

# La loi Informatique et Libertés

17 juin 2019

---

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Depuis le 1<sup>er</sup> juin 2019, la loi du 6 janvier 1978, dite « Informatique et Libertés », est en vigueur dans une nouvelle rédaction. Elle comporte notamment les dispositions relatives aux « marges de manœuvre nationales » autorisées par le [Règlement général sur la protection des données \(RGPD\)](#) que le législateur a choisi d'exercer ainsi que les mesures de transposition en droit français de la [Directive « police-justice »](#).

La lecture de la loi est simplifiée par cette nouvelle rédaction. Elle précise en effet les différents régimes applicables en fonction de la nature des traitements concernés : traitements relevant du RGPD, traitements « police-justice », traitements intéressant la défense nationale ou la sûreté de l'Etat, etc. Elle comporte en outre des dispositions communes, applicables à tout traitement.

Pour rappel, la loi « Informatique et Libertés » n'a pas pour objet de reprendre en intégralité les dispositions du RGPD, même si elle y renvoie expressément dans certains cas. Pour les seuls traitements relevant du RGPD, la bonne compréhension du cadre juridique suppose donc de lire de manière combinée le RGPD et la loi du 6 janvier 1978.

La loi « Informatique et Libertés », dans cette nouvelle rédaction, est enfin pleinement applicable dans tous les territoires d'outre-mer.

► [En savoir plus sur l'entrée en vigueur de la nouvelle loi Informatique et Libertés](#)

---

## Sommaire

### Titre Ier : Dispositions communes

#### Chapitre Ier - Principes et définitions

[Article 1<sup>er</sup>](#)

[Article 2](#)

[Article 3](#)

[Article 4](#)

[Article 5](#)

[Article 6](#)

[Article 7](#)

#### Chapitre II : La Commission nationale de l'informatique et des libertés

##### Section 1 : Organisation et missions

[Article 8](#)

[Article 9](#)

[Article 10](#)

[Article 11](#)

[Article 12](#)

[Article 13](#)

[Article 14](#)

[Article 15](#)

[Article 16](#)

[Article 17](#)

[Article 18](#)

##### Section 2 : Contrôle de la mise en œuvre des traitements

[Article 19](#)

##### Section 3 : Mesures correctrices et sanctions

[Article 20](#)

[Article 21](#)

[Article 22](#)

[Article 23](#)

##### Section 4 : Coopération

[Article 24](#)  
[Article 25](#)  
[Article 26](#)  
[Article 27](#)  
[Article 28](#)  
[Article 29](#)

### **Chapitre III : Dispositions particulières relatives au numéro d'inscription des personnes au répertoire national d'identification des personnes physiques**

[Article 30](#)

### **Chapitre IV : Formalités préalables à la mise en oeuvre des traitements**

[Article 31](#)  
[Article 32](#)  
[Article 33](#)  
[Article 34](#)  
[Article 35](#)  
[Article 36](#)

### **Chapitre V : Obligations incombant aux responsables de traitements et droits des personnes**

[Article 37](#)  
[Article 38](#)  
[Article 39](#)

### **Chapitre VI : Dispositions pénales**

[Article 40](#)  
[Article 41](#)

## **Titre II : Traitements relevant du régime de protection des données à caractère personnel prévu par le règlement (UE) 2016/679 du 27 avril 2016**

### **Chapitre Ier : Dispositions générales**

[Article 42](#)  
[Article 43](#)  
[Article 44](#)  
[Article 45](#)  
[Article 46](#)  
[Article 47](#)

### **Chapitre II : Droits de la personne concernée**

[Article 48](#)  
[Article 49](#)  
[Article 50](#)  
[Article 51](#)  
[Article 52](#)  
[Article 53](#)  
[Article 54](#)  
[Article 55](#)  
[Article 56](#)

### **Chapitre III : Obligations incombant au responsable du traitement et au sous-traitant**

#### **Section 1 : Obligations générales**

[Article 57](#)  
[Article 58](#)  
[Article 59](#)  
[Article 60](#)  
[Article 61](#)

#### **Section 2 : Obligations en cas de traitement susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques**

[Article 62](#)  
[Article 63](#)

#### **Section 3 : Traitements de données à caractère personnel dans le domaine de la santé**

[Article 64](#)

##### **Sous-section 1 : Dispositions générales**

[Article 65](#)

[Article 66](#)  
[Article 67](#)  
[Article 68](#)  
[Article 69](#)  
[Article 70](#)  
[Article 71](#)

**Sous-section 2 : Dispositions particulières relatives aux traitements à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé**

[Article 72](#)  
[Article 73](#)  
[Article 74](#)  
[Article 75](#)  
[Article 76](#)  
[Article 77](#)

**Section 4 : Traitements à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques.**

[Article 78](#)  
[Article 79](#)

**Section 5 : Traitements de données à caractère personnel aux fins de journalisme et d'expression littéraire et artistique.**

[Article 80](#)

**Chapitre IV : Droits et obligations propres aux traitements dans le secteur des communications électroniques.**

[Article 81](#)  
[Article 82](#)  
[Article 83](#)

**Chapitre V : Dispositions régissant les traitements de données à caractère personnel relatives aux personnes décédées.**

[Article 84](#)  
[Article 85](#)  
[Article 86](#)

**Titre III : Dispositions applicables aux traitements relevant de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil**

**Chapitre Ier : Dispositions générales.**

[Article 87](#)  
[Article 88](#)  
[Article 89](#)  
[Article 90](#)  
[Article 91](#)  
[Article 92](#)  
[Article 93](#)  
[Article 94](#)  
[Article 95](#)  
[Article 96](#)

**Chapitre II : Obligations incombant aux autorités compétentes, aux responsables de traitement de données à caractère personnel et aux sous-traitants.**

[Article 97](#)  
[Article 98](#)  
[Article 99](#)  
[Article 100](#)  
[Article 101](#)  
[Article 102](#)  
[Article 103](#)

**Chapitre III : Droits de la personne concernée**

[Article 104](#)  
[Article 105](#)  
[Article 106](#)

[Article 107](#)  
[Article 108](#)  
[Article 109](#)  
[Article 110](#)  
[Article 111](#)

**Chapitre IV : Transferts de données à caractère personnel vers des États n'appartenant pas à l'Union européenne ou vers des destinataires établis dans des États n'appartenant pas à l'Union européenne.**

[Article 112](#)  
[Article 113](#)  
[Article 114](#)

**Titre IV : Dispositions applicables aux traitements intéressant la sûreté de l'Etat et la défense**

[Article 115](#)  
[Article 116](#)  
[Article 117](#)  
[Article 118](#)  
[Article 119](#)  
[Article 120](#)

**Chapitre II : Autres dispositions.**

**Section 1 : Obligations incombant au responsable de traitement.**

[Article 121](#)

**Section 2 : Obligations incombant au sous-traitant**

[Article 122](#)

**Section 3 : Transferts de données à caractère personnel vers des Etats n'appartenant pas à l'Union européenne ou vers des destinataires établis dans des Etats n'appartenant pas à l'Union européenne**

[Article 123](#)  
[Article 124](#)

**Titre V : Dispositions relatives à l'outre-mer**

[Article 125](#)  
[Article 126](#)  
[Article 127](#)  
[Article 128](#)

## **Titre Ier : Dispositions communes**

### **Chapitre I<sup>er</sup> - Principes et définitions**

**Article 1er**

L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

Les droits des personnes de décider et de contrôler les usages qui sont faits des données à caractère personnel les concernant et les obligations incombant aux personnes qui traitent ces données s'exercent dans le cadre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 et de la présente loi.

## **Article 2**

La présente loi s'applique aux traitements automatisés en tout ou partie de données à caractère personnel, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers, lorsque leur responsable remplit les conditions prévues à l'article 3 de la présente loi, à l'exception des traitements mis en œuvre par des personnes physiques pour l'exercice d'activités strictement personnelles ou domestiques.

Constitue un fichier de données à caractère personnel tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique.

Sauf dispositions contraires, dans le cadre de la présente loi s'appliquent les définitions de l'article 4 du règlement (UE) 2016/679 du 27 avril 2016.

## **Article 3**

**I.** - Sans préjudice, en ce qui concerne les traitements entrant dans le champ du règlement (UE) 2016/679 du 27 avril 2016, des critères prévus par l'article 3 de ce règlement, l'ensemble des dispositions de la présente loi s'appliquent aux traitements des données à caractère personnel effectués dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire français, que le traitement ait lieu ou non en France.

**II.** - Les règles nationales prises sur le fondement des dispositions du même règlement renvoyant au droit national le soin d'adapter ou de compléter les droits et obligations prévus par ce règlement s'appliquent dès lors que la personne concernée réside en France, y compris lorsque le responsable de traitement n'est pas établi en France.

Toutefois, lorsque est en cause un des traitements mentionnés au 2 de l'article 85 du même règlement, les règles nationales mentionnées au premier alinéa du II sont celles dont relève le responsable de traitement, lorsqu'il est établi dans l'Union européenne.

## **Article 4**

Les données à caractère personnel doivent être :

1° Traitées de manière licite, loyale et, pour les traitements relevant du titre II, transparente au regard de la personne concernée ;

2° Collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités. Toutefois, un traitement ultérieur de données à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques est considéré comme compatible avec les finalités initiales de la collecte des données, s'il est réalisé dans le respect des dispositions du

règlement (UE) 2016/679 du 27 avril 2016 et de la présente loi, applicables à de tels traitements et s'il n'est pas utilisé pour prendre des décisions à l'égard des personnes concernées ;

3° Adéquates, pertinentes et, au regard des finalités pour lesquelles elles sont traitées, limitées à ce qui est nécessaire ou, pour les traitements relevant des titres III et IV, non excessives ;

4° Exactes et, si nécessaire, tenues à jour. Toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder ;

5° Conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées. Toutefois, les données à caractère personnel peuvent être conservées au-delà de cette durée dans la mesure où elles sont traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques. Le choix des données conservées à des fins archivistiques dans l'intérêt public est opéré dans les conditions prévues à l'article L. 212-3 du code du patrimoine ;

6° Traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, ou l'accès par des personnes non autorisées, à l'aide de mesures techniques ou organisationnelles appropriées.

#### **Article 5**

Un traitement de données à caractère personnel n'est licite que si, et dans la mesure où, il remplit au moins une des conditions suivantes :

1° Le traitement, lorsqu'il relève du titre II, a reçu le consentement de la personne concernée, dans les conditions mentionnées au 11 de l'article 4 et à l'article 7 du règlement (UE) 2016/679 du 27 avril 2016 précédemment mentionné ;

2° Le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;

3° Le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;

4° Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;

5° Le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;

6° Sauf pour les traitements effectués par les autorités publiques dans l'exécution de leurs missions, le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.

#### **Article 6**

**I.** - Il est interdit de traiter des données à caractère personnel qui révèlent la prétendue origine raciale ou l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne physique ou de traiter des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

**II.** - Les exceptions à l'interdiction mentionnée au I sont fixées dans les conditions prévues par le 2 de l'article 9 du règlement (UE) 2016/679 du 27 avril 2016 et par la présente loi.

**III.** - De même, ne sont pas soumis à l'interdiction prévue au I les traitements, automatisés ou non, justifiés par l'intérêt public et autorisés suivant les modalités prévues au II de l'article 31 et à l'article 32.

#### **Article 7**

Les dispositions de la présente loi ne font pas obstacle à l'application, au bénéfice de tiers, des dispositions relatives à l'accès aux documents administratifs et aux archives publiques.

En conséquence, ne peut être regardée comme une personne non autorisée au sens du 6° de l'article 4 le titulaire d'un droit d'accès exercé conformément aux autres dispositions législatives et réglementaires relatives à l'accès aux documents administratifs et aux archives publiques.

## **Chapitre II : La Commission nationale de l'informatique et des libertés**

### **Section 1 : Organisation et missions**

#### **Article 8**

**I.** - La Commission nationale de l'informatique et des libertés est une autorité administrative indépendante. Elle est l'autorité de contrôle nationale au sens et pour l'application du règlement (UE) 2016/679 du 27 avril 2016. Elle exerce les missions suivantes :

1° Elle informe toutes les personnes concernées et tous les responsables de traitements de leurs droits et obligations et peut, à cette fin, apporter une

information adaptée aux collectivités territoriales, à leurs groupements et aux petites et moyennes entreprises ;

2° Elle veille à ce que les traitements de données à caractère personnel soient mis en œuvre conformément aux dispositions de la présente loi et aux autres dispositions relatives à la protection des données personnelles prévues par les textes législatifs et réglementaires, le droit de l'Union européenne et les engagements internationaux de la France.

A ce titre :

a) Elle donne un avis sur les traitements mentionnés aux articles 31 et 32 ;

b) Elle établit et publie des lignes directrices, recommandations ou référentiels destinés à faciliter la mise en conformité des traitements de données à caractère personnel avec les textes relatifs à la protection des données à caractère personnel et à procéder à l'évaluation préalable des risques par les responsables de traitement et leurs sous-traitants. Elle encourage l'élaboration de codes de conduite définissant les obligations qui incombent aux responsables de traitement et à leurs sous-traitants, compte tenu du risque inhérent aux traitements de données à caractère personnel pour les droits et libertés des personnes physiques, notamment des mineurs. Elle homologue et publie les méthodologies de référence destinées à favoriser la conformité des traitements de données de santé à caractère personnel. Elle prend en compte, dans tous les domaines de son action, la situation des personnes dépourvues de compétences numériques, et les besoins spécifiques des collectivités territoriales, de leurs groupements et des microentreprises, petites entreprises et moyennes entreprises ;

c) En concertation avec les organismes publics et privés représentatifs des acteurs concernés, elle établit et publie des règlements types en vue d'assurer la sécurité des systèmes de traitement de données à caractère personnel et de régir les traitements de données biométriques, génétiques et de santé. A ce titre, sauf pour les traitements mis en œuvre pour le compte de l'Etat agissant dans l'exercice de ses prérogatives de puissance publique, elle peut prescrire des mesures, notamment techniques et organisationnelles, supplémentaires pour le traitement des données biométriques, génétiques et de santé en application du 4 de l'article 9 du règlement (UE) 2016/679 du 27 avril 2016 et des garanties complémentaires en matière de traitement de données à caractère personnel relatives aux condamnations pénales et aux infractions conformément à l'article 10 du même règlement ;

d) Elle traite les réclamations, pétitions et plaintes introduites par une personne concernée ou par un organisme, une organisation ou une association, examine ou enquête sur l'objet de la réclamation, dans la mesure nécessaire, et informe l'auteur de la réclamation de l'état d'avancement et de l'issue de l'enquête dans un délai raisonnable, notamment si un complément d'enquête ou une coordination avec une autre autorité de contrôle est nécessaire ;

e) Elle répond aux demandes d'avis des pouvoirs publics et, le cas échéant, des juridictions, et conseille les personnes et organismes qui mettent en œuvre ou

envisagent de mettre en œuvre des traitements automatisés de données à caractère personnel ;

f) Elle donne avis sans délai au procureur de la République, dans les conditions prévues à l'article 40 du code de procédure pénale, lorsqu'elle acquiert connaissance d'un crime ou d'un délit, et peut présenter des observations dans les procédures pénales, dans les conditions prévues à l'article 41 de la présente loi ;

g) Elle peut, par décision particulière, charger un ou plusieurs de ses membres ou le secrétaire général, dans les conditions prévues à l'article 19 de la présente loi, de procéder ou de faire procéder par les agents de ses services à des vérifications portant sur tous traitements et, le cas échéant, d'obtenir des copies de tous documents ou supports d'information utiles à ses missions ;

h) Elle peut décider de certifier des personnes, des produits, des systèmes de données ou des procédures aux fins de reconnaître qu'ils se conforment au règlement (UE) 2016/679 du 27 avril 2016 et à la présente loi. Elle prend en considération, à cette fin, les besoins spécifiques des collectivités territoriales, de leurs groupements et des microentreprises, petites entreprises et moyennes entreprises. Elle agréé, aux mêmes fins, des organismes certificateurs, sur la base, le cas échéant, de leur accréditation par l'organisme national d'accréditation mentionné au b du 1 de l'article 43 du même règlement ou décide, conjointement avec cet organisme, que ce dernier procède à leur agrément, dans des conditions précisées par décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés. La commission élabore ou approuve les critères des référentiels de certification et d'agrément ;

i) Elle peut certifier ou homologuer et publier des référentiels ou des méthodologies générales aux fins de certification, par des tiers agréés ou accrédités selon les modalités mentionnées au h du présent 2°, de la conformité à la présente loi de processus d'anonymisation des données à caractère personnel, notamment en vue de la réutilisation d'informations publiques mises en ligne dans les conditions prévues au titre II du livre III du code des relations entre le public et l'administration.

