữ liệu cá nhân;

b) Bộ phận, nhân sự có chức năng bảo vệ dữ liệu cá nhân được chỉ định trong cơ quan, tổ chức, doanh nghiệp nhằm bảo đảm thực hiện quy định về bảo vệ dữ liệu cá nhân;

c) Tổ chức, cá nhân được huy động tham gia bảo vệ dữ liệu cá nhân;

d) Bộ Công an xây dựng chương trình, kế hoạch cụ thể nhằm phát triển nguồn nhân lực bảo vệ dữ liệu cá nhân.

2. Cơ quan, tổ chức, cá nhân có trách nhiệm tuyên truyền, phổ biến kiến thức, kỹ năng, nâng cao nhận thức bảo vệ dữ liệu cá nhân cho cơ quan, tổ chức, cá nhân.

3. Bảo đảm cơ sở vật chất, điều kiện hoạt động cho Cơ quan chuyên trách bảo vệ dữ liệu cá nhân.

Điều 31. Kinh phí bảo đảm hoạt động bảo vệ dữ liệu cá nhân

1. Nguồn tài chính thực hiện bảo vệ dữ liệu cá nhân bao gồm ngân sách nhà nước; ủng hộ của cơ quan, tổ chức, cá nhân trong và ngoài nước; nguồn thu từ hoạt động cung cấp dịch vụ bảo vệ dữ liệu cá nhân; viện trợ quốc tế và các nguồn thu hợp pháp khác.

2. Kinh phí bảo vệ dữ liệu cá nhân của cơ quan nhà nước do ngân sách nhà nước bảo đảm, được bố trí trong dự toán ngân sách nhà nước hằng năm. Việc quản lý, sử dụng kinh phí từ ngân sách nhà nước được thực hiện theo quy định của pháp luật về ngân sách nhà nước.

3. Kinh phí bảo vệ dữ liệu cá nhân của tổ chức, doanh nghiệp do các tổ chức, doanh nghiệp tự bố trí và thực hiện theo quy định.

Chương III

TRÁCH NHIỆM CỦA CƠ QUAN, TỔ CHỨC, CÁ NHÂN

Điều 32. Trách nhiệm của Bộ Công an

1. Giúp Chính phủ thống nhất thực hiện quản lý nhà nước về bảo vệ dữ liệu cá nhân.

2. Hướng dẫn, triển khai hoạt động bảo vệ dữ liệu cá nhân, bảo vệ quyền của chủ thể dữ liệu trước các hành vi vi phạm quy định của pháp luật về bảo vệ dữ liệu cá nhân, đề xuất ban hành Tiêu chuẩn bảo vệ dữ liệu cá nhân và các khuyến nghị áp dụng.

3. Xây dựng, quản lý, vận hành Cổng thông tin quốc gia về bảo vệ dữ liệu cá nhân.

4. Đánh giá kết quả công tác bảo vệ dữ liệu cá nhân của cơ quan, tổ chức, cá nhân có liên quan.

5. Tiếp nhận hồ sơ, biểu mẫu, thông tin về bảo vệ dữ liệu cá nhân theo quy định tại Nghị định này.

6. Thúc đẩy các biện pháp và thực hiện nghiên cứu để đổi mới trong lĩnh vực bảo vệ dữ liệu cá nhân, triển khai hợp tác quốc tế về bảo vệ dữ liệu cá nhân.

7. Thanh tra, kiểm tra, giải quyết khiếu nại, tố cáo, xử lý hành vi vi phạm quy định về bảo vệ dữ liệu cá nhân theo quy định của pháp luật

Điều 33. Trách nhiệm của Bộ Thông tin và Truyền thông

1. Chỉ đạo các cơ quan truyền thông, báo chí, tổ chức và doanh nghiệp thuộc lĩnh vực quản lý thực hiện bảo vệ dữ liệu cá nhân theo quy định tại Nghị định này.

2. Xây dựng, hướng dẫn và triển khai các biện pháp bảo vệ dữ liệu cá nhân, bảo đảm an toàn thông tin mạng đối với dữ liệu cá nhân trong các hoạt động thông tin và truyền thông theo chức năng, nhiệm vụ được giao.

