

议定
个人资料保护

根据2015年06月19日《政府组织法》；于2019年11月22日修订和补充若干条款之《政府组织法》和《地方政府组织法》；

根据2015年11月24日《民事法》；

根据2004年12月03日《国家安全法》

根据2018年06月12日《网路安全法》；

根据公安部部长的提议；

政府颁行个人资料保护议定

第一章

总则

第1条：调整范围及适用对象

1. 本议定规定了对个人资料的保护及与个人资料保护相关之机关、组织和个人之责任。
2. 本议定适用于：
 - a) 越南机关、组织及个人；
 - b) 在越南之外国机关、组织及个人；
 - c) 在国外开展业务的越南机构、组织和个人
 - d) 直接参与或涉及越南个人资料处理活动的外国机构、组织和个人。

第2条：词语解释

在本议定中，下列术语的解释如下：

1. 个人资料是以符号、文字、数字、图像、声音等形式存在于电子存储介质上，与特定个人相关联或有助于识别特定个人的信息。个人资料包括基本个人资料及敏感个人资料。
2. 有助于识别特定个人的信息是透过个人活动与其他存储资料、信息相结合而形成之信息，其可以识别特定个人。
3. 基本个人资料包括：
 - a) 姓氏，中间名及出生登记名字及其他名字（如有）；

- b) 出生日期；死亡或失踪日期；
- c) 性别；
- d) 出生地、出生登记地、常住地、暂住地、现居住地、籍贯、联系地址；
- đ) 国籍；
- e) 个人照片；
- g) 电话号码、身份证号码、个人识别码、护照号码、驾照号码、车牌号码、个人纳税识别号、社会保险号码、医疗保险卡号码；
- h) 婚姻状况；
- i) 亲属的相关信息（父母、子女）；
- k) 有关个人数字账户的信息；反映网络空间的活动及活动历史记录的个人资料；
- l) 与特定人相关联或有助于识别特定人的其他信息不属于本条第4款所规定之范围。

4. 敏感个人资料是指与个人隐私相关的个人资料，其一旦受到侵犯将直接影响到个人的合法权益，包括：

- a) 政治观点、宗教观点；
- b) 病历中记载的健康状况及隐私，不包括血型信息；
- c) 有关民族、族裔血统的信息；
- d) 有关个人所继承或拥有的遗传特征之信息；
- đ) 有关个人的身体属性及生物特征的信息；
- e) 有关个人性生活或性取向的信息；
- g) 由执法机构收集和存储关于犯罪和违法行为的资料；
- h) 信贷机构、外国银行分行、支付中介服务机构及其他授权机构的客户信息，包括：法律规定的客户身份识别信息、账户信息、存款信息、存入资产信息、交易信息；作为信贷机构、银行分行、支付中介服务机构担保方的组织及个人信息；
- i) 透过定位服务识别的个人位置数据；
- k) 法律规定的其他个人资料属于特殊类及需要采取必要的保密措施。

5. 个人资料保护是指依法预防、发现、阻止和处理与个人资料有关的违法行为之活动。

6. 资料的主体是个人资料所反映之个人。

7. 个人资料处理是影响个人资料的一项或多项活动，例如：收集、记录、分析、确认、存储、更正、披露、组合、访问、输出、撤回、编码、解码、复制、分享、传输、提供、转交、删除、销毁个人资料或其他相关行为。

8. 资料主体的同意是指资料主体明确、自愿、肯定地表示允许处理个人资料。



个人资料管控方是决定个人资料处理目的及方式的组织、个人。

10. 个人资料处理方是指通过与资料管控方签订的合同或协议，代表资料管控方进行处理资料的组织、个人。

11. 个人资料管控及处理方是同时决定个人资料处理目的、方式并直接处理个人资料的组织、个人。

12. 第三方是除资料主体、个人资料管控方、个人资料处理方、个人资料管控及处理方之外有权处理个人资料的组织、个人。

13. 自动处理个人资料是透过电子方式执行个人资料处理的一种形式，以达到评估、分析、预测特定个人的活动，例如：习惯、偏好、兴趣、置信度、行为、地点、趋势、能力及其他情况。

14. 向境外转移个人资料是指利用网络空间、设备、电子手段或其他形式将越南公民的个人资料转移至越南社会主义共和国境外的某个地点或利用越南社会主义共和国境外的某个地点处理越南公民的个人资料，包括：