Il est tenu compte d'une telle certification, le cas échéant, pour la mise en œuvre des sanctions prévues à la section 3 du présent chapitre ;

j) Elle répond aux demandes ou saisines prévues aux articles 52,108 et 118 ;

k) Elle peut établir une liste des traitements susceptibles de créer un risque élevé devant faire l'objet d'une consultation préalable conformément à l'article 90 ;

l) Elle mène des actions de sensibilisation auprès des médiateurs de la consommation et des médiateurs publics, au sens de l'article L. 611-1 du code de la consommation, en vue de la bonne application de la présente loi ;

3° Sur demande ou de sa propre initiative, elle délivre un label à des produits ou à des procédures tendant à la protection des données à caractère personnel,

attestant leur conformité aux dispositions de la présente loi. Le président peut, lorsque la complexité du produit ou de la procédure le justifie, recourir à toute personne indépendante qualifiée pour procéder à leur évaluation. Le coût de cette évaluation est pris en charge par l'entreprise qui demande le label ; elle retire le label lorsqu'elle constate, par tout moyen, que les conditions qui ont permis sa délivrance ne sont plus satisfaites ;

4° Elle se tient informée de l'évolution des technologies de l'information et rend publique le cas échéant son appréciation des conséquences qui en résultent pour l'exercice des droits et libertés mentionnés à l'article 1er ;

A ce titre :

a) Elle est consultée sur tout projet de loi ou de décret ou toute disposition de projet de loi ou de décret relatifs à la protection des données à caractère personnel ou au traitement de telles données. Elle peut également être consultée par le président de l'Assemblée nationale, par le président du Sénat ou par les commissions compétentes de l'Assemblée nationale et du Sénat ainsi qu'à la demande d'un président de groupe parlementaire sur toute proposition de loi relative à la protection des données à caractère personnel ou au traitement de telles données. Outre les cas prévus aux articles 31 et 32, lorsqu'une loi prévoit qu'un décret ou un arrêté est pris après avis de la commission, cet avis est publié avec le décret ou l'arrêté ;

b) Elle propose au Gouvernement les mesures législatives ou réglementaires d'adaptation de la protection des libertés à l'évolution des procédés et techniques informatiques et numériques ;

c) A la demande d'autres autorités administratives indépendantes, elle peut apporter son concours en matière de protection des données ;

d) Elle peut être associée, à la demande du Premier ministre, à la préparation et à la définition de la position française dans les négociations internationales dans le domaine de la protection des données à caractère personnel. Elle peut participer, à la demande du Premier ministre, à la représentation française dans les organisations internationales et de l'Union européenne compétentes en ce domaine ;

e) Elle conduit une réflexion sur les problèmes éthiques et les questions de société soulevés par l'évolution des technologies informatiques et numériques ;

f) Elle promeut, dans le cadre de ses missions, l'utilisation des technologies protectrices de la vie privée, notamment les technologies de chiffrement des données ;

5° Elle peut présenter des observations devant toute juridiction à l'occasion d'un litige relatif à l'application de la présente loi et des dispositions relatives à la protection des données à caractère personnel prévues par les textes législatifs et réglementaires, le droit de l'Union européenne, en particulier le règlement (UE) 2016/679 du 27 avril 2016, et les engagements internationaux de la France.

**II.** - Pour l'accomplissement de ses missions, la commission peut procéder par

voie de recommandation et prendre des décisions individuelles ou réglementaires dans les cas prévus par la présente loi.

La commission présente chaque année au Président de la République et au Premier ministre un rapport public rendant compte de l'exécution de sa mission.

#### **Article 9**

**I.** - La Commission nationale de l'informatique et des libertés est composée de dix-huit membres :

1° Deux députés et deux sénateurs, désignés respectivement par l'Assemblée nationale et par le Sénat de manière à assurer une représentation pluraliste ;

2° Deux membres du Conseil économique, social et environnemental, élus par cette assemblée ;

3° Deux membres ou anciens membres du Conseil d'Etat, d'un grade au moins égal à celui de conseiller, élus par l'assemblée générale du Conseil d'Etat ;

4° Deux membres ou anciens membres de la Cour de cassation, d'un grade au moins égal à celui de conseiller, élus par l'assemblée générale de la Cour de cassation ;

5° Deux membres ou anciens membres de la Cour des comptes, d'un grade au moins égal à celui de conseiller maître, élus par l'assemblée générale de la Cour des comptes ;

6° Trois personnalités qualifiées pour leur connaissance du numérique et des questions touchant aux libertés individuelles, nommées par décret ;

7° Deux personnalités qualifiées pour leur connaissance du numérique et des questions touchant aux libertés individuelles, désignées respectivement par le président de l'Assemblée nationale et par le président du Sénat ;

8° Le président de la Commission d'accès aux documents administratifs, ou son représentant.

Elle comprend en outre, avec voix consultative, le Défenseur des droits ou son représentant.

Les deux membres désignés ou élus par une même autorité en application des 1° à 5° sont une femme et un homme. Les trois membres mentionnés au 6° comprennent au moins une femme et un homme.

Les deux membres mentionnés au 7° sont une femme et un homme. Pour l'application de cette règle, le membre succédant à une femme est un homme et celui succédant à un homme, une femme. Toutefois, le nouveau membre désigné est de même sexe que celui qu'il remplace, soit en cas de cessation du mandat avant son terme normal, soit en cas de renouvellement du mandat de l'autre membre mentionné au 7°.

Selon des modalités fixées par décret en Conseil d'Etat, le collège est, à l'exception de son président, renouvelé par moitié tous les deux ans et six mois.

Le président est nommé par décret du Président de la République parmi les membres pour la durée de son mandat. La commission élit en son sein deux vice-présidents, dont un vice-président délégué. Le président et les vice-présidents composent le bureau.

Le président exerce ses fonctions à temps plein. Sa fonction est incompatible avec toute détention, directe ou indirecte, d'intérêts dans une entreprise du secteur des communications électroniques ou de l'informatique.

La durée du mandat de président est de cinq ans.

Le président de la commission reçoit un traitement égal à celui afférent à la seconde des deux catégories supérieures des emplois de l'Etat classés hors échelle.

En cas de besoin, le vice-président délégué exerce les attributions du président.

Le secrétaire général est chargé du fonctionnement et de la coordination des services sous l'autorité du président.

La formation restreinte de la commission est composée d'un président et de cinq autres membres élus par la commission en son sein. Les membres du bureau ne sont pas éligibles à la formation restreinte.

En cas de partage égal des voix, celle du président est prépondérante.

**II.** - Le mandat des membres de la commission est de cinq ans ; il est renouvelable une fois, sous réserve des dixième et onzième alinéas du I.

#### **Article 10**

Les agents de la commission sont nommés par le président. Ceux des agents qui peuvent être appelés à participer à la mise en œuvre des missions de vérification mentionnées aux articles 19 et 25 doivent y être habilités par la commission ; cette habilitation ne dispense pas de l'application des dispositions définissant les procédures autorisant l'accès aux secrets protégés par la loi.

#### **Article 11**

Les agents de la commission sont astreints au secret pour les faits, actes ou renseignements dont ils ont pu avoir connaissance en raison de leurs fonctions, sous peine des sanctions prévues à l'article 413-10 du code pénal et, sous réserve de ce qui est nécessaire à l'établissement du rapport annuel, à l'article 226-13 du même code.

#### **Article 12**

Le règlement intérieur de la commission précise notamment les règles relatives aux délibérations, à l'instruction des dossiers et à leur présentation devant la commission, ainsi que les modalités de mise en œuvre de la procédure de labellisation prévue au 3° du I de l'article 8.

#### **Article 13**

Sous réserve des compétences du bureau et de la formation restreinte, la commission se réunit en formation plénière.

L'ordre du jour de la commission réunie en formation plénière est rendu public.

En cas de partage égal des voix, la voix du président est prépondérante.

La commission peut charger le président ou le vice-président délégué d'exercer celles de ses attributions mentionnées :

1° Aux f et g du 2° du I de l'article 8 ;

2° Au d du 2° du I de l'article 8 ;

3° Au d du 4° du I de l'article 8 ;

4° Aux articles 52, 108 et 118 ;

5° A l'article 66 ;

6° Au 4 de l'article 34 du règlement (UE) 2016/679 du 27 avril 2016, pour les décisions donnant acte du respect des conditions mentionnées au 3 du même article 34 ;

7° Aux a et h du 3 de l'article 58 du même règlement.

Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, fixe les conditions et limites dans lesquelles le président de la commission et le vice-président délégué peuvent déléguer leur signature.

#### **Article 14**

La Commission nationale de l'informatique et des libertés et la Commission d'accès aux documents administratifs se réunissent dans un collège unique, sur l'initiative conjointe de leurs présidents, lorsqu'un sujet d'intérêt commun le justifie.

#### **Article 15**

Le bureau peut être chargé par la commission d'exercer les attributions de celle-ci mentionnées au dernier alinéa de l'article 10.

#### **Article 16**

La formation restreinte prend les mesures et prononce les sanctions à l'encontre des responsables de traitements ou des sous-traitants qui ne respectent pas les obligations découlant du règlement (UE) 2016/679 du 27 avril 2016 et de la présente loi dans les conditions prévues à la section 3 du présent chapitre.

Ses membres délibèrent hors de la présence des agents de la commission, à l'exception de ceux chargés de la tenue de la séance.

Les membres de la formation restreinte ne peuvent participer à l'exercice des attributions de la commission mentionnées aux d, f et g du 2° du I de l'article 8 et à l'article 19 de la présente loi.

#### **Article 17**

Un commissaire du Gouvernement, désigné par le Premier ministre, siège auprès de la commission. Des commissaires adjoints peuvent être désignés dans les mêmes conditions.

Le commissaire du Gouvernement assiste à toutes les délibérations de la commission réunie en formation plénière ainsi qu'à celles des réunions de son bureau qui ont pour objet l'exercice des attributions déléguées en application de l'article 15. Il peut assister aux séances de la formation restreinte, sans être présent au délibéré. Il est rendu destinataire de l'ensemble des avis et décisions de la commission et de la formation restreinte.

Sauf en matière de mesures ou de sanctions relevant de la section 3 du présent chapitre, il peut provoquer une seconde délibération de la commission, qui doit intervenir dans les dix jours suivant la délibération initiale.

#### **Article 18**

Les membres du Gouvernement, autorités publiques, dirigeants d'entreprises publiques ou privées, responsables de groupements divers et plus généralement les détenteurs ou utilisateurs de traitements ou de fichiers de données à caractère personnel ne peuvent s'opposer à l'action de la Commission nationale de l'informatique et des libertés ou de ses membres et doivent au contraire prendre toutes mesures utiles afin de faciliter sa tâche.

Sauf dans les cas où elles sont astreintes au secret professionnel, les personnes interrogées dans le cadre des vérifications faites par la commission en application du g du 2° du I de l'article 8 sont tenues de fournir les renseignements demandés par celle-ci pour l'exercice de ses missions.

## **Section 2 : Contrôle de la mise en œuvre des traitements**

#### **Article 19**

**I.** - Les membres de la Commission nationale de l'informatique et des libertés ainsi que les agents de ses services habilités dans les conditions définies au dernier alinéa de l'article 10 ont accès, de 6 heures à 21 heures, pour l'exercice

de leurs missions, aux lieux, locaux, enceintes, installations ou établissements servant à la mise en œuvre d'un traitement de données à caractère personnel.

Le procureur de la République territorialement compétent en est préalablement informé.

Lorsqu'un traitement de données à caractère personnel est mis en œuvre, soit dans les parties de ces lieux, locaux, enceintes, installations ou établissements affectées au domicile privé, soit dans de tels lieux, locaux, enceintes, installations ou établissements entièrement affectés au domicile privé, la visite ne peut se dérouler qu'après l'autorisation du juge des libertés et de la détention du tribunal de grande instance dans le ressort duquel sont situés les locaux à visiter, dans les conditions prévues au II du présent article.

**II.** - Le responsable de ces lieux, locaux, enceintes, installations ou établissements est informé de son droit d'opposition à la visite. Lorsqu'il exerce ce droit, la visite ne peut se dérouler qu'après l'autorisation du juge des libertés et de la détention du tribunal de grande instance dans le ressort duquel sont situés les locaux à visiter, qui statue dans des conditions fixées par décret en Conseil d'Etat. Toutefois, lorsque l'urgence, la gravité des faits à l'origine du contrôle ou le risque de destruction ou de dissimulation de documents le justifie, la visite peut avoir lieu sans que le responsable des locaux en ait été informé, sur autorisation préalable du juge des libertés et de la détention. Dans ce cas, le responsable des lieux ne peut s'opposer à la visite.

La visite s'effectue sous l'autorité et le contrôle du juge des libertés et de la détention qui l'a autorisée, en présence de l'occupant des lieux ou de son représentant qui peut se faire assister d'un conseil de son choix ou, à défaut, en présence de deux témoins qui ne sont pas placés sous l'autorité des personnes chargées de procéder au contrôle.

L'ordonnance ayant autorisé la visite est exécutoire au seul vu de la minute. Elle mentionne que le juge ayant autorisé la visite peut être saisi à tout moment d'une demande de suspension ou d'arrêt de cette visite. Elle indique le délai et la voie de recours. Elle peut faire l'objet, suivant les règles prévues par le code de procédure civile, d'un appel devant le premier président de la cour d'appel. Celui-ci connaît également des recours contre le déroulement des opérations de visite dont la finalité est l'exercice effectif des missions prévues au III.

**III.** - Pour l'exercice des missions relevant de la Commission nationale de l'informatique et des libertés en application du règlement (UE) 2016/679 du 27 avril 2016 et de la présente loi, les membres et agents mentionnés au premier alinéa du I du présent article peuvent demander communication de tous documents nécessaires à l'accomplissement de leur mission, quel qu'en soit le support, et en prendre copie. Ils peuvent recueillir, notamment sur place ou sur convocation, tout renseignement et toute justification utiles et nécessaires à l'accomplissement de leur mission. Ils peuvent accéder, dans des conditions préservant la confidentialité à l'égard des tiers, aux programmes informatiques et aux données ainsi qu'en demander la transcription par tout traitement approprié dans des documents directement utilisables pour les besoins du contrôle. Le secret ne peut leur être opposé sauf concernant les informations

couvertes par le secret professionnel applicable aux relations entre un avocat et son client, par le secret des sources des traitements journalistiques ou, sous réserve du deuxième alinéa du présent III, par le secret médical.

Le secret médical est opposable s'agissant des informations qui figurent dans un traitement nécessaire aux fins de la médecine préventive, de la recherche médicale, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de service de santé. La communication des données médicales individuelles incluses dans cette catégorie de traitement ne peut alors se faire que sous l'autorité et en présence d'un médecin.

En dehors des contrôles sur place et sur convocation, ils peuvent procéder à toute constatation utile. Ils peuvent notamment, à partir d'un service de communication au public en ligne, consulter les données librement accessibles ou rendues accessibles, y compris par imprudence, par négligence ou par le fait d'un tiers, le cas échéant en accédant et en se maintenant dans des systèmes de traitement automatisé de données le temps nécessaire aux constatations. Ils peuvent retranscrire les données par tout traitement approprié dans des documents directement utilisables pour les besoins du contrôle.

Pour le contrôle de services de communication au public en ligne, les membres et agents mentionnés au premier alinéa du I peuvent réaliser toute opération en ligne nécessaire à leur mission sous une identité d'emprunt. A peine de nullité, leurs actes ne peuvent constituer une incitation à commettre une infraction. L'utilisation d'une identité d'emprunt est sans incidence sur la régularité des constatations effectuées conformément au troisième alinéa du présent III. Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, précise les conditions dans lesquelles ces membres et agents procèdent dans ces cas à leurs constatations.

Les membres et agents mentionnés au premier alinéa du I peuvent, à la demande du président de la commission, être assistés par des experts.

Il est dressé procès-verbal des vérifications et visites menées en application du présent article. Ce procès-verbal est dressé contradictoirement lorsque les vérifications et visites sont effectuées sur place ou sur convocation.

**IV.** - Pour les traitements intéressant la sûreté de l'Etat et qui sont dispensés de la publication de l'acte réglementaire qui les autorise en application du III de l'article 31, le décret en Conseil d'Etat qui prévoit cette dispense peut également prévoir que le traitement n'est pas soumis aux dispositions du présent article.

**V.** - Dans l'exercice de son pouvoir de contrôle portant sur les traitements relevant du règlement (UE) 2016/679 du 27 avril 2016 et de la présente loi, la Commission nationale de l'informatique et des libertés n'est pas compétente pour contrôler les opérations de traitement effectuées, dans l'exercice de leur fonction juridictionnelle, par les juridictions.

### **Section 3 : Mesures correctrices et sanctions**

**I.** - Le président de la Commission nationale de l'informatique et des libertés peut avertir un responsable de traitement ou son sous-traitant du fait que les opérations de traitement envisagées sont susceptibles de violer les dispositions du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi.

**II.** - Lorsque le responsable de traitement ou son sous-traitant ne respecte pas les obligations résultant du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut, si le manquement constaté est susceptible de faire l'objet d'une mise en conformité, prononcer à son égard une mise en demeure, dans le délai qu'il fixe :

1° De satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits ;

2° De mettre les opérations de traitement en conformité avec les dispositions applicables ;

3° A l'exception des traitements qui intéressent la sûreté de l'Etat ou la défense, de communiquer à la personne concernée une violation de données à caractère personnel ;

4° De rectifier ou d'effacer des données à caractère personnel, ou de limiter le traitement de ces données.