3. Phối hợp với Bộ Công an trong thanh tra, kiểm tra, xử lý vi phạm pháp luật về bảo vệ dữ liệu cá nhân.

Điều 34. Trách nhiệm của Bộ Quốc phòng

Quản lý, thanh tra, kiểm tra, giám sát, xử lý vi phạm và áp dụng các quy định bảo vệ dữ liệu cá nhân đối với các cơ quan, tổ chức, cá nhân thuộc phạm vi quản lý của Bộ Quốc phòng theo quy định pháp luật và chức năng, nhiệm vụ được giao.

Điều 35. Trách nhiệm của Bộ Khoa học và Công nghệ

1. Phối hợp với Bộ Công an trong xây dựng Tiêu chuẩn bảo vệ dữ liệu cá nhân và các khuyến nghị áp dụng Tiêu chuẩn bảo vệ dữ liệu cá nhân.

2. Nghiên cứu, trao đổi Bộ Công an về các biện pháp bảo vệ dữ liệu cá nhân theo kịp sự phát triển của khoa học, công nghệ.

Điều 36. Trách nhiệm của bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ

1. Thực hiện quản lý nhà nước đối với bảo vệ dữ liệu cá nhân đối với các ngành, lĩnh vực quản lý theo quy định của pháp luật về bảo vệ dữ liệu cá nhân.

2. Xây dựng và triển khai các nội dung, nhiệm vụ bảo vệ dữ liệu cá nhân tại Nghị định này.

3. Bổ sung các quy định bảo vệ dữ liệu cá nhân trong xây dựng, triển khai các nhiệm vụ của các bộ, ngành.

4. Bố trí kinh phí phục vụ hoạt động bảo vệ dữ liệu cá nhân theo phân cấp quản lý ngân sách hiện hành.

5. Ban hành Danh mục dữ liệu mở phù hợp với quy định bảo vệ dữ liệu cá nhân.

Điều 37. Trách nhiệm của Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương

1. Thực hiện quản lý nhà nước đối với bảo vệ dữ liệu cá nhân đối với các ngành, lĩnh vực quản lý theo quy định của pháp luật về bảo vệ dữ liệu cá nhân.

2. Triển khai các quy định về bảo vệ dữ liệu cá nhân tại Nghị định này.

3. Bố trí kinh phí phục vụ hoạt động bảo vệ dữ liệu cá nhân theo phân cấp quản lý ngân sách hiện hành.

4. Ban hành Danh mục dữ liệu mở phù hợp với quy định bảo vệ dữ liệu cá nhân.

Điều 38. Trách nhiệm của Bên Kiểm soát dữ liệu cá nhân

1. Thực hiện các biện pháp tổ chức và kỹ thuật cùng các biện pháp an toàn, bảo mật phù hợp để chứng minh các hoạt động xử lý dữ liệu đã được thực hiện theo quy định của pháp luật về bảo vệ dữ liệu cá nhân, rà soát và cập nhật các biện pháp này khi cần thiết.

2. Ghi lại và lưu trữ nhật ký hệ thống quá trình xử lý dữ liệu cá nhân.

3. Thông báo hành vi vi phạm quy định về bảo vệ dữ liệu cá nhân theo quy định tại Điều 23 Nghị định này.

4. Lựa chọn Bên Xử lý dữ liệu cá nhân phù hợp với nhiệm vụ rõ ràng và chỉ làm việc với Bên Xử lý dữ liệu cá nhân có các biện pháp bảo vệ phù hợp.

5. Bảo đảm các quyền của chủ thể dữ liệu theo quy định tại Điều 9 Nghị định này.

6. Bên Kiểm soát dữ liệu cá nhân chịu trách nhiệm trước chủ thể dữ liệu về các thiệt hại do quá trình xử lý dữ liệu cá nhân gây ra.

7. Phối hợp với Bộ Công an, cơ quan nhà nước có thẩm quyền trong bảo vệ dữ liệu cá nhân, cung cấp thông tin phục vụ điều tra, xử lý hành vi vi phạm quy định của pháp luật về bảo vệ dữ liệu cá nhân.

Điều 39. Trách nhiệm của Bên Xử lý dữ liệu cá nhân

1. Chỉ tiếp nhận dữ liệu cá nhân sau khi có hợp đồng hoặc thỏa thuận về xử lý dữ liệu với Bên Kiểm soát dữ liệu cá nhân.

2. Xử lý dữ liệu cá nhân theo đúng hợp đồng hoặc thỏa thuận ký kết với Bên Kiểm soát dữ liệu cá nhân.

3. Thực hiện đầy đủ các biện pháp bảo vệ dữ liệu cá nhân quy định tại Nghị định này và các văn bản pháp luật khác có liên quan.