a) 将越南公民的个人资料传输给境外组织、企业、管理部门的组织、企业、个人应当按照资料主体同意的目的进行处理；

b) 个人资料管控方、个人资料管控及处理方、个人资料处理方透过位于越南社会主义共和国境外的自动系统处理越南公民的个人资料应当按照资料主体同意的目的进行处理；

第3条：个人资料保护之原则

1. 个人资料应当依法处理。

2. 除非法律另有规定，资料主体对其个人资料的相关处理活动享有知情权。

3. 个人资料只能按照个人资料管控方、个人资料处理方、个人资料管控及处理方、第三方登记及指定的目的进行处理。

4. 个人资料的收集必须符合及仅限于需要处理的范围和目的。除非法律另有规定，不得以任何形式买卖个人资料。

5. 个人资料应根据处理目的进行更新和补充。

6. 个人资料正处理过程中可以采取各种保护、保密措施，包括防止违反个人资料保护规定的行为以及防范丢失、损坏或因事故、使用技术措施造成的损失。

7. 除非法律另有规定，个人资料仅在适合资料处理目的的期限内存储。

8. 资料管控方、个人资料管控及处理方有责任遵守本条第1至第7款所规定的资料处理原则，并需要证明其遵守该资料处理原则。

第4条：违反个人资料保护规定的处分

对于违反个人资料保护规定的机关、组织及个人，视情节轻重，可按照规定给予纪律处分、行政处分或刑事处罚。



第5条：国家对个人资料保护的管理

政府统一个人资料保护的国家管理工作。

国家对个人资料保护管理的内容包括：

1. 报送国家主管机关颁布或者依据职权颁布法律文件并指导、组织实施个人资料保护的法律文件。
2. 制定并组织实施个人资料保护策略、政策、提案、项目、方案和计划。
3. 按照法律规定向机关、组织和个人提供个人资料保护措施、流程和标准的指导。
4. 宣传、教育个人资料保护法；布告、传播保护个人资料的知识技能。
5. 建设、培训及培养干部、公务员、公职人员及被指派从事个人资料保护的专员。
6. 稽查、检查个人资料保护法规的执行情况；依法处理投诉、举报以及处理违反个人资料保护法的行为。
7. 向国家主管机关提供个人资料保护情况和个人资料保护法实施情况的统计、资讯及报告。
8. 保护个人资料的国际合作。

第6条：个人资料保护议定、相关法律及国际条约的适用

个人资料的保护按照越南社会主义共和国作为缔约国之国际条约规定、相关法律及本议定的其他规定执行。

第7条：保护个人资料的国际合作

1. 建立国际合作机制以促进个人资料保护法的有效执行。
2. 参与他国保护个人资料的司法协助，包括通知、建议投诉、协助调查及信息交换，并以适当的保护措施来保护个人资料。
3. 举办会议、研讨会、科学研究及促进保护个人资料的国际执法合作活动。
4. 举办双边和多边会议，交流个人资料保护的法制建设和实践经验。
5. 个人资料保护的技术转让。

第8条：严厉禁止的行为

1. 违反个人资料保护法的规定进行处理个人资料。
2. 以创建危害越南社会主义共和国的信息、资料为目的进行处理个人资料。
3. 以创建影响国家安全、社会秩序安全以及其他组织和个人合法权益的信息、资料为目的进行处理个人资料。
4. 阻碍主管机关的个人资料保护活动。
5. 利用个人资料保护活动进行违法行为。

第二章

个人资料保护活动

第1节：资料主体的权利及义务

第9条：资料主体的权利

1. 知情权

除非法律另有规定，资料主体对其个人资料的处理活动享有知情权。

2. 同意权

除本议定第17条规定的情况外，资料主体对其个人资料的处理享有同意和拒绝权。

3. 访问权

除非法律另有规定，资料主体对其个人资料享有浏览、编辑或要求修改个人资料的访问权。

4. 同意撤回权

除非法律另有规定，资料主体有权撤回其同意。

5. 资料删除权

除非法律另有规定，资料主体有权删除或要求删除其个人资料。

6. 资料处理限制权

a) 除非法律另有规定，资料主体有权对其个人资料要求限制处理；

b) 除非法律另有规定，在资料主体提出请求后72个小时内对资料主体请求限制的所有个人资料进行限制处理。

7. 资料取得权

除非法律另有规定，资料主体有权要求个人资料管控方、个人资料管控及处理方提供其个人资料。

8. 资料处理反对权

a) 除非法律另有规定，资料主体有权反对个人资料管控方、个人资料管控及处理方处理其个人资料，以防止或限制个人资料的披露或用于广告和营销目的。

b) 除非法律另有规定，个人资料管控方、个人资料管控及处理方应当在收到资料主体的请求后于72个小时内满足资料主体的请求。

9. 投诉、举报、起诉权

资料主体有权依法投诉、举报或起诉。

10. 损失索赔权

除非当事人另有约定或者法律另有规定，当发生违反个人资料保护规定的行为时，资料主体有权依法索赔损失。

11. 自卫权

资料主体有权依照《民事法》、其他有关法律及本协议的规定保护自己，或者要求主管机构、组织依照《民事法》第11条规定实施保护民事权利的措施。

第10条：资料主体的义务

1. 保护自己的个人资料；要求其他相关组织和个人保护其个人资料。
2. 尊重、保护他人的个人资料。
3. 在同意允许处理个人资料时提供完整且准确的个人资料。
4. 参与个人资料保护技能的宣传和传播。
5. 遵守个人资料保护法的规定，参与防治个人资料保护法违法行为。