Dans le cas prévu au 4° du présent II, le président peut, dans les mêmes conditions, mettre en demeure le responsable de traitement ou son sous-traitant de notifier aux destinataires des données les mesures qu'il a prises.

Le délai de mise en conformité peut être fixé à vingt-quatre heures en cas d'extrême urgence.

Le président prononce, le cas échéant, la clôture de la procédure de mise en demeure.

Le président peut demander au bureau de rendre publique la mise en demeure. Dans ce cas, la décision de clôture de la procédure de mise en demeure fait l'objet de la même publicité.

**III.** - Lorsque le responsable de traitement ou son sous-traitant ne respecte pas les obligations résultant du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut également, le cas échéant après lui avoir adressé l'avertissement prévu au I du présent article ou, le cas échéant en complément d'une mise en demeure prévue au II, saisir la formation restreinte de la commission en vue du prononcé, après procédure contradictoire, de l'une ou de plusieurs des mesures suivantes :

1° Un rappel à l'ordre ;

2° Une injonction de mettre en conformité le traitement avec les obligations résultant du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi ou

de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits, qui peut être assortie, sauf dans des cas où le traitement est mis en œuvre par l'Etat, d'une astreinte dont le montant ne peut excéder 100 000 € par jour de retard à compter de la date fixée par la formation restreinte ;

3° A l'exception des traitements qui intéressent la sûreté de l'Etat ou la défense ou de ceux relevant du titre III de la présente loi lorsqu'ils sont mis en œuvre pour le compte de l'Etat, la limitation temporaire ou définitive du traitement, son interdiction ou le retrait d'une autorisation accordée en application du même règlement ou de la présente loi ;

4° Le retrait d'une certification ou l'injonction, à l'organisme certificateur concerné, de refuser une certification ou de retirer la certification accordée ;

5° A l'exception des traitements qui intéressent la sûreté de l'Etat ou la défense ou de ceux relevant du titre III de la présente loi lorsqu'ils sont mis en œuvre pour le compte de l'Etat, la suspension des flux de données adressées à un destinataire situé dans un pays tiers ou à une organisation internationale ;

6° La suspension partielle ou totale de la décision d'approbation des règles d'entreprise contraignantes ;

7° A l'exception des cas où le traitement est mis en œuvre par l'Etat, une amende administrative ne pouvant excéder 10 millions d'euros ou, s'agissant d'une entreprise, 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu. Dans les hypothèses mentionnées aux 5 et 6 de l'article 83 du règlement (UE) 2016/679 du 27 avril 2016, ces plafonds sont portés, respectivement, à 20 millions d'euros et 4 % dudit chiffre d'affaires. La formation restreinte prend en compte, dans la détermination du montant de l'amende, les critères précisés au même article 83.

Le projet de mesure est, le cas échéant, soumis aux autres autorités de contrôle concernées selon les modalités définies à l'article 60 du même règlement.

#### **Article 21**

**I.** - Lorsque le non-respect des dispositions du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi entraîne une violation des droits et libertés mentionnés à l'article 1er de la présente loi et que le président de la commission considère qu'il est urgent d'intervenir, il saisit la formation restreinte, qui peut, dans le cadre d'une procédure d'urgence contradictoire définie par décret en Conseil d'Etat, adopter l'une des mesures suivantes :

1° L'interruption provisoire de la mise en œuvre du traitement, y compris d'un transfert de données hors de l'Union européenne, pour une durée maximale de trois mois, si le traitement n'est pas au nombre de ceux qui intéressent la sûreté de l'Etat ou la défense ou de ceux relevant du titre III lorsqu'ils sont mis en œuvre pour le compte de l'Etat ;

2° La limitation du traitement de certaines des données à caractère personnel

traitées, pour une durée maximale de trois mois, si le traitement n'est pas au nombre de ceux qui intéressent la sûreté de l'Etat ou la défense ou de ceux relevant du titre III lorsqu'ils sont mis en œuvre pour le compte de l'Etat ;

3° La suspension provisoire de la certification délivrée au responsable de traitement ou à son sous-traitant ;

4° La suspension provisoire de l'agrément délivré à un organisme de certification ou un organisme chargé du respect d'un code de conduite ;

5° La suspension provisoire de l'autorisation délivrée sur le fondement du III de l'article 66 de la présente loi ;

6° L'injonction de mettre en conformité le traitement avec les obligations résultant du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi ou de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits, qui peut être assortie, sauf dans le cas où le traitement est mis en œuvre par l'Etat, d'une astreinte dont le montant ne peut excéder 100 000 € par jour de retard à compter de la date fixée par la formation restreinte ;

7° Un rappel à l'ordre ;

8° L'information du Premier ministre pour qu'il prenne, le cas échéant, les mesures permettant de faire cesser la violation constatée, si le traitement en cause est au nombre de ceux qui intéressent la sûreté de l'Etat ou la défense ou de ceux relevant du titre III de la présente loi lorsqu'ils sont mis en œuvre pour le compte de l'Etat. Le Premier ministre fait alors connaître à la formation restreinte les suites qu'il a données à cette information au plus tard quinze jours après l'avoir reçue.

**II.** - En cas de circonstances exceptionnelles prévues au 1 de l'article 66 du règlement (UE) 2016/679 du 27 avril 2016, lorsque la formation restreinte adopte les mesures provisoires prévues aux 1° à 4° du I du présent article, elle informe sans délai de la teneur des mesures prises et de leurs motifs les autres autorités de contrôle concernées, le comité européen de la protection des données mentionné à l'article 68 du même règlement et la Commission européenne.

Lorsque la formation restreinte a pris de telles mesures et qu'elle estime que des mesures définitives doivent être prises, elle met en œuvre les dispositions du 2 de l'article 66 du règlement (UE) 2016/679 du 27 avril 2016.

**III.** - Pour les traitements relevant du règlement (UE) 2016/679 du 27 avril 2016, lorsqu'une autorité de contrôle compétente en application du même règlement n'a pas pris de mesure appropriée dans une situation où il est urgent d'intervenir afin de protéger les droits et libertés des personnes concernées, la formation restreinte, saisie par le président de la commission, peut demander au comité européen de la protection des données un avis d'urgence ou une décision contraignante d'urgence dans les conditions et selon les modalités prévues aux 3 et 4 de l'article 66 dudit règlement.

**IV.** - En cas d'atteinte grave et immédiate aux droits et libertés mentionnés à

l'article 1er de la présente loi, le président de la commission peut en outre demander, par la voie du référé, à la juridiction compétente d'ordonner, le cas échéant sous astreinte, toute mesure nécessaire à la sauvegarde de ces droits et libertés.

#### **Article 22**

Les mesures prévues au III de l'article 20 et aux 1° à 7° du I de l'article 21 de la présente loi sont prononcées sur la base d'un rapport établi par l'un des membres de la Commission nationale de l'informatique et des libertés, désigné par le président de celle-ci parmi les membres n'appartenant pas à la formation restreinte. Ce rapport est notifié au responsable de traitement ou à son sous-traitant, qui peut déposer des observations et se faire représenter ou assister. Le rapporteur peut présenter des observations orales à la formation restreinte mais ne prend pas part à ses délibérations. La formation restreinte peut entendre toute personne dont l'audition lui paraît susceptible de contribuer utilement à son information, y compris les agents des services de la commission.

La formation restreinte peut rendre publiques les mesures qu'elle prend. Elle peut également ordonner leur insertion dans des publications, journaux et supports qu'elle désigne, aux frais des personnes sanctionnées.

Sans préjudice des obligations d'information qui incombent au responsable de traitement ou à son sous-traitant en application de l'article 34 du règlement (UE) 2016/679 du 27 avril 2016, la formation restreinte peut ordonner que ce responsable ou ce sous-traitant informe individuellement, à ses frais, chacune des personnes concernées de la violation relevée des dispositions de la présente loi ou du règlement précité ainsi que, le cas échéant, de la mesure prononcée.

Lorsque la formation restreinte a prononcé une sanction pécuniaire devenue définitive avant que le juge pénal ait statué définitivement sur les mêmes faits ou des faits connexes, celui-ci peut ordonner que l'amende administrative s'impute sur l'amende pénale qu'il prononce.

L'astreinte est liquidée par la formation restreinte, qui en fixe le montant définitif.

Les sanctions pécuniaires et les astreintes sont recouvrées comme les créances de l'Etat étrangères à l'impôt et au domaine.

#### **Article 23**

Lorsqu'un organisme de certification ou un organisme chargé du respect d'un code de conduite a manqué à ses obligations ou n'a pas respecté les dispositions du règlement (UE) 2016/679 du 27 avril 2016 ou celles de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut, le cas échéant après mise en demeure, saisir la formation restreinte de la commission, qui peut prononcer, dans les mêmes conditions que celles prévues aux articles 20 à 22, le retrait de l'agrément qui a été délivré à cet organisme.

*NOTA : Conformément à l'article 29 de l'ordonnance n° 2018-1125 du 12 décembre 2018, ces dispositions entrent en vigueur en même temps que le décret modifiant le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dans sa rédaction résultant de la présente ordonnance, et au plus tard le 1er juin 2019.*

## **Section 4 : Coopération**

### **Article 24**

Dans les conditions prévues aux articles 60 à 67 du règlement (UE) 2016/679 du 27 avril 2016, la Commission nationale de l'informatique et des libertés met en œuvre des procédures de coopération et d'assistance mutuelle avec les autorités de contrôle des autres Etats membres de l'Union européenne et réalise avec ces autorités des opérations conjointes.

La commission, le président, le bureau, la formation restreinte et les agents de la commission mettent en œuvre, chacun pour ce qui le concerne, les procédures mentionnées au premier alinéa du présent article.

La commission peut charger le bureau :

1° D'exercer ses prérogatives en tant qu'autorité concernée, au sens de l'article 4 du règlement (UE) 2016/679 du 27 avril 2016, et en particulier d'émettre une objection pertinente et motivée au projet de décision d'une autre autorité de contrôle ;

2° Lorsque la commission adopte un projet de décision en tant qu'autorité chef de file ou autorité concernée, de mettre en œuvre les procédures de coopération, de contrôle de la cohérence et de règlement des litiges prévues par le règlement (UE) 2016/679 du 27 avril 2016 et d'arrêter la décision au nom de la commission.

### **Article 25**

**I.** - Pour l'application de l'article 62 du règlement (UE) 2016/679 du 27 avril 2016, la Commission nationale de l'informatique et des libertés coopère avec les autorités de contrôle des autres Etats membres de l'Union européenne, dans les conditions prévues au présent article.

**II.** - Qu'elle agisse en tant qu'autorité de contrôle concernée ou en tant qu'autorité chef de file au sens des articles 4 et 56 du règlement (UE) 2016/679 du 27 avril 2016, la Commission nationale de l'informatique et des libertés est compétente pour traiter une réclamation ou une éventuelle violation des dispositions du même règlement affectant par ailleurs d'autres Etats membres. Le président de la commission invite les autres autorités de contrôle concernées à participer aux opérations de contrôle conjointes qu'il décide de conduire.

**III.** - Lorsqu'une opération de contrôle conjointe se déroule sur le territoire

français, des membres ou agents habilités de la commission, agissant en tant qu'autorité de contrôle d'accueil, sont présents aux côtés des membres et agents des autres autorités de contrôle participant, le cas échéant, à l'opération. A la demande de l'autorité de contrôle d'un Etat membre, le président de la commission peut habiliter, par décision particulière, ceux des membres ou agents de l'autorité de contrôle concernée qui présentent des garanties comparables à celles requises des agents de la commission, en application de l'article 10 de la présente loi, à exercer, sous son autorité, tout ou partie des pouvoirs de vérification et d'enquête dont disposent les membres et les agents de la commission.

**IV.** - Lorsque la commission est invitée à contribuer à une opération de contrôle conjointe décidée par l'autorité de contrôle d'un autre Etat membre, le président de la commission se prononce sur le principe et les conditions de la participation, désigne les membres et agents habilités et en informe l'autorité requérante dans les conditions prévues à l'article 62 du règlement (UE) 2016/679 du 27 avril 2016.

#### **Article 26**

**I.** - Les traitements relevant du titre III font l'objet d'une coopération entre la Commission nationale de l'informatique et des libertés et les autorités de contrôle des autres Etats membres de l'Union européenne dans les conditions prévues au présent article.

**II.** - La commission communique aux autorités de contrôle des autres Etats membres les informations utiles et leur prête assistance en mettant notamment en œuvre, à leur demande, des mesures de contrôle telles que des mesures de consultation, d'inspection et d'enquête.

La commission répond à une demande d'assistance mutuelle formulée par une autre autorité de contrôle dans les meilleurs délais et au plus tard un mois après réception de la demande contenant toutes les informations nécessaires, notamment sa finalité et ses motifs. Elle ne peut refuser de satisfaire à cette demande que si elle n'est pas compétente pour traiter l'objet de la demande ou les mesures qu'elle est invitée à exécuter, ou si une disposition du droit de l'Union européenne ou du droit français y fait obstacle.

La commission informe l'autorité de contrôle requérante des résultats obtenus ou, selon le cas, de l'avancement du dossier ou des mesures prises pour donner suite à la demande.

La commission peut, pour l'exercice de ses missions, solliciter l'assistance d'une autorité de contrôle d'un autre Etat membre de l'Union européenne.

La commission donne les motifs de tout refus de satisfaire à une demande lorsqu'elle estime ne pas être compétente ou lorsqu'elle considère que satisfaire à la demande constituerait une violation du droit de l'Union européenne ou du droit français.

#### **Article 27**

Lorsque la commission agit en tant qu'autorité de contrôle chef de file au sens de l'article 56 du règlement (UE) 2016/679 du 27 avril 2016 s'agissant d'un traitement transfrontalier au sein de l'Union européenne, elle communique sans tarder aux autres autorités de contrôle concernées le rapport du rapporteur mentionné au premier alinéa de l'article 22 ainsi que l'ensemble des informations utiles de la procédure ayant permis d'établir le rapport, avant l'éventuelle audition du responsable de traitement ou de son sous-traitant. Les autorités concernées sont mises en mesure d'assister, par tout moyen de retransmission approprié, à l'audition par la formation restreinte du responsable de traitement ou de son sous-traitant, ou de prendre connaissance d'un procès-verbal dressé à la suite de l'audition.

Après en avoir délibéré, la formation restreinte soumet son projet de décision aux autres autorités de contrôle concernées conformément à la procédure définie à l'article 60 du règlement (UE) 2016/679 du 27 avril 2016. A ce titre, elle se prononce sur la prise en compte des objections pertinentes et motivées émises par ces autorités et saisit, si elle décide d'écarter l'une des objections, le comité européen de la protection des données conformément à l'article 65 du même règlement.

Les conditions d'application du présent article sont définies par décret en Conseil d'Etat, après avis de la Commission nationale de l'informatique et des libertés.

#### **Article 28**

Lorsque la commission agit en tant qu'autorité de contrôle concernée, au sens de l'article 4 du règlement (UE) 2016/679 du 27 avril 2016, le président de la commission est saisi des projets de mesures correctrices soumis à la commission par une autorité de contrôle chef de file.

Lorsque ces mesures sont d'objet équivalent à celles définies aux I et II de l'article 20 de la présente loi, le président décide, le cas échéant, d'émettre une objection pertinente et motivée, selon les modalités prévues à l'article 60 du même règlement.

Lorsque ces mesures sont d'objet équivalent à celles définies au III de l'article 20 de la présente loi, le président saisit la formation restreinte. Le président de la formation restreinte ou le membre de la formation restreinte qu'il désigne peut, le cas échéant, émettre une objection pertinente et motivée selon les mêmes modalités.

#### **Article 29**

La Commission nationale de l'informatique et des libertés peut, à la demande d'une autorité exerçant des compétences analogues aux siennes dans un Etat non membre de l'Union européenne, sous réserve de garanties appropriées pour la protection des données à caractère personnel et d'autres libertés et droits fondamentaux, procéder à des vérifications dans les mêmes conditions que celles prévues à l'article 19, sauf s'il s'agit d'un traitement mentionné aux I ou II

de l'article 31. Sous les mêmes réserves, elle peut présenter des demandes aux mêmes fins à une autorité exerçant des compétences analogues aux siennes.

La commission est habilitée à communiquer les informations qu'elle recueille ou qu'elle détient, à leur demande, aux autorités exerçant des compétences analogues aux siennes dans des Etats non membres de l'Union européenne, sous réserve de garanties appropriées pour la protection des données à caractère personnel et d'autres libertés et droits fondamentaux, sauf s'il s'agit d'un traitement mentionné aux I ou II de l'article 31.

Pour la mise en œuvre du présent article, la commission conclut préalablement une convention organisant ses relations avec l'autorité exerçant des compétences analogues aux siennes. Cette convention est publiée au Journal officiel.

### **Chapitre III : Dispositions particulières relatives au numéro d'inscription des personnes au répertoire national d'identification des personnes physiques**

#### **Article 30**

Un décret en Conseil d'Etat, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés, détermine les catégories de responsables de traitement et les finalités de ces traitements au vu desquelles ces derniers peuvent être mis en œuvre lorsqu'ils portent sur des données comportant le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques. La mise en œuvre des traitements intervient sans préjudice des obligations qui incombent aux responsables de traitement ou à leurs sous-traitants en application de la section 3 du chapitre IV du règlement (UE) 2016/679 du 27 avril 2016.