4. Bên Xử lý dữ liệu cá nhân chịu trách nhiệm trước chủ thể dữ liệu về các thiệt hại do quá trình xử lý dữ liệu cá nhân gây ra.

5. Xóa, trả lại toàn bộ dữ liệu cá nhân cho Bên Kiểm soát dữ liệu cá nhân sau khi kết thúc xử lý dữ liệu.

6. Phối hợp với Bộ Công an, cơ quan nhà nước có thẩm quyền trong bảo vệ dữ liệu cá nhân, cung cấp thông tin phục vụ điều tra, xử lý hành vi vi phạm quy định của pháp luật về bảo vệ dữ liệu cá nhân.

Điều 40. Trách nhiệm của Bên Kiểm soát và xử lý dữ liệu

Thực hiện đầy đủ các quy định về trách nhiệm của Bên Kiểm soát dữ liệu cá nhân và Bên Xử lý dữ liệu cá nhân.

Điều 41. Trách nhiệm của Bên thứ Ba

Thực hiện đầy đủ các quy định về trách nhiệm xử lý dữ liệu cá nhân theo quy định tại Nghị định này.

Điều 42. Trách nhiệm của tổ chức, cá nhân có liên quan

1. Có biện pháp bảo vệ dữ liệu cá nhân của mình, chịu trách nhiệm về tính chính xác của dữ liệu cá nhân do mình cung cấp.

2. Thực hiện quy định về bảo vệ dữ liệu cá nhân tại Nghị định này.

3. Thông báo kịp thời cho Bộ Công an về những vi phạm liên quan tới hoạt động bảo vệ dữ liệu cá

nhân.

4. Phối hợp với Bộ Công an trong xử lý những vi phạm liên quan tới hoạt động bảo vệ dữ liệu cá nhân.

Chương IV

ĐIỀU KHOẢN THI HÀNH

Điều 43. Hiệu lực thi hành

1. Nghị định này có hiệu lực thi hành từ ngày 01 tháng 7 năm 2023.

2. Các doanh nghiệp siêu nhỏ, doanh nghiệp nhỏ, doanh nghiệp vừa, doanh nghiệp khởi nghiệp được quyền lựa chọn miễn trừ quy định về chỉ định cá nhân và bộ phận bảo vệ dữ liệu cá nhân trong thời gian 02 năm đầu kể từ khi thành lập doanh nghiệp.

3. Các doanh nghiệp siêu nhỏ, doanh nghiệp nhỏ, doanh nghiệp vừa, doanh nghiệp khởi nghiệp trực tiếp kinh doanh hoạt động xử lý dữ liệu cá nhân không áp dụng quy định tại khoản 2 Điều này.

Điều 44. Trách nhiệm thi hành

1. Bộ trưởng Bộ Công an đôn đốc, kiểm tra, hướng dẫn việc thực hiện Nghị định này.

2. Bộ trưởng, Thủ trưởng cơ quan ngang bộ, Thủ trưởng cơ quan thuộc Chính phủ, Chủ tịch Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương chịu trách nhiệm thi hành Nghị định này./.

Nơi nhận:
- Ban Bí thư Trung ương Đảng;
- Thủ tướng, các Phó Thủ tướng Chính phủ;
- Các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ;
- HĐND, UBND các tỉnh, thành phố trực thuộc trung ương;
- Văn phòng Trung ương và các Ban của Đảng;
- Văn phòng Tổng Bí thư;
- Văn phòng Chủ tịch nước;
- Hội đồng Dân tộc và các Ủy ban của Quốc hội;
- Văn phòng Quốc hội;
- Viện kiểm sát nhân dân tối cao;
- Tòa án nhân dân tối cao;
- Kiểm toán nhà nước;
- Ủy ban Giám sát tài chính Quốc gia;
- Ngân hàng Chính sách xã hội;
- Ngân hàng Phát triển Việt Nam;
- Ủy ban trung ương Mặt trận Tổ quốc Việt Nam;
- Cơ quan trung ương của các đoàn thể;
- VPCP: BTCN, các PCN, Trợ lý TTg, TGĐ Cổng TTĐT, các Vụ, Cục, đơn vị trực thuộc, Công báo;
- Lưu: VT, KSTT (2b)TM.

TM. CHÍNH PHỦ
KT. THỦ TƯỚNG
PHÓ THỦ TƯỚNG

Trần Lưu Quang