第2节：个人资料处理过程中的个人资料保护

第11条：资料主体的同意

1. 除非法律另有规定，资料主体的同意适用于个人资料处理程序的所有活动。
2. 仅在资料主体自愿且完全了解以下内容时，资料主体的同意才有效：
 - a) 被处理的个人资料类型；
 - b) 处理个人资料的目的；
 - c) 被允许处理个人资料的组织、个人；
 - d) 资料主体的权利和义务。
3. 资料主体必须明确表达同意，具体是以书面形式、语音、勾选同意框、发送同意短讯、选择同意的技术设置或者透过其他可明确表达的行为。
4. 资料主体的同意必须与目的相符。当存在多种目的时，个人资料管控方、个人资料管控及处理方应列出各项目的，供资料主体对一项或多项所述目的给予同意。
5. 资料主体的同意必须以可以打印、书面复制的格式表达，包括电子或可验证的格式。
6. 资料主体的沉默或不回应不被视为同意。
7. 资料主体可以给予部分或有条件的同意。
8. 对于敏感个人资料的处理，必须告知资料主体所处理的资料属于敏感个人资料。
9. 资料主体的同意一直生效直至资料主体另有决定或主管当局提出书面要求时为止。
10. 如果发生争议，证明资料主体同意的责任由个人资料管控方、个人资料管控及处理方承担。
11. 在资料主体已知悉并根据本条第3款规定予以同意的情况下，经依照《民事法》的规定授权的组织和个人可代表资料主体以配合个人资料管控方、个人资料管控及处理方进行个人资料处理的相关程序；对法律另有规定者除外。

第12条：撤回同意

1. 撤回同意并不影响资料处理在撤回同意前的合法性。
2. 资料主体的撤回同意必须以可以打印、书面复制的格式表达，包括电子或可验证的格式。
3. 在收到资料主体撤回同意的请求后，个人资料管控方、个人资料管控及处理方应通知资料主体撤回同意时可能产生的后果和损害。
4. 资料管控方、资料处理方、资料管控及处理方、第三方在执行本条第2款规定后，必须停止并要求相关组织和个人停止处理已撤回同意的资料主体的资料。

第13条：个人资料处理的通知

1. 在进行个人资料处理活动之前应发出一次通知。
2. 向资料主体发出有关个人资料处理的通知内容：
 - a) 处理目的；
 - b) 与本条第2款a点所规定之处理目的相关的个人资料类型；
 - c) 处理方式；
 - d) 与本条第2款a点所规定之处理目的相关的其他组织、个人的资讯；
 - d) 可能发生的不良后果及损害；
 - e) 资料处理的开始时间和结束时间。
3. 对资料主体的通知必须以可以打印、书面复制的格式表达，包括电子或可验证的格式。
4. 个人资料管控方、个人资料管控及处理方在下列情况下无需执行本条第1款规定：
 - a) 资料主体在同意予以个人资料管控方、个人资料管控及处理方按照本议定第9条规定进行收集个人资料之前，已知晓并完全同意本条第1款及第2款规定的内容；
 - b) 个人资料由国家主管机关依法处理，以服务国家机关的运作。

第14条：提供个人资料

1. 资料主体有权要求个人资料管控方、个人资料管控及处理方提供其个人资料。
2. 个人资料管控方、个人资料管控及处理方：
 - a) 经资料主体的同意后可以向其他组织、个人提供个人资料，法律另有规定除外；
 - b) 在资料主体同意允许代表及授权的情况下，代表资料主体向其他组织或个人提供资料主体的个人资料，法律另有规定除外；
3. 资料主体的个人资料之提供由个人资料管控方、个人资料管控及处理方在资料主体提出请求后于72个小时内执行，法律另有规定除外。
4. 个人资料管控方、个人资料管控及处理方在下列情况下不提供个人资料：
 - a) 对国防、国家安全、社会秩序和安全造成危害；