N'entrent pas dans le champ d'application du premier alinéa du présent article ceux des traitements portant sur des données à caractère personnel parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques ou qui requièrent une consultation de ce répertoire :

1° Qui ont exclusivement des finalités de statistique publique, sont mis en œuvre par le service statistique public et ne comportent aucune des données mentionnées au I de l'article 6 ou à l'article 46 ;

2° Qui ont exclusivement des finalités de recherche scientifique ou historique ;

3° Qui ont pour objet de mettre à la disposition des usagers de l'administration un ou plusieurs téléservices de l'administration électronique définis à l'article 1er de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives au sens de ce même article 1er, et entre ces mêmes autorités administratives.

La dérogation prévue pour les traitements dont les finalités sont mentionnées

aux 1° et 2° du présent article, n'est applicable que si le numéro d'inscription au répertoire national d'identification des personnes physiques fait préalablement l'objet d'une opération cryptographique lui substituant un code statistique non significatif. Cette opération est renouvelée à une fréquence définie par décret en Conseil d'Etat, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés. Les traitements ayant comme finalité exclusive de réaliser cette opération cryptographique ne sont pas soumis au premier alinéa.

Pour les traitements dont les finalités sont mentionnées au 1°, l'utilisation du code statistique non significatif n'est autorisée qu'au sein du service statistique public.

Pour les traitements dont les finalités sont mentionnées au 2°, l'opération cryptographique et, le cas échéant, l'interconnexion de deux fichiers par l'utilisation du code spécifique non significatif qui en est issu ne peuvent être assurées par la même personne ni par le responsable de traitement.

Par dérogation au premier alinéa, les traitements de données à caractère personnel dans le domaine de la santé sont régis par la section 3 du chapitre III du titre II, à l'exception :

1° Des traitements mentionnés à l'article 67 ;

2° Des traitements comportant le numéro d'inscription au répertoire national d'identification des personnes physiques utilisé comme identifiant de santé des personnes en application de l'article L. 1111-8-1 du code de la santé publique, en dehors de ceux de ces traitements mis en œuvre à des fins de recherche.

## **Chapitre IV : Formalités préalables à la mise en oeuvre des traitements.**

### **Article 31**

**I.** - Sont autorisés par arrêté du ou des ministres compétents, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés, les traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat et :

1° Qui intéressent la sûreté de l'Etat, la défense ou la sécurité publique ;

2° Ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté.

L'avis de la commission est publié avec l'arrêté autorisant le traitement.

**II.** - Ceux de ces traitements qui portent sur des données mentionnées au I de l'article 6 sont autorisés par décret en Conseil d'Etat pris après avis motivé et publié de la commission. Cet avis est publié avec le décret autorisant le traitement.

**III.** - Certains traitements mentionnés au I et au II peuvent être dispensés, par décret en Conseil d'Etat, de la publication de l'acte réglementaire qui les autorise. Pour ces traitements, est publié, en même temps que le décret autorisant la dispense de publication de l'acte, le sens de l'avis émis par la commission.

**IV.** - Pour l'application du présent article, les traitements qui répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires peuvent être autorisés par un acte réglementaire unique. Dans ce cas, le responsable de chaque traitement adresse à la commission un engagement de conformité de celui-ci à la description figurant dans l'autorisation.

#### **Article 32**

Sont autorisés par décret en Conseil d'Etat, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés, les traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat, agissant dans l'exercice de ses prérogatives de puissance publique, qui portent sur des données génétiques ou sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes.

#### **Article 33**

**I.** - Les demandes d'avis adressées à la Commission nationale de l'informatique et des libertés en vertu de la présente loi précisent :

1° L'identité et l'adresse du responsable du traitement ou, si celui-ci n'est établi ni sur le territoire national ni sur celui d'un autre Etat membre de l'Union européenne, celle de son représentant et, le cas échéant, celle de la personne qui présente la demande ;

2° La ou les finalités du traitement, ainsi que, pour les traitements relevant des articles 31 et 32, la description générale de ses fonctions ;

3° Le cas échéant, les interconnexions, les rapprochements ou toutes autres formes de mise en relation avec d'autres traitements ;

4° Les données à caractère personnel traitées, leur origine et les catégories de personnes concernées par le traitement ;

5° La durée de conservation des informations traitées ;

6° Le ou les services chargés de mettre en œuvre le traitement ainsi que, pour les traitements relevant des articles 31 et 32, les catégories de personnes qui, en raison de leurs fonctions ou pour les besoins du service, ont directement accès aux données enregistrées ;

7° Les destinataires ou catégories de destinataires habilités à recevoir communication des données ;

8° La fonction de la personne ou le service auprès duquel s'exerce le droit d'accès prévu aux articles 49,105 et 119, ainsi que les mesures relatives à l'exercice de ce droit ;

9° Les dispositions prises pour assurer la sécurité des traitements et des données et la garantie des secrets protégés par la loi et, le cas échéant, l'indication du recours à un sous-traitant ;

10° Le cas échéant, les transferts de données à caractère personnel envisagés à destination d'un Etat non membre de l'Union européenne, sous quelque forme que ce soit.

Les demandes d'avis portant sur les traitements intéressant la sûreté de l'Etat, la défense ou la sécurité publique peuvent ne pas comporter tous les éléments d'information énumérés ci-dessus. Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, fixe la liste de ces traitements et des informations que les demandes d'avis portant sur ces traitements doivent comporter au minimum.

**II.** - Le responsable d'un traitement déjà autorisé et susceptible de faire l'objet d'une mise à jour rendue publique dans les conditions prévues à l'article 36 informe sans délai la commission :

1° De tout changement affectant les informations mentionnées au I ;

2° De toute suppression du traitement.

#### **Article 34**

**I.** - La Commission nationale de l'informatique et des libertés, saisie dans le cadre des articles 31 ou 32, se prononce dans un délai de huit semaines à compter de la réception de la demande. Toutefois, ce délai peut être renouvelé de six semaines sur décision motivée du président.

**II.** - L'avis demandé à la commission sur un traitement, qui n'est pas rendu à l'expiration du délai prévu au I, est réputé favorable.

#### **Article 35**

Les actes autorisant la création d'un traitement en application des articles 31 et 32 précisent :

1° La finalité du traitement et, le cas échéant, sa dénomination ;

2° Le service auprès duquel s'exerce le droit d'accès prévu aux articles 49,105 et 119 ;

3° Les catégories de données à caractère personnel enregistrées ;

4° Les destinataires ou catégories de destinataires habilités à recevoir communication de ces données ;

5° Le cas échéant, les dérogations à l'obligation d'information prévues au III de l'article 116 ;

6° Le cas échéant, les limitations et restrictions aux droits des personnes concernées prévues à l'article 23 du règlement (UE) 2016/679 du 27 avril 2016 et à l'article 107.

7° Le cas échéant, la désignation, parmi les responsables conjoints du traitement, du point de contact pour les personnes concernées.

#### **Article 36**

**I.** - La commission met à la disposition du public, dans un format ouvert et aisément réutilisable, la liste des traitements automatisés ayant fait l'objet d'une des formalités prévues par les articles 31 et 32, à l'exception de ceux mentionnés au III de l'article 31, ainsi que par la section 3 du chapitre III du titre II.

Cette liste précise pour chacun de ces traitements :

1° L'acte décidant la création du traitement ;

2° La finalité du traitement et, le cas échéant la dénomination ;

3° L'identité et l'adresse du responsable du traitement ou, si celui-ci n'est établi ni sur le territoire national ni sur celui d'un autre Etat membre de l'Union européenne, celles de son représentant ;

4° La fonction de la personne ou le service auprès duquel s'exerce le droit d'accès prévu aux articles 49,105 et 119 ;

5° Les catégories de données à caractère personnel faisant l'objet du traitement, ainsi que les destinataires et catégories de destinataires habilités à en recevoir communication ;

6° Le cas échéant, les transferts de données à caractère personnel envisagés à destination d'un Etat non membre de l'Union européenne.

**II.** - La commission tient à la disposition du public ses avis, décisions ou recommandations.

## **Chapitre V : Obligations incombant aux responsables de traitements et droits des personnes**

#### **Article 37**

**I.** - Sous réserve du présent article, le chapitre Ier du titre V de la loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXI<sup>e</sup> siècle et le chapitre X du titre VII du livre VII du code de justice administrative s'appliquent à l'action ouverte sur le fondement du présent article.

**II.** - Lorsque plusieurs personnes physiques placées dans une situation similaire

subissent un dommage ayant pour cause commune un manquement de même nature aux dispositions du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi par un responsable de traitement de données à caractère personnel ou un sous-traitant, une action de groupe peut être exercée devant la juridiction civile ou la juridiction administrative compétente au vu des cas individuels présentés par le demandeur, qui en informe la Commission nationale de l'informatique et des libertés.

**III.** - Cette action peut être exercée en vue soit de faire cesser le manquement mentionné au II, soit d'engager la responsabilité de la personne ayant causé le dommage afin d'obtenir la réparation des préjudices matériels et moraux subis, soit de ces deux fins.

Toutefois, la responsabilité de la personne ayant causé le dommage ne peut être engagée que si le fait générateur du dommage est postérieur au 24 mai 2018.

**IV.** - Peuvent seules exercer cette action :

1° Les associations régulièrement déclarées depuis cinq ans au moins ayant dans leur objet statutaire la protection de la vie privée ou la protection des données à caractère personnel ;

2° Les associations de défense des consommateurs représentatives au niveau national et agréées en application de l'article L. 811-1 du code de la consommation, lorsque le traitement de données à caractère personnel affecte des consommateurs ;

3° Les organisations syndicales de salariés ou de fonctionnaires représentatives au sens des articles L. 2122-1, L. 2122-5 ou L. 2122-9 du code du travail ou du III de l'article 8 bis de la loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires ou les syndicats représentatifs de magistrats de l'ordre judiciaire, lorsque le traitement affecte les intérêts des personnes que les statuts de ces organisations les chargent de défendre.

Lorsque l'action tend à la réparation des préjudices subis, elle s'exerce dans le cadre de la procédure individuelle de réparation définie au chapitre Ier du titre V de la loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXI<sup>e</sup> siècle et au chapitre X du titre VII du livre VII du code de justice administrative.

#### **Article 38**

Toute personne peut mandater une association ou une organisation mentionnée au IV de l'article 37, une association ou une organisation dont l'objet statutaire est en relation avec la protection des droits et libertés lorsque ceux-ci sont méconnus dans le cadre d'un traitement de données à caractère personnel, ou une association dont cette personne est membre et dont l'objet statutaire implique la défense d'intérêts en relation avec les finalités du traitement litigieux, aux fins d'exercer en son nom les droits prévus aux articles 77 à 79 et 82 du règlement (UE) 2016/679 du 27 avril 2016. Elle peut également les mandater pour agir devant la Commission nationale de l'informatique et des

libertés, contre celle-ci devant un juge ou contre le responsable de traitement ou son sous-traitant devant une juridiction lorsqu'est en cause un traitement relevant du titre III de la présente loi.

#### **Article 39**

Dans le cas où, saisie d'une réclamation dirigée contre un responsable de traitement ou son sous-traitant, la Commission nationale de l'informatique et des libertés estime fondés les griefs avancés relatifs à la protection des droits et libertés d'une personne à l'égard du traitement de ses données à caractère personnel, ou de manière générale afin d'assurer la protection de ces droits et libertés dans le cadre de sa mission, elle peut demander au Conseil d'Etat d'ordonner, le cas échéant sous astreinte, soit la suspension d'un transfert de données, soit la prolongation de la suspension d'un tel transfert qu'elle aurait elle-même préalablement ordonnée, et elle assortit alors ses conclusions d'une demande de question préjudicielle à la Cour de justice de l'Union européenne en vue d'apprécier la validité de la décision d'adéquation de la Commission européenne prise sur le fondement de l'article 45 du règlement (UE) 2016/679 du 27 avril 2016 ainsi que de tous les actes pris par la Commission européenne relativement aux garanties appropriées dans le cadre des transferts de données mentionnées à l'article 46 du même règlement.

Lorsque le transfert de données en cause ne constitue pas une opération de traitement effectuée par une juridiction dans l'exercice de sa fonction juridictionnelle, la Commission nationale de l'informatique et des libertés peut saisir, dans les mêmes conditions, le Conseil d'Etat aux fins d'ordonner, soit la suspension du transfert de données fondé sur une décision d'adéquation de la Commission européenne prise sur le fondement de l'article 36 de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016, soit la prolongation de la suspension de ce transfert qu'elle aurait elle-même déjà ordonnée, dans l'attente de l'appréciation par la Cour de justice de l'Union européenne de la validité de cette décision d'adéquation.

## **Chapitre VI : Dispositions pénales**

#### **Article 40**

Les infractions aux dispositions de la présente loi sont prévues par la section 5 du chapitre VI du titre II du livre II du code pénal.

#### **Article 41**

Le procureur de la République avise le président de la Commission nationale de l'informatique et des libertés de toutes les poursuites relatives aux infractions prévues par la section 5 du chapitre VI du titre II du livre II du code pénal et, le cas échéant, des suites qui leur sont données. Il l'informe de la date et de l'objet de l'audience de jugement par lettre recommandée adressée au moins dix jours avant cette date.

La juridiction d'instruction ou de jugement peut appeler le président de la Commission nationale de l'informatique et des libertés ou son représentant à déposer ses observations ou à les développer oralement à l'audience.

## **Titre II : Traitements relevant du régime de protection des données à caractère personnel prévu par le règlement (UE) 2016/679 du 27 avril 2016**

### **Chapitre Ier : Dispositions générales**

#### **Article 42**

**I.** -Le présent titre ne s'applique pas aux traitements de données à caractère personnel effectués :

1° Dans le cadre d'une activité qui ne relève pas du champ d'application du droit de l'Union européenne, notamment les traitements mentionnés au titre IV ;

2° Dans le cadre d'activités qui relèvent du champ d'application du chapitre II du titre V du traité sur l'Union européenne ;

3° Par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces ;

4° Aux copies temporaires qui sont faites dans le cadre des activités techniques de transmission et de fourniture d'accès à un réseau numérique, en vue du stockage automatique, intermédiaire et transitoire des données et à seule fin de permettre à d'autres destinataires du service le meilleur accès possible aux informations transmises.

**II.** -Le présent titre s'applique sans préjudice des articles 32-3-3,32-3-4 et 34-4 du code des postes et des télécommunications relatifs à la responsabilité des prestataires de services intermédiaires tels que modifiés par l'article 9 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique et 10 de la loi n° 2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle.

**III.** -Le présent titre s'applique sans préjudice des dispositions de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

#### **Article 43**

Les principes, règles et conditions de licéité d'un traitement de données à caractère personnel applicables sont ceux définis au chapitre II du règlement (UE) 2016/679 du 27 avril 2016 et du chapitre Ier du titre Ier de la présente loi.

#### **Article 44**

L'article 6 ne s'applique pas si l'une des conditions prévues au 2 de l'article 9 du règlement (UE) 2016/679 du 27 avril 2016 est remplie, ainsi que pour :

1° Les traitements nécessaires aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé et mis en œuvre par un membre d'une profession de santé, ou par une autre personne à laquelle s'impose en raison de ses fonctions l'obligation de secret professionnel dont l'atteinte est réprimée par l'article 226-13 du code pénal ;

2° Les traitements statistiques réalisés par l'Institut national de la statistique et des études économiques ou l'un des services statistiques ministériels dans le respect de la loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques, après avis du Conseil national de l'information statistique ;

3° Les traitements comportant des données concernant la santé justifiés par l'intérêt public et conformes aux dispositions de la section 3 du chapitre III du présent titre ;

4° Les traitements conformes aux règlements types mentionnés au c du 2° du I de l'article 8 mis en œuvre par les employeurs ou les administrations qui portent sur des données biométriques strictement nécessaires au contrôle de l'accès aux lieux de travail ainsi qu'aux appareils et aux applications utilisés dans le cadre des missions confiées aux salariés, aux agents, aux stagiaires ou aux prestataires ;

5° Les traitements portant sur la réutilisation des informations publiques figurant dans les décisions mentionnées à l'article L. 10 du code de justice administrative et à l'article L. 111-13 du code de l'organisation judiciaire, sous réserve que ces traitements n'aient ni pour objet ni pour effet de permettre la réidentification des personnes concernées ;

6° Les traitements nécessaires à la recherche publique au sens de l'article L. 112-1 du code de la recherche, sous réserve que des motifs d'intérêt public important les rendent nécessaires, dans les conditions prévues par le g du 2 de l'article 9 du règlement (UE) 2016/679 du 27 avril 2016, après avis motivé et publié de la Commission nationale de l'informatique et des libertés rendu selon les modalités prévues à l'article 34 de la présente loi.

#### **Article 45**

En application du 1 de l'article 8 du règlement (UE) 2016/679 du 27 avril 2016, un mineur peut consentir seul à un traitement de données à caractère personnel en ce qui concerne l'offre directe de services de la société de l'information à compter de l'âge de quinze ans.