b) 资料主体的个人资料之提供可能会影响他人的安全、身体或心理健康；

c) 资料主体不同意提供、不允许代表或授权接收个人资料。

5. 要求提供个人资料的形式：

a) 资料主体直接或授权他人前往个人资料管控方、个人资料管控及处理方之总部要求提供个人资料。

请求接收者有责任指导提出请求的组织、个人按《个人资料提供申请表》填写内容。

如果提出请求的组织、个人是文盲或残疾人，无法撰写请求，则请求接收者有责任帮助填写《个人资料提供申请表》的内容。

b) 依照本议定附录的第1号、2号表格填写内容并透过电子网络、邮政服务、传真向个人资料管控方、个人资料管控及处理方发送《个人资料提供申请表》。

6. 《个人资料提供申请表》必须以越南语提交，包括以下主要内容：

a) 姓氏、名字；居所、地址；请求提出者的身份证号码、公民身份证号码或护照号码；传真、电话号码、电子邮箱地址（如有）；

b) 对所要求提供的个人资料注明文件、档案、资料的名称；

c) 个人资料的提供形式；

d) 要求提供个人资料的理由、目的。

7. 如果要求提供本条第2款所规定的个人资料则必须附上有关的个人、组织的书面同意。

8. 接收个人资料的提供请求

a) 个人资料管控方、个人资料管控及处理方负责接收提供个人资料的请求，并根据请求监控个人资料的提供过程和清单；

b) 如果所请求的个人资料不属于其权限范围，收到请求的个人资料管控方、个人资料管控及处理方必须通知并对提出请求的组织或个人引导至主管机关或明确告知无法提供个人资料。

9. 处理个人资料的提供请求

在接收到合格的个人资料提供请求后，个人资料管控方、个人资料管控及处理方负责提供个人资料，并通知提供个人资料的期限、地点、形式；打印、复印、拍照及透过邮政服务发送信息和传真（如有）的实际费用以及付款方式和期限；按照本条规定的顺序和程序提供个人资料。

第15条：个人资料的修改

1. 资料主体：

a) 有权访问以查阅、修改其已同意允许个人资料管控方、个人资料管控及处理方收集的个人资料，法律另有规定除外；

b) 如果因技术原因或其他原因无法直接修改，资料主体可要求个人资料管控方、个人资料管控及处理方修改其个人资料。



2. 个人资料管控方、个人资料管控及处理方在获得资料主体同意后应尽快修改资料主体的个人资料或者按照专门法的规定进行修改。如果无法进行，则必须在收到资料主体的个人资料修改请求后于72个小时内通知资料主体。

3. 个人资料处理方、第三方在获得个人资料管控方、个人资料管控及处理方的书面同意及明确知道资料主体已同意后，可以修改资料主体的个人资料。

第16条：个人资料的存储、删除及销毁

1. 在下列情况下，资料主体可以要求个人资料管控方、个人资料管控及处理方删除其个人资料：

- a) 对已同意的收集目的不再认为是必要并接受要求删除资料可能造成的损害；
- b) 撤回同意；
- c) 反对资料的处理且个人资料管控方、个人资料管控及处理方没有充分的理由继续处理；
- d) 未按照约定目的处理个人资料或违法处理个人资料；
- d) 个人资料必须依法删除。

2. 资料主体的请求在下列情况下不适用于资料的删除；

- a) 法律规定不允许删除资料；
- b) 由国家主管机关以服务国家机关依法运作为目的进行处理的个人资料；
- c) 已依法公开的个人资料；
- d) 依照法律规定以服务于法律、科研、统计目的来处理的个人资料；
- d) 在国防、国家安全、社会秩序与安全、重大灾害、危险的流行病等紧急情况下；当存在威胁安全和国防的风险但未达到宣布紧急状态的程度时；防治骚乱、恐怖主义、打击犯罪分子和违法行为；
- e) 应对威胁资料主体或其他个人生命、健康或安全的紧急情况。

3. 如果进行企业分立、拆分、合并、整合或者解散则应当依法转移个人资料。

4. 如果进行机关、组织、行政单位分立、拆分、合并及国有企业重组、转换所有制形式则应当依法转移个人资料。

5. 在资料主体对个人资料管控方、个人资料管控及处理方所收集之全部资料提出请求后应在72个小时内执行资料的删除，法律另有规定除外。

6. 个人资料管控方、个人资料管控及处理方、个人资料处理方、第三方应以适合其活动的形式存储个人资料并依法采取个人资料的保护措施。

7. 个人资料管控方、个人资料管控及处理方、个人资料处理方、第三方在下列情况可永久删除资料：

- a) 资料处理不当或已完成经资料主体同意的个人资料处理目的；



- b) 个人资料管控方、个人资料管控及处理方、个人资料处理方、第三方的运营不再需要存储个人资料；
- c) 个人资料管控方、个人资料管控及处理方、个人资料处理方、第三方依法解散或不再运营或宣布破产或被强制终止经营。

第17条：在不需要资料主体同意的情况下处理个人资料

1. 在发生紧急情况时，需要立即处理相关个人资料以保护资料主体或他人的生命和健康。个人资料管控方、个人资料处理方、个人资料管控及处理方、第三方负责证明该情况。
2. 依法公开个人资料。
3. 国家主管机关在国防、国家安全、社会秩序与安全、重大灾害、危险的流行病等紧急情况下进行的资料处理；当存在威胁安全和国防的风险但未达到宣布紧急状态的程度时；防治骚乱、恐怖主义、打击犯罪分子和违法行为。
4. 依法履行资料主体与有关机关、组织和个人的合同义务。
5. 依照专门法的规定，为国家机关的活动服务。

第18条：处理在公共场所录音、录像活动获得的个人资料

主管机关和组织为了维护国家安全、社会秩序与安全、法律规定的组织和个人的合法权益，可以在不需要获得主体同意的情况下在公共场所进行录音、录像及处理透过录音、录像活动所获得的个人资料。在进行录音、录像时，主管机关有责任告知当事人了解其被录音、录像的情况，法律另有规定除外。

第19条：处理被宣布为失踪者、死亡者的个人资料

1. 除了本议定第17条及第18条所规定的情况，处理与被宣布为失踪者、死亡者个人资料相关的个人资料时必须获得其配偶或成年子女的同意，如果上述人等不存在则必须获得被宣布为失踪者、死亡者父母的同意。
2. 本条第1款所述人等均不存在则视为不同意。

第20条：处理儿童的个人资料

1. 儿童个人资料的处理始终遵循保护儿童权利和最大利益的原则。
2. 除了本议定第17条所规定的情况，处理年满7周岁及以上年龄的儿童个人资料时必须获得儿童的同意以及依法征得其父母或监护人的同意。个人资料管控方、个人资料处理方、个人资料管控及处理方、第三方必须在进行处理儿童个人资料前核实儿童的年龄。
3. 在下列情况下，停止处理儿童个人资料，永久删除或销毁儿童个人资料：
 - a) 资料处理不当或已完成经资料主体同意的个人资料处理目的，法律另有规定除外；
 - b) 儿童的父母或监护人撤回其允许处理儿童个人资料的同意，法律另有规定除外；
 - c) 当有充分的依据证明个人资料的处理影响儿童的合法权益时应当配合主管机关的要求，法律另有规定除外。

第21条：营销服务、介绍广告产品业务中的个人资料保护

1. 经营营销服务、介绍广告产品的组织和个人，仅在征得资料主体同意的情况下才可以将透过其业务活动所收集的顾客之个人资料用于营销服务、介绍广告产品的业务。
2. 在营销服务、介绍广告产品业务中处理顾客的个人资料必须在顾客清楚了解产品介绍的内容、方式、形式及频率的基础上征得顾客的同意。
3. 经营营销服务、介绍广告产品的组织和个人有责任证明所推介产品的顾客个人资料的使用符合本条第1和第2款的规定。

第22条：违法收集、转交、买卖个人资料

1. 个人资料处理的相关组织和个人必须采取个人资料保护措施以防止其服务系统、设备非法收集个人资料的情况。
2. 未经资料主体同意而设置软件系统、技术措施或者组织收集、转交、买卖个人资料的活动属于违法行为。

第23条：关于违反个人资料保护规定的通知

1. 如果发现违反个人资料保护规定的行为，个人资料管控方、个人资料管控及处理方应当在发生本议定附录第3号表单所载之违规行为后的72个小时内通知公安部（网络安全及防治高科技犯罪分子局）。对于72个小时后的通知，必须附上延迟通知的原因。
2. 个人资料处理方当发现违反个人资料保护规定的行为后，必须尽快通知个人资料管控方。
3. 违反个人资料保护规定的通知内容：
 - a) 描述违反个人资料保护规定的性质，包括：时间、地点、行为、组织、个人、个人资料类型以及涉及的资料数量；
 - b) 指派保护资料的人员或负责保护个人资料的组织、个人的联系方式；
 - c) 描述违反个人资料保护规定可能造成的后果和损害；
 - d) 描述为解决和减少由违反个人资料保护规定引起的危害而采取的措施。
4. 如果本条第3款所规定的内容无法悉数通知则可以进行分批、分阶段通知。
5. 个人资料管控方、个人资料管控及处理方必须对个人资料保护规定之违反行为的发生作出书面确认，并配合公安部（网络安全及防治高科技犯罪分子局）处理违规行为。
6. 组织和个人当发现下列情况，应通报公安部（网络安全及防治高科技犯罪分子局）：
 - a) 发现个人资料方面的违法行为；
 - b) 个人资料的处理目的不当，与资料主体和个人资料管控方、个人资料管控及处理方之间的原始约定不符或违反法律规定；
 - c) 资料主体的权利得不到保障或没有正确落实；
 - d) 法律所规定的其他情况。

第3节：影响评估及向境外转移个人资料

第24条：评估个人资料处理的影响

1. 个人资料管控方、个人资料管控及处理方应从开始处理个人资料时建立并贮存其处理个人资料的影响评估档案。

个人资料管控方、个人资料管控及处理方的个人资料处理影响评估档案包括：

- a) 个人资料管控方、个人资料管控及处理方的资讯及联系方式；
- b) 被指定执行个人资料保护任务的组织以及个人资料管控方、个人资料管控及处理方的个人资料保护官的姓名和联系方式；
- c) 处理个人资料的目的；
- d) 所处理的个人资料类型；
- d) 接收个人资料的组织和个人，包括越南境外的组织和个人；
- e) 向境外转移个人资料的情况；
- g) 个人资料处理时间；删除或销毁个人资料的预计时间（如有）；
- h) 所采用的个人资料保护措施の説明；
- i) 评估个人资料处理的影响；后果、可能发生的不必要损害、减少或消除此类风险和损害的措施。