Lorsque le mineur est âgé de moins de quinze ans, le traitement n'est licite que si le consentement est donné conjointement par le mineur concerné et le ou les

titulaires de l'autorité parentale à l'égard de ce mineur.

Le responsable de traitement rédige en des termes clairs et simples, aisément compréhensibles par le mineur, les informations et communications relatives au traitement qui le concerne.

#### **Article 46**

Les traitements de données à caractère personnel relatives aux condamnations pénales, aux infractions ou aux mesures de sûreté connexes ne peuvent être effectués que par :

1° Les juridictions, les autorités publiques et les personnes morales gérant un service public, agissant dans le cadre de leurs attributions légales ainsi que les personnes morales de droit privé collaborant au service public de la justice et appartenant à des catégories dont la liste est fixée par décret en Conseil d'Etat, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés, dans la mesure strictement nécessaire à leur mission ;

2° Les auxiliaires de justice, pour les stricts besoins de l'exercice des missions qui leur sont confiées par la loi ;

3° Les personnes physiques ou morales, aux fins de leur permettre de préparer et, le cas échéant, d'exercer et de suivre une action en justice en tant que victime, mise en cause, ou pour le compte de ceux-ci et de faire exécuter la décision rendue, pour une durée strictement proportionnée à ces finalités. La communication à un tiers n'est alors possible que sous les mêmes conditions et dans la mesure strictement nécessaire à la poursuite de ces mêmes finalités ;

4° Les personnes morales mentionnées aux articles L. 321-1 et L. 331-1 du code de la propriété intellectuelle, agissant au titre des droits dont elles assurent la gestion ou pour le compte des victimes d'atteintes aux droits prévus aux livres Ier, II et III du même code aux fins d'assurer la défense de ces droits ;

5° Les réutilisateurs des informations publiques figurant dans les décisions mentionnées à l'article L. 10 du code de justice administrative et à l'article L. 111-13 du code de l'organisation judiciaire, sous réserve que les traitements mis en œuvre n'aient ni pour objet ni pour effet de permettre la réidentification des personnes concernées.

#### **Article 47**

Aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour fondement un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de la personnalité de cette personne.

Aucune décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative ne peut être prise sur le seul fondement d'un traitement automatisé de données à caractère personnel, y compris le profilage, à l'exception :

1° Des cas mentionnés aux a et c du 2 de l'article 22 du règlement (UE) 2016/679 du 27 avril 2016, sous les réserves mentionnées au 3 du même article 22 et à condition que les règles définissant le traitement ainsi que les principales caractéristiques de sa mise en œuvre soient communiquées, à l'exception des secrets protégés par la loi, par le responsable de traitement à l'intéressé s'il en fait la demande ;

2° Des décisions administratives individuelles prises dans le respect de l'article L. 311-3-1 et du chapitre Ier du titre Ier du livre IV du code des relations entre le public et l'administration, à condition que le traitement ne porte pas sur des données mentionnées au I de l'article 6 de la présente loi. Ces décisions comportent, à peine de nullité, la mention explicite prévue à l'article L. 311-3-1 du code des relations entre le public et l'administration. Pour ces décisions, le responsable de traitement s'assure de la maîtrise du traitement algorithmique et de ses évolutions afin de pouvoir expliquer, en détail et sous une forme intelligible, à la personne concernée la manière dont le traitement a été mis en œuvre à son égard.

Par dérogation au 2° du présent article, aucune décision par laquelle l'administration se prononce sur un recours administratif mentionné au titre Ier du livre IV du code des relations entre le public et l'administration ne peut être prise sur le seul fondement d'un traitement automatisé de données à caractère personnel.

## **Chapitre II : Droits de la personne concernée**

### **Article 48**

Le droit à l'information s'exerce dans les conditions prévues aux articles 12 à 14 du règlement (UE) 2016/679 du 27 avril 2016.

En particulier, lorsque les données à caractère personnel sont collectées auprès d'un mineur de moins de quinze ans, le responsable de traitement transmet au mineur les informations mentionnées à l'article 13 de ce règlement dans un langage clair et facilement accessible.

La personne auprès de laquelle sont recueillies des données à caractère personnel la concernant est également informée, sauf si elle l'a été au préalable, par le responsable du traitement ou son représentant du droit de définir des directives relatives au sort de ses données à caractère personnel après sa mort, dans les conditions prévues à l'article 85.

En application de l'article 23 du même règlement, le droit à l'information ne s'applique pas aux données collectées dans les conditions prévues à l'article 14 de ce règlement et utilisées lors d'un traitement mis en œuvre pour le compte de l'Etat et intéressant la sécurité publique, dans la mesure où une telle limitation est nécessaire au respect des fins poursuivies par ce traitement et prévue par l'acte instaurant le traitement.

Il est fait application des dispositions de l'alinéa précédent lorsque le traitement est mis en œuvre par les administrations publiques qui ont pour mission soit de

contrôler ou de recouvrer des impositions soit d'effectuer des contrôles de l'activité de personnes physiques ou morales pouvant donner lieu à la constatation d'une infraction ou d'un manquement, à des amendes administratives ou à des pénalités.

#### **Article 49**

Le droit d'accès de la personne concernée s'exerce dans les conditions prévues à l'article 15 du règlement (UE) 2016/679 du 27 avril 2016.

En cas de risque de dissimulation ou de disparition des données à caractère personnel, le juge compétent peut ordonner, y compris en référé, toutes mesures de nature à éviter cette dissimulation ou cette disparition.

Les dispositions du premier alinéa ne s'appliquent pas lorsque les données à caractère personnel sont conservées sous une forme excluant manifestement tout risque d'atteinte à la vie privée et à la protection des données des personnes concernées et pendant une durée n'excédant pas celle nécessaire aux seules finalités d'établissement de statistiques ou de réalisation de recherche scientifique ou historique.

#### **Article 50**

Le droit de rectification s'exerce dans les conditions prévues à l'article 16 du règlement (UE) 2016/679 du 27 avril 2016.

#### **Article 51**

I.-Le droit à l'effacement s'exerce dans les conditions prévues à l'article 17 du règlement (UE) 2016/679 du 27 avril 2016.

II.-En particulier, sur demande de la personne concernée, le responsable du traitement est tenu d'effacer dans les meilleurs délais les données à caractère personnel qui ont été collectées dans le cadre de l'offre de services de la société de l'information lorsque la personne concernée était mineure au moment de la collecte. Lorsqu'il a transmis les données en cause à un tiers lui-même responsable de traitement, il prend des mesures raisonnables, y compris d'ordre technique, compte tenu des technologies disponibles et des coûts de mise en œuvre, pour informer le tiers qui traite ces données que la personne concernée a demandé l'effacement de tout lien vers celles-ci, ou de toute copie ou de toute reproduction de celles-ci.

En cas de non-exécution de l'effacement des données à caractère personnel ou en cas d'absence de réponse du responsable du traitement dans un délai d'un mois à compter de la demande, la personne concernée peut saisir la Commission nationale de l'informatique et des libertés, qui se prononce sur cette demande dans un délai de trois semaines à compter de la date de réception de la réclamation.

#### **Article 52**

Par dérogation aux articles 49 à 51, pour les traitements mis en œuvre par les administrations publiques et les personnes privées chargées d'une mission de service public qui ont pour mission de contrôler ou recouvrer des impositions, les droit d'accès, de rectification et d'effacement s'exercent dans les conditions prévues à l'article 118, si de telles restrictions ont été prévues par l'acte instaurant le traitement.

Il est fait application des mêmes dispositions lorsque le traitement intéresse la sécurité publique, sous réserve de l'application des dispositions du titre III.

Par dérogation aux articles 49 à 51, pour les traitements mis en œuvre par les juridictions financières, dans le cadre de leurs missions non juridictionnelles prévues par le code des juridictions financières, notamment lorsque de telles missions sont susceptibles de révéler des irrégularités appelant la mise en œuvre d'une procédure juridictionnelle, le droit d'accès peut être limité dans les conditions prévues aux e et h du 1 de l'article 23 du règlement (UE) 2016/679 du 27 avril 2016.

#### **Article 53**

Le droit à la limitation du traitement s'exerce dans les conditions prévues à l'article 18 du règlement (UE) 2016/679 du 27 avril 2016.

#### **Article 54**

L'obligation de notification en cas de rectification ou d'effacement de données à caractère personnel ou la limitation du traitement s'exerce dans les conditions prévues à l'article 19 du règlement (UE) 2016/679 du 27 avril 2016.

#### **Article 55**

Le droit à la portabilité des données s'exerce dans les conditions prévues à l'article 20 du règlement (UE) 2016/679 du 27 avril 2016.

#### **Article 56**

Le droit d'opposition s'exerce dans les conditions prévues à l'article 21 du règlement (UE) 2016/679 du 27 avril 2016.

Ce droit ne s'applique pas lorsque le traitement répond à une obligation légale ou, dans les conditions prévues à l'article 23 du même règlement, lorsque l'application de ces dispositions a été écartée par une disposition expresse de l'acte instaurant le traitement.

## **Chapitre III : Obligations incombant au responsable du traitement et au sous-traitant**

### **Section 1 : Obligations générales**

#### **Article 57**

En application de l'article 24 du règlement (UE) 2016/679 du 27 avril 2016, le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément à ce même règlement et à la présente loi.

Le responsable du traitement et, le cas échéant, son représentant tiennent le registre des activités de traitement dans les conditions prévues à l'article 30 de ce règlement. Ils désignent un délégué à la protection des données dans les conditions prévues par la section 4 du chapitre IV du même règlement.

#### **Article 58**

**I.** -Le responsable de traitement notifie à la Commission nationale de l'informatique et des libertés et communique à la personne concernée toute violation de données à caractère personnel en application des articles 33 et 34 du règlement (UE) 2016/679 du 27 avril 2016.

**II.** -Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, fixe la liste des traitements et des catégories de traitements autorisés à déroger au droit à la communication d'une violation de données régi par l'article 34 du même règlement lorsque la notification d'une divulgation ou d'un accès non autorisé à ces données est susceptible de représenter un risque pour la sécurité nationale, la défense nationale ou la sécurité publique.

La dérogation prévue au présent article n'est applicable qu'aux seuls traitements de données à caractère personnel nécessaires au respect d'une obligation légale qui requiert le traitement de ces données ou à l'exercice d'une mission d'intérêt public dont est investi le responsable de traitement.

#### **Article 59**

Lorsque les finalités et les moyens du traitement sont déterminés par plusieurs responsables du traitement, leurs obligations respectives s'exercent dans les conditions prévues à l'article 26 du règlement (UE) 2016/679 du 27 avril 2016 et par la présente loi.

#### **Article 60**

La qualité de sous-traitant n'exonère en rien du respect des dispositions applicables du règlement (UE) 2016/679 du 27 avril 2016 et de la présente loi.

Le traitement réalisé par un sous-traitant est régi par un contrat ou tout acte juridique qui lie le sous-traitant à l'égard du responsable du traitement, sous une forme écrite, y compris en format électronique, respectant les conditions prévues à l'article 28 du règlement.

Le sous-traitant et, le cas échéant, son représentant doivent tenir le registre mentionné à l'article 30 de ce même règlement.

Lorsqu'un sous-traitant a recours à un autre sous-traitant pour mener les activités de traitement spécifiques pour le compte du responsable du traitement, il conclut avec ce sous-traitant le contrat mentionné au deuxième alinéa. Le troisième alinéa s'applique également.

#### **Article 61**

Conformément à l'article 29 du règlement (UE) 2016/679 du 27 avril 2016, sauf dispositions législatives ou réglementaires contraires, il est interdit au sous-traitant ou à toute autre personne agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant ayant accès à des données à caractère personnel de traiter ces données sans l'accord du responsable du traitement.

### **Section 2 : Obligations en cas de traitement susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques**

#### **Article 62**

Le responsable du traitement effectue préalablement à la mise en œuvre du traitement une analyse d'impact des opérations de traitement envisagées sur la protection des données à caractère personnel dans les conditions prévues à l'article 35 du règlement (UE) 2016/679 du 27 avril 2016.

#### **Article 63**

Conformément à l'article 36 du règlement (UE) 2016/679 du 27 avril 2016, le responsable du traitement est tenu de consulter la Commission nationale de l'informatique et des libertés préalablement à la mise en œuvre du traitement lorsqu'il ressort de l'analyse d'impact prévue à l'article 62 que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque.

### **Section 3 : Traitements de données à caractère personnel dans le domaine de la santé**

#### **Article 64**

Lorsque l'exercice du droit d'accès s'applique à des données de santé à caractère personnel, celles-ci peuvent être communiquées à la personne concernée, selon son choix, directement ou par l'intermédiaire d'un médecin qu'elle désigne à cet effet, dans le respect des dispositions de l'article L. 1111-7 du code de la santé publique.

#### **Sous-section 1 : Dispositions générales**

#### **Article 65**

Les traitements contenant des données concernant la santé des personnes sont soumis, outre à celles du règlement (UE) 2016/679 du 27 avril 2016, aux dispositions de la présente section, à l'exception des catégories de traitements suivantes :

1° Les traitements relevant du 1° de l'article 44 de la présente loi et des a et c à f du 2 de l'article 9 du règlement (UE) 2016/679 du 27 avril 2016 ;

2° Les traitements permettant d'effectuer des études à partir des données recueillies en application du 1° de l'article 44 de la présente loi lorsque ces études sont réalisées par les personnels assurant ce suivi et destinées à leur usage exclusif ;

3° Les traitements mis en œuvre aux fins d'assurer le service des prestations ou le contrôle par les organismes chargés de la gestion d'un régime de base d'assurance maladie ainsi que la prise en charge des prestations par les organismes d'assurance maladie complémentaire ;

4° Les traitements effectués au sein des établissements de santé par les médecins responsables de l'information médicale, dans les conditions prévues au deuxième alinéa de l'article L. 6113-7 du code de la santé publique ;

5° Les traitements effectués par les agences régionales de santé, par l'Etat et par la personne publique qu'il désigne en application du premier alinéa de l'article L. 6113-8 du même code, dans le cadre défini au même article L. 6113-8.

#### **Article 66**

**I.** -Les traitements relevant de la présente section ne peuvent être mis en œuvre qu'en considération de la finalité d'intérêt public qu'ils présentent. La garantie de normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux constitue une finalité d'intérêt public.

**II.** -Des référentiels et règlements types, au sens des b et c du 2° du I de l'article 8, s'appliquant aux traitements relevant de la présente section sont établis par la Commission nationale de l'informatique et des libertés, en concertation avec l'Institut national des données de santé mentionné à l'article L. 1462-1 du code de la santé publique et des organismes publics et privés représentatifs des acteurs concernés.

Les traitements conformes à ces référentiels peuvent être mis en œuvre à la condition que leurs responsables adressent préalablement à la Commission nationale de l'informatique et des libertés une déclaration attestant de cette conformité.

Ces référentiels peuvent également porter sur la description et les garanties de procédure permettant la mise à disposition en vue de leur traitement de jeux de données de santé présentant un faible risque d'impact sur la vie privée.

**III.** -Les traitements mentionnés au I qui ne sont pas conformes à un référentiel

mentionné au II ne peuvent être mis en œuvre qu'après autorisation de la Commission nationale de l'informatique et des libertés. La demande d'autorisation est présentée dans les formes prévues à l'article 33.

**IV.** -La Commission nationale de l'informatique et des libertés peut, par décision unique, délivrer à un même demandeur une autorisation pour des traitements répondant à une même finalité, portant sur des catégories de données identiques et ayant des catégories de destinataires identiques.

**V.** -La Commission nationale de l'informatique et des libertés se prononce dans un délai de deux mois à compter de la réception de la demande. Toutefois, ce délai peut être prolongé une fois pour la même durée sur décision motivée de son président ou lorsque l'Institut national des données de santé est saisi en application du second alinéa de l'article 72.

Lorsque la Commission nationale de l'informatique et des libertés ne s'est pas prononcée dans ces délais, la demande d'autorisation est réputée acceptée. Cette disposition n'est toutefois pas applicable si l'autorisation fait l'objet d'un avis préalable en application de la sous-section 2 de la présente section et que l'avis ou les avis rendus ne sont pas expressément favorables.

#### **Article 67**

Par dérogation à l'article 66, les traitements de données à caractère personnel dans le domaine de la santé mis en œuvre par les organismes ou les services chargés d'une mission de service public figurant sur une liste fixée par arrêté des ministres chargés de la santé et de la sécurité sociale, pris après avis de la Commission nationale de l'informatique et des libertés, ayant pour seule finalité de répondre, en cas de situation d'urgence, à une alerte sanitaire et d'en gérer les suites, au sens de la section 1 du chapitre III du titre Ier du livre IV de la première partie du code de la santé publique, sont soumis aux seules dispositions de la section 3 du chapitre IV du règlement (UE) 2016/679 du 27 avril 2016.

Les traitements mentionnés au premier alinéa du présent article qui utilisent le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques sont mis en œuvre dans les conditions prévues à l'article 30 de la présente loi.

Les dérogations régies par le premier alinéa du présent article prennent fin un an après la création du traitement si ce dernier continue à être mis en œuvre au-delà de ce délai.