2. 个人资料处理方在与个人资料管控方履行合约时，应当建立并贮存个人资料处理的影响评估档案。个人资料处理方的个人资料处理影响评估档案包括：

- a) 个人资料处理方的资讯和联系方式；
- b) 被指定执行个人资料处理的组织以及个人资料处理方的个人资料处理人员的姓名和联系方式；
- c) 依照与个人资料管控方签订的合约进行个人资料的处理活动及类型的描述；
- d) 个人资料处理时间；删除或销毁个人资料的预计时间（如有）；
- d) 向境外转移个人资料的情况；
- e) 所采用的个人资料保护措施的一般说明；
- g) 后果、可能发生的不必要损害、减少或消除此类风险和损害的措施。

3. 本条第1款和第2款所规定的个人资料处理影响评估档案应当以个人资料管控方、个人资料管控及处理方或个人资料处理方的合法有效文件为建立依据。

4. 个人资料处理影响档案应始终可用以服务公安部的检查、评估活动以及在进行处理个人资料之日起60天内向公安部（网络安全和防治高科技犯罪分子局）寄送1份依照本议定附录第4号表单的原件。

5. 如果档案不完整且符合规定，公安部（网络安全和防治高科技犯罪分子局）将进行评估及要求个人资料管控方、个人资料管控及处理方、个人资料处理方完善个人资料处理影响评估档案。

6. 个人资料管控方、个人资料管控及处理方、个人资料处理方应在已寄送至公安部（网络安全和防治高科技犯罪分子局）的档案内容（依照本议定附录的第5号表单）发生变化时，对个人资料处理影响评估档案进行更新、补充。

第25条：向境外转移个人资料

1. 越南公民的个人资料在跨境资料转移方已建立了向境外转移个人资料之影响评估档案并执行本条第3、4和5款规定程序的情况下可以向境外转移。跨境资料转移方包括个人资料管控方、个人资料管控及处理方、个人资料处理方、第三方。

2. 向境外转移个人资料之影响评估档案包括：

- a) 越南公民个人资料的资料转移方及资料接收方的资讯及联系方式；
- b) 有关转移和接收越南公民个人资料的资料转移方之组织、负责人姓名和联系方式；
- c) 描述并解释越南公民的个人资料经转移至境外后的资料处理活动之目的；
- d) 描述并阐明转移至境外的个人资料类型；
- d) 描述并明确表达遵守本议定的个人资料保护规定、详细说明所采用的个人资料保护措施；
- e) 评估个人资料处理的影响程度；可能产生的后果、不必要的损害；减少或消除此类风险或损害的措施；
- g) 在资料主体充分了解出现问题或请求时的反馈、投诉机制的基础上征得本议定第11条规定的资料主体的同意。
- h) 在转移和接收越南公民个人资料的组织、个人之间应存在对处理个人资料具有表达约束和责任的书面文件。

3. 向境外转移个人资料的影响评估档案必须始终可用以服务公安部的检查、评估活动。

向境外转移资料的当事方应当自进行处理个人资料之日起60天内向公安部（网络安全和防治高科技犯罪分子局）寄送1份依照本议定附录第6号表单的正本档案。

4. 在资料转移成功后，资料转移方应当将资料转移的情况及负责的单位和个人之联系方式以书面形式通报至公安部（网络安全和防治高科技犯罪分子局）。

5. 如果档案不完整且符合规定，公安部（网络安全和防治高科技犯罪分子局）将进行评估及要求向境外转移资料的当事方完善向境外转移个人资料影响评估档案。

6. 向境外转移资料的当事方应在已寄送至公安部（网络安全和防治高科技犯罪分子局）的档案内容（依照本议定附录的第5号表单）发生变化时，对向境外转移个人资料影响评估档案进行更新、补充。向境外转移资料的当事方完善档案的期限为自要求之日起的10天内。

7. 根据具体情况，公安部决定对个人资料的境外转移进行检查的次数为1次/年。发现本议定所规定的违反个人资料保护法行为或发生越南公民个人资料的泄露、丢失事故的情况除外。

8. 在下列情况下，公安部决定要求向境外转移资料的当事方停止向境外转移个人资料：
- a) 当发现所转移的个人资料用于侵犯越南社会主义共和国的利益和国家安全的活动时；
 - b) 向境外转移资料的当事方不遵守本条第5、第6款的规定；
 - c) 发生越南公民个人资料的泄露、丢失事故。