#### **Article 68**

Nonobstant les règles relatives au secret professionnel, les membres des professions de santé peuvent transmettre au responsable d'un traitement de données autorisé en application de l'article 66 les données à caractère personnel qu'ils détiennent.

Lorsque ces données permettent l'identification des personnes, leur

transmission doit être effectuée dans des conditions de nature à garantir leur confidentialité. La Commission nationale de l'informatique et des libertés peut adopter des recommandations ou des référentiels sur les procédés techniques à mettre en œuvre.

Lorsque le résultat du traitement de données est rendu public, l'identification directe ou indirecte des personnes concernées doit être impossible.

Les personnes appelées à mettre en œuvre le traitement de données ainsi que celles qui ont accès aux données sur lesquelles il porte sont astreintes au secret professionnel sous les peines prévues à l'article 226-13 du code pénal.

#### **Article 69**

Les personnes auprès desquelles sont recueillies des données à caractère personnel ou à propos desquelles de telles données sont transmises sont individuellement informées conformément aux dispositions du règlement (UE) 2016/679 du 27 avril 2016.

Toutefois, ces informations peuvent ne pas être délivrées si la personne concernée a entendu faire usage du droit qui lui est reconnu par l'article L. 1111-2 du code de la santé publique d'être laissée dans l'ignorance d'un diagnostic ou d'un pronostic.

#### **Article 70**

Sont destinataires de l'information et exercent les droits de la personne concernée par le traitement les titulaires de l'exercice de l'autorité parentale, pour les mineurs, ou la personne chargée d'une mission de représentation dans le cadre d'une tutelle, d'une habilitation familiale ou d'un mandat de protection future, pour les majeurs protégés dont l'état ne leur permet pas de prendre seuls une décision personnelle éclairée.

Par dérogation au premier alinéa du présent article, pour les traitements de données à caractère personnel réalisés dans le cadre de recherches mentionnées aux 2° et 3° de l'article L. 1121-1 du code de la santé publique ou d'études ou d'évaluations dans le domaine de la santé, ayant une finalité d'intérêt public et incluant des personnes mineures, l'information peut être effectuée auprès d'un seul des titulaires de l'exercice de l'autorité parentale s'il est impossible d'informer l'autre titulaire ou s'il ne peut être consulté dans des délais compatibles avec les exigences méthodologiques propres à la réalisation de la recherche, de l'étude ou de l'évaluation au regard de ses finalités. Le présent alinéa ne fait pas obstacle à l'exercice ultérieur, par chaque titulaire de l'exercice de l'autorité parentale, des droits mentionnés au premier alinéa.

Pour ces traitements, le mineur âgé de quinze ans ou plus peut s'opposer à ce que les titulaires de l'exercice de l'autorité parentale aient accès aux données le concernant recueillies au cours de la recherche, de l'étude ou de l'évaluation. Le mineur reçoit alors l'information et exerce seul ses droits.

Pour ces mêmes traitements, le mineur âgé de quinze ans ou plus peut s'opposer à ce que les titulaires de l'exercice de l'autorité parentale soient informés du traitement de données si le fait d'y participer conduit à révéler une information sur une action de prévention, un dépistage, un diagnostic, un traitement ou une intervention pour laquelle le mineur s'est expressément opposé à la consultation des titulaires de l'autorité parentale, en application des articles L. 1111-5 et L. 1111-5-1 du code de la santé publique, ou si les liens de famille sont rompus et que le mineur bénéficie à titre personnel du remboursement des prestations en nature de l'assurance maladie et maternité et de la couverture complémentaire mise en place par la loi n° 99-641 du 27 juillet 1999 portant création d'une couverture maladie universelle. Il exerce alors seul ses droits.

#### **Article 71**

Une information relative aux dispositions de la présente sous-section doit être assurée notamment dans tout établissement ou centre où s'exercent des activités de prévention, de diagnostic et de soins donnant lieu à la transmission de données à caractère personnel en vue d'un traitement mentionné au présent titre.

#### **Sous-section 2 : Dispositions particulières relatives aux traitements à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé**

#### **Article 72**

Les traitements automatisés de données à caractère personnel dont la finalité est ou devient la recherche ou les études dans le domaine de la santé ainsi que l'évaluation ou l'analyse des pratiques ou des activités de soins ou de prévention sont soumis à la sous-section 1 de la présente section, sous réserve de la présente sous-section.

L'Institut national des données de santé mentionné à l'article L. 1462-1 du code de la santé publique peut se saisir ou être saisi, dans des conditions définies par décret en Conseil d'Etat, par la Commission nationale de l'informatique et des libertés ou le ministre chargé de la santé sur le caractère d'intérêt public que présentent les traitements mentionnés au premier alinéa du présent article.

#### **Article 73**

Au titre des référentiels mentionnés au II de l'article 66 de la présente loi, des méthodologies de référence sont homologuées et publiées par la Commission nationale de l'informatique et des libertés. Elles sont établies en concertation avec l'Institut national des données de santé mentionné à l'article L. 1462-1 du code de la santé publique et des organismes publics et privés représentatifs des acteurs concernés.

Lorsque le traitement est conforme à une méthodologie de référence, il peut être mis en œuvre, sans autorisation mentionnée à l'article 66 de la présente loi, à la condition que son responsable adresse préalablement à la Commission

nationale de l'informatique et des libertés une déclaration attestant de cette conformité.

#### **Article 74**

Toute personne a le droit de s'opposer à ce que des données à caractère personnel la concernant fassent l'objet de la levée du secret professionnel rendue nécessaire par un traitement de la nature de ceux mentionnés à l'article 65.

#### **Article 75**

Dans le cas où la recherche nécessite l'examen des caractéristiques génétiques, le consentement éclairé et exprès des personnes concernées doit être obtenu préalablement à la mise en œuvre du traitement de données. Le présent article n'est pas applicable aux recherches réalisées en application de l'article L. 1131-1-1 du code de la santé publique.

#### **Article 76**

L'autorisation du traitement est accordée par la Commission nationale de l'informatique et des libertés dans les conditions définies à l'article 66, après avis :

1° Du comité compétent de protection des personnes mentionné à l'article L. 1123-6 du code de la santé publique, pour les demandes d'autorisation relatives aux recherches impliquant la personne humaine mentionnées à l'article L. 1121-1 du même code ;

2° Du comité d'expertise pour les recherches, les études et les évaluations dans le domaine de la santé, pour les demandes d'autorisation relatives à des études ou à des évaluations ainsi qu'à des recherches n'impliquant pas la personne humaine, au sens du 1° du présent article. Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, fixe la composition de ce comité et définit ses règles de fonctionnement. Les membres du comité d'expertise sont soumis à l'article L. 1451-1 du code de la santé publique.

Les dossiers présentés dans le cadre de la présente section, à l'exclusion des recherches impliquant la personne humaine, sont déposés auprès d'un secrétariat unique assuré par l'Institut national des données de santé, qui assure leur orientation vers les instances compétentes.

#### **Article 77**

Dans le respect des missions et des pouvoirs de la Commission nationale de l'informatique et des libertés et aux fins de renforcer la bonne application des règles de sécurité et de protection des données, un comité d'audit du système national des données de santé est institué. Ce comité d'audit définit une stratégie d'audit puis une programmation, dont il informe la commission. Il fait

réaliser des audits sur l'ensemble des systèmes réunissant, organisant ou mettant à disposition tout ou partie des données du système national des données de santé à des fins de recherche, d'étude ou d'évaluation ainsi que sur les systèmes composant le système national des données de santé.

Le comité d'audit comprend des représentants des services des ministères chargés de la santé, de la sécurité sociale et de la solidarité, de la Caisse nationale d'assurance maladie responsable du traitement du système national des données de santé, des autres producteurs de données du système national des données de santé, de l'Institut national des données de santé, ainsi qu'une personne représentant les acteurs privés du domaine de la santé. Des personnalités qualifiées peuvent y être désignées. Le président de la Commission nationale de l'informatique et des libertés, ou son représentant, y assiste en tant qu'observateur.

Les audits, dont le contenu est défini par le comité d'audit, sont réalisés par des prestataires sélectionnés selon des critères et modalités permettant de disposer de garanties attestant de leur compétence en matière d'audit de systèmes d'information et de leur indépendance à l'égard de l'entité auditée.

Le prestataire retenu soumet au président du comité d'audit la liste des personnes en charge de chaque audit et les informations permettant de garantir leurs compétences et leur indépendance.

Les missions d'audit s'exercent sur pièces et sur place. La procédure suivie inclut une phase contradictoire. La communication des données médicales individuelles ne peut se faire que sous l'autorité et en présence d'un médecin, s'agissant des informations qui figurent dans un traitement nécessaire aux fins de la médecine préventive, de la recherche médicale, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de service de santé.

Pour chaque mission diligentée, des échanges ont lieu, si nécessaire, entre les personnes en charge des audits, le président du comité d'audit, le responsable du traitement mentionné au II de l'article L. 1461-1 du code de la santé publique et le président de la Commission nationale de l'informatique et des libertés.

Si le comité d'audit a connaissance d'informations de nature à révéler des manquements graves en amont ou au cours d'un audit ou en cas d'opposition ou d'obstruction à l'audit, un signalement est adressé sans délai par le président du comité d'audit au président de la Commission nationale de l'informatique et des libertés.

Chaque mission diligentée établit un rapport relevant notamment les anomalies constatées et les manquements aux règles applicables aux systèmes d'information audités.

Si la mission constate, à l'issue de l'audit, de graves manquements, elle en informe sans délai le président du comité d'audit, qui informe sans délai le président de la Commission nationale de l'informatique et des libertés et le responsable du traitement mentionné au II de l'article L. 1461-1 du code de la

santé publique.

En cas d'urgence, le directeur général de la Caisse nationale d'assurance maladie peut suspendre temporairement l'accès au système national des données de santé avant le terme de l'audit s'il dispose d'éléments suffisamment préoccupants concernant des manquements graves aux règles précitées. Il doit en informer immédiatement le président du comité et le président de la commission. Le rétablissement de l'accès ne peut se faire qu'avec l'accord de ce dernier au regard des mesures correctives prises par l'entité auditée. Ces dispositions sont sans préjudice des prérogatives propres de la Commission nationale de l'informatique et des libertés.

Le rapport définitif de chaque mission est transmis au comité d'audit, au président de la Commission nationale de l'informatique et des libertés et au responsable du traitement audité.

Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, précise la composition du comité et définit ses règles de fonctionnement ainsi que les modalités de l'audit.

#### **Section 4 : Traitements à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques**

##### **Article 78**

Lorsque les traitements de données à caractère personnel sont mis en œuvre par les services publics d'archives à des fins archivistiques dans l'intérêt public conformément à l'article L. 211-2 du code du patrimoine, les droits prévus aux articles 15,16 et 18 à 21 du règlement (UE) 2016/679 du 27 avril 2016 ne s'appliquent pas dans la mesure où ces droits rendent impossible ou entravent sérieusement la réalisation de ces finalités. Les conditions et garanties appropriées prévues à l'article 89 du même règlement sont déterminées par le code du patrimoine et les autres dispositions législatives et réglementaires applicables aux archives publiques. Elles sont également assurées par le respect des normes conformes à l'état de l'art en matière d'archivage électronique.

Un décret en Conseil d'Etat, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés, détermine dans quelles conditions et sous réserve de quelles garanties il peut être dérogé en tout ou partie aux droits prévus aux articles 15,16,18 et 21 du même règlement, en ce qui concerne les traitements à des fins de recherche scientifique ou historique, ou et à des fins statistiques.

##### **Article 79**

Dans les conditions du b du 5 de l'article 14 du règlement (UE) 2016/679 du 27 avril 2016, lorsque les données à caractère personnel ont été initialement recueillies pour un autre objet, les dispositions du 1 à 4 du même article 14 ne s'appliquent pas aux traitements à des fins archivistiques dans l'intérêt public, à

des fins de recherche scientifique ou historique ou à des fins statistiques, ou à la réutilisation de ces données à des fins statistiques dans les conditions de l'article 7 bis de la loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques.

## **Section 5 : Traitements de données à caractère personnel aux fins de journalisme et d'expression littéraire et artistique**

### **Article 80**

A titre dérogatoire, les dispositions du 5° de l'article 4, celles des articles 6,46,48,49,50,53,118,119 et celles du chapitre V du règlement (UE) 2016/679 du 27 avril 2016 ne s'appliquent pas, lorsqu'une telle dérogation est nécessaire pour concilier le droit à la protection des données à caractère personnel et la liberté d'expression et d'information, aux traitements mis en œuvre aux fins :

1° D'expression universitaire, artistique ou littéraire ;

2° D'exercice à titre professionnel, de l'activité de journaliste, dans le respect des règles déontologiques de cette profession.

Les dispositions des alinéas précédents ne font pas obstacle à l'application des dispositions du code civil, des lois relatives à la presse écrite ou audiovisuelle et du code pénal, qui prévoient les conditions d'exercice du droit de réponse et qui préviennent, limitent, réparent et, le cas échéant, répriment les atteintes à la vie privée et à la réputation des personnes.

## **Chapitre IV : Droits et obligations propres aux traitements dans le secteur des communications électroniques**

### **Article 81**

Les droits et obligations mentionnés aux chapitres II et III s'appliquent sous réserve des dispositions particulières du présent chapitre.

### **Article 82**

Tout abonné ou utilisateur d'un service de communications électroniques doit être informé de manière claire et complète, sauf s'il l'a été au préalable, par le responsable du traitement ou son représentant :

1° De la finalité de toute action tendant à accéder, par voie de transmission électronique, à des informations déjà stockées dans son équipement terminal de communications électroniques, ou à inscrire des informations dans cet équipement ;

2° Des moyens dont il dispose pour s'y opposer.

Ces accès ou inscriptions ne peuvent avoir lieu qu'à condition que l'abonné ou la personne utilisatrice ait exprimé, après avoir reçu cette information, son

consentement qui peut résulter de paramètres appropriés de son dispositif de connexion ou de tout autre dispositif placé sous son contrôle.

Ces dispositions ne sont pas applicables si l'accès aux informations stockées dans l'équipement terminal de l'utilisateur ou l'inscription d'informations dans l'équipement terminal de l'utilisateur :

1° Soit, a pour finalité exclusive de permettre ou faciliter la communication par voie électronique ;

2° Soit, est strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur.

#### **Article 83**

**I.** - Le présent article s'applique au traitement des données à caractère personnel mis en œuvre dans le cadre de la fourniture au public de services de communications électroniques sur les réseaux de communications électroniques ouverts au public, y compris ceux prenant en charge les dispositifs de collecte de données et d'identification.

Pour l'application du présent article, on entend par violation de données à caractère personnel toute violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à des données à caractère personnel faisant l'objet d'un traitement dans le cadre de la fourniture au public de services de communications électroniques.

**II.** - En cas de violation de données à caractère personnel, le fournisseur de services de communications électroniques accessibles au public avertit, sans délai, la Commission nationale de l'informatique et des libertés.

Lorsque cette violation peut porter atteinte aux données à caractère personnel ou à la vie privée d'un abonné ou d'une autre personne physique, le fournisseur avertit également, sans délai, l'intéressé.

La notification d'une violation des données à caractère personnel à l'intéressé n'est toutefois pas nécessaire si la Commission nationale de l'informatique et des libertés a constaté que des mesures de protection appropriées ont été mises en œuvre par le fournisseur afin de rendre les données incompréhensibles à toute personne non autorisée à y avoir accès et ont été appliquées aux données concernées par ladite violation.

A défaut, la Commission nationale de l'informatique et des libertés peut, après avoir examiné la gravité de la violation, mettre en demeure le fournisseur d'informer également les intéressés.

**III.** - Chaque fournisseur de services de communications électroniques tient à jour un inventaire des violations de données à caractère personnel, notamment de leurs modalités, de leur effet et des mesures prises pour y remédier et le conserve à la disposition de la commission.

## **Chapitre V : Dispositions régissant les traitements de données à caractère personnel relatives aux personnes décédées**

### **Article 84**

Les traitements de données à caractère personnel relatives aux personnes décédées sont régis par les dispositions du présent chapitre.

Les droits mentionnés au chapitre II s'éteignent au décès de la personne concernée. Toutefois, ils peuvent être provisoirement maintenus dans les conditions fixées à l'article 85.

### **Article 85**

**I.** - Toute personne peut définir des directives relatives à la conservation, à l'effacement et à la communication de ses données à caractère personnel après son décès. Ces directives sont générales ou particulières.

Les directives générales concernent l'ensemble des données à caractère personnel se rapportant à la personne concernée et peuvent être enregistrées auprès d'un tiers de confiance numérique certifié par la Commission nationale de l'informatique et des libertés.

Les références des directives générales et le tiers de confiance auprès duquel elles sont enregistrées sont inscrites dans un registre unique dont les modalités et l'accès sont fixés par décret en Conseil d'Etat, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés.

Les directives particulières concernent les traitements de données à caractère personnel mentionnées par ces directives. Elles sont enregistrées auprès des responsables de traitement concernés. Elles font l'objet du consentement spécifique de la personne concernée et ne peuvent résulter de la seule approbation par celle-ci des conditions générales d'utilisation.

Les directives générales et particulières définissent la manière dont la personne entend que soient exercés, après son décès, les droits mentionnés au chapitre II du présent titre. Le respect de ces directives est sans préjudice des dispositions applicables aux archives publiques comportant des données à caractère personnel.

Lorsque les directives prévoient la communication de données qui comportent également des données à caractère personnel relatives à des tiers, cette communication s'effectue dans le respect de la présente loi.

La personne peut modifier ou révoquer ses directives à tout moment.

Les directives mentionnées au premier alinéa du présent I peuvent désigner une personne chargée de leur exécution. Celle-ci a alors qualité, lorsque la personne est décédée, pour prendre connaissance des directives et demander leur mise

en œuvre aux responsables de traitement concernés. A défaut de désignation ou, sauf directive contraire, en cas de décès de la personne désignée, ses héritiers ont qualité pour prendre connaissance des directives au décès de leur auteur et demander leur mise en œuvre aux responsables de traitement concernés.

Toute clause contractuelle des conditions générales d'utilisation d'un traitement portant sur des données à caractère personnel limitant les prérogatives reconnues à la personne en vertu du présent article est réputée non écrite.

**II.** - En l'absence de directives ou de mention contraire dans ces directives, les héritiers de la personne concernée peuvent exercer, après son décès, les droits mentionnés au chapitre II du présent titre II dans la mesure nécessaire :

1° A l'organisation et au règlement de la succession du défunt. A ce titre, les héritiers peuvent accéder aux traitements de données à caractère personnel qui le concernent afin d'identifier et d'obtenir communication des informations utiles à la liquidation et au partage de la succession. Ils peuvent aussi recevoir communication des biens numériques ou des données s'apparentant à des souvenirs de famille, transmissibles aux héritiers ;

2° A la prise en compte, par les responsables de traitement, de son décès. A ce titre, les héritiers peuvent faire procéder à la clôture des comptes utilisateurs du défunt, s'opposer à la poursuite des traitements de données à caractère personnel le concernant ou faire procéder à leur mise à jour.

Lorsque les héritiers en font la demande, le responsable du traitement doit justifier, sans frais pour le demandeur, qu'il a procédé aux opérations exigées en application du précédent alinéa.

Les désaccords entre héritiers sur l'exercice des droits prévus au présent II sont portés devant le tribunal de grande instance compétent.

**III.** - Tout prestataire d'un service de communication au public en ligne informe l'utilisateur du sort des données qui le concernent à son décès et lui permet de choisir de communiquer ou non ses données à un tiers qu'il désigne.

#### **Article 86**

Les informations concernant les personnes décédées, y compris celles qui figurent sur les certificats des causes de décès, peuvent faire l'objet d'un traitement à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé, sauf si l'intéressé a, de son vivant, exprimé son refus par écrit.

## **Titre III : Dispositions applicables aux traitements relevant de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des**

# **personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil**

## **Chapitre Ier : Dispositions générales**

### **Article 87**

Le présent titre s'applique, sans préjudice du titre Ier, aux traitements de données à caractère personnel mis en œuvre, à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, par toute autorité publique compétente ou tout autre organisme ou entité à qui a été confié, à ces mêmes fins, l'exercice de l'autorité publique et des prérogatives de puissance publique, ci-après dénommés autorité compétente.

Ces traitements ne sont licites que si et dans la mesure où ils sont nécessaires à l'exécution d'une mission effectuée, pour l'une des finalités énoncées au premier alinéa, par une autorité compétente au sens du même premier alinéa et où sont respectées les dispositions des articles 89 et 90. Le traitement assure notamment la proportionnalité de la durée de conservation des données à caractère personnel, compte tenu de l'objet du fichier et de la nature ou de la gravité des infractions concernées.

### **Article 88**

Le traitement de données mentionnées au I de l'article 6 est possible uniquement en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et soit s'il est autorisé par une disposition législative ou réglementaire, soit s'il vise à protéger les intérêts vitaux d'une personne physique, soit s'il porte sur des données manifestement rendues publiques par la personne concernée.

### **Article 89**

**I.** - Si le traitement est mis en œuvre pour le compte de l'Etat pour au moins l'une des finalités énoncées au premier alinéa de l'article 87, il est prévu par une disposition législative ou réglementaire prise dans les conditions prévues au I de l'article 31 et aux articles 33 à 36.

**II.** - Si le traitement porte sur des données mentionnées au I de l'article 6, il est prévu par une disposition législative ou réglementaire prise dans les conditions prévues au II de l'article 31.

#### **Article 90**

Si le traitement est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques, notamment parce qu'il porte sur des données mentionnées au I de l'article 6, le responsable de traitement effectue une analyse d'impact relative à la protection des données à caractère personnel.

Si le traitement est mis en œuvre pour le compte de l'Etat, cette analyse d'impact est adressée à la Commission nationale de l'informatique et des libertés avec la demande d'avis prévue à l'article 33.

Dans les autres cas, le responsable de traitement ou son sous-traitant consulte la Commission nationale de l'informatique et des libertés préalablement à la mise en œuvre du traitement de données à caractère personnel, qui se prononce également dans les délais prévus à l'article 34 :

1° Soit lorsque l'analyse d'impact relative à la protection des données indique que le traitement présenterait un risque élevé si le responsable de traitement ne prenait pas de mesures pour atténuer le risque ;

2° Soit lorsque le type de traitement, en particulier en raison de l'utilisation de nouveaux mécanismes, technologies ou procédures, présente des risques élevés pour les libertés et les droits des personnes concernées.

#### **Article 91**

Les données à caractère personnel collectées par les autorités compétentes pour les finalités énoncées au premier alinéa de l'article 87 ne peuvent être traitées pour d'autres finalités, à moins qu'un tel traitement ne soit autorisé par des dispositions législatives ou réglementaires ou par le droit de l'Union européenne. Lorsque des données à caractère personnel sont traitées à de telles autres fins, le règlement (UE) 2016/679 du 27 avril 2016 s'applique, à moins que le traitement ne soit effectué dans le cadre d'une activité ne relevant pas du champ d'application du droit de l'Union européenne.

Lorsque les autorités compétentes sont chargées d'exécuter des missions autres que celles exécutées pour les finalités énoncées au premier alinéa de l'article 87, le règlement (UE) 2016/679 du 27 avril 2016 s'applique au traitement effectué à de telles fins, y compris à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, à moins que le traitement ne soit effectué dans le cadre d'une activité ne relevant pas du champ d'application du droit de l'Union européenne.

Si le traitement est soumis à des conditions spécifiques, l'autorité compétente qui transmet les données informe le destinataire de ces données à caractère personnel de ces conditions et de l'obligation de les respecter.

L'autorité compétente qui transmet les données n'applique pas, en vertu du troisième alinéa du présent article, aux destinataires établis dans les autres Etats membres de l'Union européenne ou aux services, organes et organismes établis en vertu des chapitres 4 et 5 du titre V du traité sur le fonctionnement de l'Union européenne des conditions différentes de celles applicables aux transferts de données similaires à l'intérieur de l'Etat membre dont relève l'autorité compétente qui transmet les données.

#### **Article 92**

Les traitements effectués pour l'une des finalités énoncées au premier alinéa de l'article 87 autre que celles pour lesquelles les données ont été collectées sont autorisés s'ils sont nécessaires et proportionnés à cette finalité, sous réserve du respect des dispositions prévues au chapitre Ier du titre Ier et au présent titre.

Ces traitements peuvent comprendre l'archivage dans l'intérêt public, à des fins scientifiques, statistiques ou historiques, pour l'une des finalités énoncées au premier alinéa de l'article 87.

#### **Article 93**

Les traitements à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques sont mis en œuvre dans les conditions prévues aux 2° et 5° de l'article 4 ainsi que, pour les traitements mentionnés à l'article 91, à la section 4 du chapitre III du titre II.

#### **Article 94**

Les données à caractère personnel fondées sur des faits sont, dans la mesure du possible, distinguées de celles fondées sur des appréciations personnelles.

#### **Article 95**

Aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour fondement un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de la personnalité de cette personne.

Aucune autre décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à prévoir ou à évaluer certains aspects personnels relatifs à la personne concernée.

Tout profilage qui entraîne une discrimination à l'égard des personnes physiques sur la base des catégories particulières de données à caractère personnel mentionnées au I de l'article 6 est interdit.

#### **Article 96**

Les données à caractère personnel ne peuvent faire l'objet d'une opération de traitement de la part d'un sous-traitant que dans les conditions prévues aux 1,2 et 10 de l'article 28 et à l'article 29 du règlement (UE) 2016/679 du 27 avril 2016 et au présent article.

Les sous-traitants doivent présenter des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées, de manière que le traitement réponde aux exigences du présent titre et garantisse la protection des droits de la personne concernée.

Le traitement par un sous-traitant est régi par un contrat ou un autre acte juridique, qui lie le sous-traitant à l'égard du responsable de traitement, définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, les obligations et les droits du responsable de traitement ainsi que les mesures techniques et organisationnelles destinées à garantir la sécurité du traitement, et prévoit que le sous-traitant n'agit que sur instruction du responsable de traitement. Le contenu de ce contrat ou de cet acte juridique est précisé par décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés.

## **Chapitre II : Obligations incombant aux autorités compétentes, aux responsables de traitement de données à caractère personnel et aux sous-traitants**

### **Article 97**

Les autorités compétentes prennent toutes les mesures raisonnables pour garantir que les données à caractère personnel qui sont inexactes, incomplètes ou ne sont plus à jour soient effacées ou rectifiées sans tarder ou ne soient pas transmises ou mises à disposition. A cette fin, chaque autorité compétente vérifie, dans la mesure du possible, la qualité des données à caractère personnel avant leur transmission ou mise à disposition.

Dans la mesure du possible, lors de toute transmission de données à caractère personnel, sont ajoutées des informations permettant à l'autorité compétente destinataire de juger de l'exactitude, de l'exhaustivité et de la fiabilité des données à caractère personnel et de leur niveau de mise à jour.

S'il s'avère que des données à caractère personnel inexactes ont été transmises ou que des données à caractère personnel ont été transmises de manière illicite, le destinataire en est informé sans retard. Dans ce cas, les données à caractère personnel sont rectifiées ou effacées ou leur traitement est limité conformément à l'article 106.

### **Article 98**

Le responsable de traitement établit, dans la mesure du possible et le cas échéant, une distinction claire entre les données à caractère personnel de différentes catégories de personnes concernées, telles que :

1° Les personnes à l'égard desquelles il existe des motifs sérieux de croire qu'elles ont commis ou sont sur le point de commettre une infraction pénale ;

2° Les personnes reconnues coupables d'une infraction pénale ;

3° Les victimes d'une infraction pénale ou les personnes à l'égard desquelles certains faits portent à croire qu'elles pourraient être victimes d'une infraction pénale ;

4° Les tiers à une infraction pénale, tels que les personnes pouvant être appelées à témoigner lors d'enquêtes en rapport avec des infractions pénales ou des procédures pénales ultérieures, des personnes pouvant fournir des informations sur des infractions pénales ou des contacts ou des associés de l'une des personnes mentionnées aux 1° et 2°.

#### **Article 99**

**I.** - Afin de démontrer que le traitement est effectué conformément au présent titre, le responsable de traitement et son sous-traitant mettent en œuvre les mesures prévues aux 1 et 2 des articles 24 et 25 du règlement (UE) 2016/679 du 27 avril 2016 et celles appropriées afin de garantir un niveau de sécurité adapté au risque, notamment en ce qui concerne le traitement portant sur des catégories particulières de données à caractère personnel mentionnées au I de l'article 6 de la présente loi.

**II.** - En ce qui concerne le traitement automatisé, le responsable de traitement ou son sous-traitant met en œuvre, à la suite d'une évaluation des risques, des mesures destinées à :

1° Empêcher toute personne non autorisée d'accéder aux installations utilisées pour le traitement ;

2° Empêcher que des supports de données puissent être lus, copiés, modifiés ou supprimés de façon non autorisée ;

3° Empêcher l'introduction non autorisée de données à caractère personnel dans le fichier, ainsi que l'inspection, la modification ou l'effacement non autorisé de données à caractère personnel enregistrées ;

4° Empêcher que les systèmes de traitement automatisé puissent être utilisés par des personnes qui n'y sont pas autorisées à l'aide d'installations de transmission de données ;

5° Garantir que les personnes autorisées à utiliser un système de traitement automatisé ne puissent accéder qu'aux données à caractère personnel sur lesquelles porte leur autorisation ;

6° Garantir qu'il puisse être vérifié et constaté à quelles instances des données à caractère personnel ont été ou peuvent être transmises ou mises à disposition par des installations de transmission de données ;

7° Garantir qu'il puisse être vérifié et constaté a posteriori quelles données à

caractère personnel ont été introduites dans les systèmes de traitement automatisé et à quel moment et par quelle personne elles y ont été introduites ;

8° Empêcher que, lors de la transmission de données à caractère personnel ainsi que lors du transport de supports de données, les données puissent être lues, copiées, modifiées ou supprimées de façon non autorisée ;

9° Garantir que les systèmes installés puissent être rétablis en cas d'interruption ;

10° Garantir que les fonctions du système opèrent, que les erreurs de fonctionnement soient signalées et que les données à caractère personnel conservées ne puissent pas être corrompues par un dysfonctionnement du système.

#### **Article 100**

Le responsable de traitement et son sous-traitant tiennent un registre des activités de traitement dans les conditions prévues aux 1 à 4 de l'article 30 du règlement (UE) 2016/679 du 27 avril 2016. Ce registre contient aussi la description générale des mesures visant à garantir un niveau de sécurité adapté au risque, notamment en ce qui concerne le traitement portant sur des catégories particulières de données à caractère personnel mentionnées au I de l'article 6 de la présente loi, l'indication de la base juridique de l'opération de traitement, y compris les transferts, à laquelle les données à caractère personnel sont destinées et, le cas échéant, le recours au profilage.

#### **Article 101**

Le responsable de traitement ou son sous-traitant établit pour chaque traitement automatisé un journal des opérations de collecte, de modification, de consultation, de communication, y compris les transferts, d'interconnexion et d'effacement, portant sur de telles données.

Les journaux des opérations de consultation et de communication permettent d'en établir le motif, la date et l'heure. Ils permettent également, dans la mesure du possible, d'identifier les personnes qui consultent ou communiquent les données et les destinataires de celles-ci.

Ce journal est uniquement utilisé à des fins de vérification de la licéité du traitement, d'autocontrôle, de garantie de l'intégrité et de la sécurité des données et à des fins de procédures pénales.

Ce journal est mis à la disposition de la Commission nationale de l'informatique et des libertés à sa demande.

#### **Article 102**

Les articles 31,33 et 34 du règlement (UE) 2016/679 du 27 avril 2016 sont applicables aux traitements de données à caractère personnel relevant du

présent titre.

Si la violation de données à caractère personnel porte sur des données à caractère personnel qui ont été transmises par le responsable de traitement établi dans un autre Etat membre de l'Union européenne ou à celui-ci, le responsable de traitement établi en France notifie également la violation au responsable de traitement de l'autre Etat membre dans les meilleurs délais.

La communication d'une violation de données à caractère personnel à la personne concernée peut être retardée, limitée ou ne pas être délivrée dès lors et aussi longtemps qu'une mesure de cette nature constitue une mesure nécessaire et proportionnée dans une société démocratique, en tenant compte des droits fondamentaux et des intérêts légitimes de la personne, pour éviter de gêner des enquêtes, des recherches ou des procédures administratives ou judiciaires, pour éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales, pour protéger la sécurité publique, pour protéger la sécurité nationale ou pour protéger les droits et libertés d'autrui.

#### **Article 103**

Sauf pour les juridictions agissant dans l'exercice de leur fonction juridictionnelle, le responsable de traitement désigne un délégué à la protection des données.

Un seul délégué à la protection des données peut être désigné pour plusieurs autorités compétentes, en fonction de leur structure organisationnelle et de leur taille.

Les dispositions des 5 et 7 de l'article 37, des 1 et 2 de l'article 38 et du 1 de l'article 39 du règlement (UE) 2016/679 du 27 avril 2016, en ce qu'elles concernent le responsable de traitement, sont applicables aux traitements de données à caractère personnel relevant du présent titre.

## **Chapitre III : Droits de la personne concernée**

#### **Article 104**

**I.** - Le responsable de traitement met à la disposition de la personne concernée les informations suivantes :

- 1° L'identité et les coordonnées du responsable de traitement et, le cas échéant, celles de son représentant ;
- 2° Le cas échéant, les coordonnées du délégué à la protection des données ;
- 3° Les finalités poursuivies par le traitement auquel les données sont destinées ;
- 4° Le droit d'introduire une réclamation auprès de la Commission nationale de l'informatique et des libertés et les coordonnées de la commission ;

5° L'existence du droit de demander au responsable de traitement l'accès aux données à caractère personnel, leur rectification ou leur effacement, et l'existence du droit de demander une limitation du traitement des données à caractère personnel relatives à une personne concernée.