第4节：个人资料保护的保障措施及条件

第26条：保护个人资料的措施

1. 个人资料保护措施适用于个人资料处理的开始以及整个处理过程。
2. 个人资料的保护措施包括：
 - a) 由参与个人资料处理的组织、个人执行的管理措施；
 - b) 由参与个人资料处理的组织、个人执行的技术措施
 - c) 由国家主管管理机关依照本议定和相关法律规定采取的措施；
 - d) 由国家主管机关执行的调查、诉讼措施；
 - d) 法律规定的其他措施。

第27条：保护基本个人资料

1. 采用本议定第26条第2款所规定的措施。
2. 制定和发布个人资料保护条例，明确需要依照本议定规定执行的事项。
3. 鼓励采用适合个人资料处理相关领域、行业和活动的个人资料保护标准。
4. 在对存储个人资料的设备进行处理、永久删除或销毁之前，应对服务于个人资料处理的系统、工具和设备进行网络安全的检查。

第28条：保护敏感个人资料

1. 采用本议定第26条第2款及第27条所规定的措施。
2. 指定具有个人资料保护职能的部门，指定个人资料保护负责人，并与保护个人资料的专门机构交换负责个人资料保护的部门、个人的资讯。如果个人资料管控方、个人资料管控和处理方、资料处理方、第三方是个人则进行交换执行人的个人信息。
3. 除本议定第13条第4款、第17条及第18条规定的情况外，应向资料主体通知资料主体的敏感个人资料已被处理。

第29条：个人资料保护的专门机构和国家个人资料保护门户网站

1. 个人资料保护的专门机构是公安部 – 网络安全和防治高科技犯罪分子局，负责协助公安部执行个人资料保护的国家管理工作。
2. 国家个人资料保护门户网站：
 - a) 提供党对个人资料保护的方针、路径、政策资讯及国家对个人资料保护的资讯；



- b) 宣传和传播有关个人资料保护的政策和法律；
- c) 更新个人资料保护的资讯和情况；
- d) 通过网络空间接收有关个人资料保护活动的资讯、档案和资料；
- d) 提供有关参与个人资料保护的机关、组织、个人的工作结果评估资讯；
- e) 接收违反个人资料保护规定的通知；
- g) 依法对侵犯个人资料的风险和行为进行警示及协助警示；
- h) 依法处理违反个人资料保护的行为；
- i) 依照个人资料保护法进行其他活动。

第30条：个人资料保护活动的保障条件

1. 保护个人资料队伍：

- a) 从事个人资料保护的专门队伍应在个人资料保护的专门机关设立；
- b) 机关、组织、企业应指定具有个人资料保护职能的部门和人员以确保个人资料保护法规的实施；
- c) 依号召参与个人资料保护的组织和个人；
- d) 公安部制定具体的方案和计划以发展个人资料保护的人力资源。

2. 机关、组织和个人有责任宣传和传播知识和技能，提高机关、组织和个人的个人资料保护意识。

3. 确保个人资料保护专门机构的设施和运营条件。

第31条：确保个人资料保护活动的资金

1. 实施个人资料保护的资金来源包括国家预算；国内外机关、组织和个人的支持；来自提供个人资料保护服务的收入；国际援助以及其他合法的收入来源。

2. 国家机关的个人资料保护经费由国家预算保障，并纳入国家年度预算概算。国家预算资金的管理和使用必须遵守国家预算法。

3. 组织、企业的个人资料保护经费由组织、企业自行安排及按照规定落实。

第三章

机关、组织和个人的责任

第32条：公安部的责任

- 1. 协助政府对个人资料保护进行国家统一管理。
- 2. 指导和实施个人资料保护活动，保护资料主体的权利免受违反个人资料保护法行为的侵害，提出颁布个人资料保护标准和适用的建议。
- 3. 建立、管理和运营国家个人资料保护门户网站。



4. 评估有关机构、组织和个人的个人资料保护工作结果。
5. 根据本议定的规定接收有关个人资料保护的档案、表单和资讯。
6. 推动个人资料保护领域的创新措施和研究，开展个人资料保护的国际合作。
7. 依法稽查、检查、处理投诉、举报、处理违反个人资料保护规定的行为。

第33条：信息与传媒部的责任

1. 指导媒体机构、通讯社、管理领域所属组织和企业依照本议定的规定保护个人资料。
2. 根据被分配的职责任务，制定、指导和实施个人资料保护措施，保障信息通信活动中个人资料的网络信息安全。
3. 配合公安部稽查、检查和处理个人资料保护违法行为。

第34条：国防部的责任

按照法律规定和被分配的职责任务，对隶属国防部的机构、组织和个人进行管理、稽查、检查、监督、处理违规行为以及采用个人资料保护规定。

第35条：科学技术部的责任

1. 配合公安部制定个人资料保护标准以及适用个人资料保护标准的建议。
2. 与公安部就个人资料保护措施进行研究、交流，以适应科学、科技的发展情况。

第36条：各部委、部级机构、政府所属机关的责任

1. 依照个人资料保护法的规定，对保护个人资料的管理部门及领域实施国家管理。
2. 制定并落实本议定的个人资料保护内容和任务。
3. 在制定、落实各部委的任务中对个人资料保护规定进行补充。
4. 依照现行的分级管理预算法规为个人资料保护活动分配资金。
5. 发布符合个人资料保护规定的开放资料名录

第37条：各省、直辖市人民委员会的责任

1. 依照个人资料保护法的规定，对保护个人资料的管理部门及领域实施国家管理。
2. 落实本议定有关个人资料保护的规定。
3. 依照现行的分级管理预算法规为个人资料保护活动分配资金。
4. 发布符合个人资料保护规定的开放资料名录

第38条：个人资料管控方的责任

1. 实施组织和技术措施以及适当的安全、保密措施，以证明资料处理活动已按照个人资料保护法的规定进行，并根据需要对这些措施进行检查和更新。
2. 记录并存储个人资料处理过程的系统日志。
3. 发出违反本议定第23条规定的个人资料保护条例的通知。



4. 选择明确与任务相符的个人资料处理方并仅与具有适当保护措施的个人资料处理方合作。
5. 确保本议定第九条所规定的资料主体的权利。
6. 个人资料管控方就个人资料处理过程造成的损害对资料主体负责。
7. 在个人资料保护活动方面配合公安部及国家主管机关，为查处违反个人资料保护法行为提供资讯。

第39条：个人资料处理方的责任

1. 仅在与个人资料管控方签订资料处理合同或协议后才能接收个人资料。
2. 根据与个人资料管控方签订的合同或协议处理个人资料。
3. 全面落实本议定及其他相关法律文件规定的个人资料保护措施。
4. 个人资料处理方就个人资料处理过程造成的损害对资料主体负责。
5. 在资料处理完成后，删除、向个人资料管控方返还所有个人资料。
6. 在个人资料保护活动方面配合公安部及国家主管机关，为查处违反个人资料保护法行为提供资讯。

第40条：资料管控及处理方的责任

全面遵守有关个人资料管控方和个人资料处理方职责的规定。

第41条：第三方的责任

全面遵守本议定所规定的个人资料处理责任规定。

第42条：相关组织和个人的责任

1. 采取保护自己个人资料的措施，并对所提供的个人资料的准确性负责。
2. 遵守本议定有关个人资料保护的规定。
3. 及时通知公安部有关个人资料保护活动的违规行为。
4. 配合公安部处理有关个人资料保护活动的违法行为。

第四章

执行条款

第43条：执行效力

1. 本议定自2023年07月01日起生效。
2. 微型企业、小型企业、中型企业和初创企业有权选择在企业成立之日起的前两年内免除指定个人资料保护的個人、部門的规定。
3. 直接从事个人资料处理活动的微型企业、小型企业、中型企业、初创企业不适用本条第二款的规定。



第44条：执行责任

1. 公安部部长督促、检查、指导本议定的实施。
2. 部长、部级机关负责人、政府所属机关负责人；省、直辖市人民委员会主席负责执行本议定。

收件处：

- 党中央书记委员会；
- 总理、各政府副总理；
- 各部委、部级机关、政府所属机关；
- 各省、直辖市人民议会、人民委员会；
- 中央办公室及各党委；
- 总书记办公室；
- 国家主席办公室；
- 国会的民族议会及委员会；
- 国会办公室；
- 最高人民检察院；
- 最高人民法院；
- 国家审计；
- 国家政策监察委员会；
- 社会政策银行；
- 越南发展银行；
- 越南祖国阵线中央委员会；
- 各团体的中央机关；
- 政府办公室：主任、副主任、总理助理、电子信息门户网站总经理、各司、局、直属单位、公报；
- 存档：文书、行政程序控制局(2b)TM.

代表政府
代替总理签署
副总理
(已签名盖章)

陈留光

~ 恒利翻译，仅供参考 ~

CHÍNH PHỦ

Số: 13/2023/NĐ-CP

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

Độc lập - Tự do - Hạnh phúc

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

- 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.
- Nghị định này áp dụng đối với:
 - Cơ quan, tổ chức, cá nhân Việt Nam;
 - Cơ quan, tổ chức, cá nhân nước ngoài tại Việt Nam;
 - Cơ quan, tổ chức, cá nhân Việt Nam hoạt động tại nước ngoài;
 - 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:

- 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.
- 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.
- Dữ liệu cá nhân cơ bản bao gồm:
 - Họ, chữ đệm và tên khai sinh, tên gọi khác (nếu có);
 - Ngày, tháng, năm sinh; ngày, tháng, năm chết hoặc mất tích;
 - Giới tính;
 - Nơi sinh, nơi đăng ký khai sinh, nơi thường trú, nơi tạm trú, nơi ở hiện tại, quê quán, địa chỉ liên hệ;
 - 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 pháp 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 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 chuyên 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 chuyên 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 chuyên 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 chuyên 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.

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 đơn 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 Công 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