**II.** - En plus des informations mentionnées au I, le responsable de traitement fournit à la personne concernée, dans des cas particuliers, les informations additionnelles suivantes afin de lui permettre d'exercer ses droits :

1° La base juridique du traitement ;

2° La durée de conservation des données à caractère personnel ou, à défaut lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;

3° Le cas échéant, les catégories de destinataires des données à caractère personnel, y compris ceux établis dans les Etats n'appartenant pas à l'Union européenne ou au sein d'organisations internationales ;

4° Au besoin, des informations complémentaires, en particulier lorsque les données à caractère personnel sont collectées à l'insu de la personne concernée.

#### **Article 105**

La personne concernée a le droit d'obtenir du responsable de traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, le droit d'accéder auxdites données ainsi qu'aux informations suivantes :

1° Les finalités du traitement ainsi que sa base juridique ;

2° Les catégories de données à caractère personnel concernées ;

3° Les destinataires ou catégories de destinataires auxquels les données à caractère personnel ont été communiquées, en particulier les destinataires qui sont établis dans des Etats n'appartenant pas à l'Union européenne ou au sein d'organisations internationales ;

4° Lorsque cela est possible, la durée de conservation des données à caractère personnel envisagée ou, à défaut lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;

5° L'existence du droit de demander au responsable de traitement la rectification ou l'effacement des données à caractère personnel, et l'existence du droit de demander une limitation du traitement de ces données ;

6° Le droit d'introduire une réclamation auprès de la Commission nationale de l'informatique et des libertés et les coordonnées de la commission ;

7° La communication des données à caractère personnel en cours de traitement ainsi que toute information disponible quant à leur source.

## Article 106

**I.** - La personne concernée a le droit d'obtenir du responsable de traitement :

1° Que soient rectifiées dans les meilleurs délais des données à caractère personnel la concernant qui sont inexactes ;

2° Que soient complétées des données à caractère personnel la concernant incomplètes, y compris en fournissant à cet effet une déclaration complémentaire ;

3° Que soient effacées dans les meilleurs délais des données à caractère personnel la concernant lorsque le traitement est réalisé en violation des dispositions de la présente loi ou lorsque ces données doivent être effacées pour respecter une obligation légale à laquelle est soumis le responsable de traitement ;

4° Que le traitement soit limité dans les cas prévus au III du présent article.

**II.** - Lorsque l'intéressé en fait la demande, le responsable de traitement doit justifier qu'il a procédé aux opérations exigées en application du I.

**III.** - Au lieu de procéder à l'effacement, le responsable de traitement limite le traitement :

1° Soit lorsque l'exactitude des données à caractère personnel est contestée par la personne concernée sans qu'il soit possible de déterminer si les données sont exactes ou non ;

2° Soit lorsque les données à caractère personnel doivent être conservées à des fins probatoires.

Lorsque le traitement est limité en application du 1° du présent III, le responsable de traitement informe la personne concernée avant de mettre fin à la limitation du traitement.

**IV.** - Le responsable de traitement informe la personne concernée de tout refus de rectifier ou d'effacer des données à caractère personnel ou de limiter le traitement de ces données, ainsi que des motifs du refus.

**V.** - Le responsable de traitement communique la rectification des données à caractère personnel inexactes à l'autorité compétente de laquelle ces données proviennent.

**VI.** - Lorsque des données à caractère personnel ont été rectifiées ou effacées ou que le traitement a été limité au titre des I et III, le responsable de traitement le notifie aux destinataires afin que ceux-ci rectifient ou effacent les données ou limitent le traitement des données sous leur responsabilité.

## Article 107

**I.** - Les droits de la personne physique concernée peuvent faire l'objet de

restrictions selon les modalités prévues au II du présent article dès lors et aussi longtemps qu'une telle restriction constitue une mesure nécessaire et proportionnée dans une société démocratique en tenant compte des droits fondamentaux et des intérêts légitimes de la personne pour :

- 1° Eviter de gêner des enquêtes, des recherches ou des procédures administratives ou judiciaires ;
- 2° Eviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales ;
- 3° Protéger la sécurité publique ;
- 4° Protéger la sécurité nationale ;
- 5° Protéger les droits et libertés d'autrui.

Ces restrictions sont prévues par l'acte instaurant le traitement.

**II.** - Lorsque les conditions prévues au I sont remplies, le responsable de traitement peut :

- 1° Retarder ou limiter la communication à la personne concernée des informations mentionnées au II de l'article 104 ou ne pas communiquer ces informations ;
- 2° Refuser ou limiter le droit d'accès de la personne concernée prévu à l'article 105 ;
- 3° Ne pas informer la personne du refus de rectifier ou d'effacer des données à caractère personnel ou de limiter le traitement de ces données, ni des motifs de cette décision, par dérogation au IV de l'article 106.

**III.** - Dans les cas mentionnés au 2° du II du présent article, le responsable de traitement informe la personne concernée, dans les meilleurs délais, de tout refus ou de toute limitation d'accès ainsi que des motifs du refus ou de la limitation. Ces informations peuvent ne pas être fournies lorsque leur communication risque de compromettre l'un des objectifs énoncés au I. Le responsable de traitement consigne les motifs de fait ou de droit sur lesquels se fonde la décision et met ces informations à la disposition de la Commission nationale de l'informatique et des libertés.

**IV.** - En cas de restriction des droits de la personne concernée intervenue en application des II ou III, le responsable de traitement informe la personne concernée de la possibilité, prévue à l'article 108, d'exercer ses droits par l'intermédiaire de la Commission nationale de l'informatique et des libertés. Hors le cas prévu au 1° du II, il l'informe également de la possibilité de former un recours juridictionnel.

#### **Article 108**

En cas de restriction des droits de la personne concernée intervenue en

application des II ou III de l'article 107, la personne concernée peut saisir la Commission nationale de l'informatique et des libertés.

La commission désigne l'un de ses membres appartenant ou ayant appartenu au Conseil d'Etat, à la Cour de cassation ou à la Cour des comptes pour mener les investigations utiles et faire procéder aux modifications nécessaires. Celui-ci peut se faire assister d'un agent de la commission. La commission informe la personne concernée qu'il a été procédé aux vérifications nécessaires et de son droit de former un recours juridictionnel.

Lorsque la commission constate, en accord avec le responsable du traitement, que la communication des données qui y sont contenues ne met pas en cause ses finalités, la sûreté de l'Etat, la défense ou la sécurité publique, ces données peuvent être communiquées au requérant.

#### **Article 109**

**I.** -Les informations mentionnées aux articles 104 à 106 sont fournies par le responsable de traitement à la personne concernée par tout moyen approprié, y compris par voie électronique et, de manière générale, sous la même forme que la demande.

**II.** -Aucun paiement n'est exigé pour prendre les mesures et fournir ces mêmes informations, sauf en cas de demande manifestement infondée ou abusive.

En cas de demande manifestement infondée ou abusive, le responsable de traitement peut également refuser de donner suite à la demande.

En cas de contestation, la charge de la preuve du caractère manifestement infondé ou abusif des demandes incombe au responsable de traitement auquel elles sont adressées.

#### **Article 110**

Toute personne physique a le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement.

Les dispositions du premier alinéa ne s'appliquent pas lorsque le traitement répond à une obligation légale ou lorsque l'application de ces dispositions a été écartée par une disposition expresse de l'acte instaurant le traitement.

#### **Article 111**

Les dispositions du présent chapitre ne s'appliquent pas lorsque les données à caractère personnel figurent soit dans une décision judiciaire, soit dans un dossier judiciaire faisant l'objet d'un traitement lors d'une procédure pénale. Dans ces cas, l'accès à ces données et les conditions de rectification ou d'effacement de ces données ne peuvent être régis que par les dispositions du code de procédure pénale.

## **Chapitre IV : Transferts de données à caractère personnel vers des États n'appartenant pas à l'Union européenne ou vers des destinataires établis dans des États n'appartenant pas à l'Union européenne**

### **Article 112**

Le responsable de traitement de données à caractère personnel ne peut transférer des données ou autoriser le transfert de données déjà transmises vers un Etat n'appartenant pas à l'Union européenne que lorsque les conditions suivantes sont respectées :

1° Le transfert de ces données est nécessaire à l'une des finalités énoncées au premier alinéa de l'article 87 ;

2° Les données à caractère personnel sont transférées à un responsable établi dans cet Etat n'appartenant pas à l'Union européenne ou au sein d'une organisation internationale qui est une autorité compétente chargée des fins relevant en France du premier alinéa de l'article 87 ;

3° Si les données à caractère personnel proviennent d'un autre Etat, l'Etat qui a transmis ces données a préalablement autorisé ce transfert conformément à son droit national.

Toutefois, si l'autorisation préalable ne peut pas être obtenue en temps utile, ces données à caractère personnel peuvent être transmises à nouveau sans l'autorisation préalable de l'Etat qui a transmis ces données lorsque cette nouvelle transmission est nécessaire à la prévention d'une menace grave et immédiate pour la sécurité publique d'un autre Etat ou pour la sauvegarde des intérêts essentiels de la France. L'autorité dont provenaient ces données personnelles en est informée sans retard ;

4° La Commission européenne a adopté une décision d'adéquation en application de l'article 36 de la directive (UE) 2016/680 du 27 avril 2016 ou, en l'absence d'une telle décision, un instrument juridiquement contraignant fournit des garanties appropriées en ce qui concerne la protection des données à caractère personnel ou, en l'absence d'une telle décision et d'un tel instrument, le responsable de traitement a évalué toutes les circonstances du transfert et estime qu'il existe de telles garanties appropriées.

Les garanties appropriées fournies par un instrument juridique contraignant mentionnées au 4° peuvent résulter soit des garanties relatives à la protection des données mentionnées dans les conventions mises en œuvre avec cet Etat n'appartenant pas à l'Union européenne, soit de dispositions juridiquement contraignantes exigées à l'occasion de l'échange de données.

Lorsque le responsable de traitement autre qu'une juridiction effectuant une activité de traitement dans le cadre de ses activités juridictionnelles transfère des données à caractère personnel sur le seul fondement de l'existence de garanties appropriées au regard de la protection des données à caractère

personnel, il avise la Commission nationale de l'informatique et des libertés des catégories de transferts relevant de ce fondement.

Dans ce cas, le responsable de traitement doit garder trace de la date et de l'heure du transfert, des informations sur l'autorité compétente destinataire, de la justification du transfert et des données à caractère personnel transférées. Ces informations sont mises à la disposition de la Commission nationale de l'informatique et des libertés à sa demande.

Lorsque la Commission européenne a abrogé, modifié ou suspendu une décision d'adéquation adoptée en application de l'article 36 de la directive (UE) 2016/680 du 27 avril 2016, le responsable de traitement peut néanmoins transférer des données à caractère personnel ou autoriser le transfert de données déjà transmises vers un Etat n'appartenant pas à l'Union européenne si des garanties appropriées en ce qui concerne la protection des données à caractère personnel sont fournies dans un instrument juridiquement contraignant ou si ce responsable estime, après avoir évalué toutes les circonstances du transfert, qu'il existe des garanties appropriées au regard de la protection des données à caractère personnel.

#### **Article 113**

Par dérogation à l'article 112, le responsable de traitement de données à caractère personnel ne peut, en l'absence de décision d'adéquation ou de garanties appropriées, transférer ces données ou autoriser le transfert de données déjà transmises vers un Etat n'appartenant pas à l'Union européenne que lorsque le transfert est nécessaire :

1° A la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne ;

2° A la sauvegarde des intérêts légitimes de la personne concernée lorsque le droit français le prévoit ;

3° Pour prévenir une menace grave et immédiate pour la sécurité publique d'un autre Etat ;

4° Dans des cas particuliers, à l'une des finalités énoncées au premier alinéa de l'article 87 ;

5° Dans un cas particulier, à la constatation, à l'exercice ou à la défense de droits en justice en rapport avec les mêmes fins.

Dans les cas mentionnés aux 4° et 5° du présent article, le responsable de traitement de données à caractère personnel ne transfère pas ces données s'il estime que les libertés et droits fondamentaux de la personne concernée l'emportent sur l'intérêt public dans le cadre du transfert envisagé.

Lorsqu'un transfert est effectué aux fins de la sauvegarde des intérêts légitimes de la personne concernée, le responsable de traitement garde trace de la date et de l'heure du transfert, des informations sur l'autorité compétente

destinataire, de la justification du transfert et des données à caractère personnel transférées. Il met ces informations à la disposition de la Commission nationale de l'informatique et des libertés à sa demande.

#### **Article 114**

Toute autorité publique compétente mentionnée au premier alinéa de l'article 87 peut, dans certains cas particuliers, transférer des données à caractère personnel directement à des destinataires établis dans un Etat n'appartenant pas à l'Union européenne lorsque les autres dispositions de la présente loi applicables aux traitements relevant du même article 87 sont respectées et que les conditions ci-après sont remplies :

1° Le transfert est nécessaire à l'exécution de la mission de l'autorité compétente qui transfère ces données pour l'une des finalités énoncées au premier alinéa dudit article 87 ;

2° L'autorité compétente qui transfère ces données établit qu'il n'existe pas de libertés ni de droits fondamentaux de la personne concernée qui prévalent sur l'intérêt public rendant nécessaire le transfert dans le cas considéré ;

3° L'autorité compétente qui transfère ces données estime que le transfert à l'autorité compétente de l'autre Etat est inefficace ou inapproprié, notamment parce que le transfert ne peut pas être effectué en temps opportun ;

4° L'autorité compétente de l'autre Etat est informée dans les meilleurs délais, à moins que cela ne soit inefficace ou inapproprié ;

5° L'autorité compétente qui transfère ces données informe le destinataire de la finalité ou des finalités pour lesquelles les données à caractère personnel transmises doivent exclusivement faire l'objet d'un traitement par ce destinataire, à condition qu'un tel traitement soit nécessaire.

L'autorité compétente qui transfère des données informe la Commission nationale de l'informatique et des libertés des transferts répondant aux conditions prévues au présent article.

L'autorité compétente garde trace de la date et de l'heure de ce transfert, des informations sur le destinataire, de la justification du transfert et des données à caractère personnel transférées.

### **Titre IV : Dispositions applicables aux traitements intéressant la sûreté de l'Etat et la défense**

#### **Article 115**

Le présent titre s'applique, sans préjudice du titre Ier, aux traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat et qui intéressent la sûreté de l'Etat ou la défense.

### **Chapitre Ier : Droits de la personne concernée**

## Article 116

**I.** - La personne auprès de laquelle sont recueillies des données à caractère personnel la concernant est informée, sauf si elle l'a été au préalable, par le responsable de traitement ou son représentant :

1° De l'identité du responsable du traitement et, le cas échéant, de celle de son représentant ;

2° De la finalité poursuivie par le traitement auquel les données sont destinées ;

3° Du caractère obligatoire ou facultatif des réponses ;

4° Des conséquences éventuelles, à son égard, d'un défaut de réponse ;

5° Des destinataires ou catégories de destinataires des données ;

6° Des droits qu'elle tient des dispositions des articles 117 à 120 ;

7° Le cas échéant, des transferts de données à caractère personnel envisagés à destination d'un Etat non membre de l'Union européenne ;

8° De la durée de conservation des catégories de données traitées ou, en cas d'impossibilité, des critères utilisés permettant de déterminer cette durée.

Lorsque de telles données sont recueillies par voie de questionnaires, ceux-ci doivent porter mention des prescriptions figurant aux 1°, 2°, 3° et 6°.

**II.** - Lorsque les données à caractère personnel n'ont pas été recueillies auprès de la personne concernée, le responsable de traitement ou son représentant doit fournir à cette dernière les informations énumérées au I dès l'enregistrement des données ou, si une communication des données à des tiers est envisagée, au plus tard lors de la première communication des données.

Lorsque les données à caractère personnel ont été initialement recueillies pour un autre objet, les dispositions de l'alinéa précédent ne s'appliquent pas lorsque la personne concernée est déjà informée ou quand son information se révèle impossible ou exige des efforts disproportionnés par rapport à l'intérêt de la démarche.

**III.** - Les dispositions du I ne s'appliquent pas aux données recueillies dans les conditions prévues au II dans la mesure où une telle limitation est nécessaire au respect des fins poursuivies par le traitement.

## Article 117

Toute personne physique a le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement.

Les dispositions du premier alinéa ne s'appliquent pas lorsque le traitement répond à une obligation légale ou lorsque l'application de ces dispositions a été

écartée par une disposition expresse de l'acte autorisant le traitement.

#### **Article 118**

**I.** - Les demandes tendant à l'exercice du droit d'accès, de rectification et d'effacement sont adressées à la Commission nationale de l'informatique et des libertés qui désigne l'un de ses membres appartenant ou ayant appartenu au Conseil d'Etat, à la Cour de cassation ou à la Cour des comptes pour mener les investigations utiles et faire procéder aux modifications nécessaires. Celui-ci peut se faire assister d'un agent de la commission. La commission informe la personne concernée qu'il a été procédé aux vérifications nécessaires et de son droit de former un recours juridictionnel.

Lorsque la commission constate, en accord avec le responsable du traitement, que la communication des données qui y sont contenues ne met pas en cause ses finalités, la sûreté de l'Etat, la défense ou la sécurité publique, ces données peuvent être communiquées au requérant.

#### **Article 119**

**I.** - Par dérogation à l'article 118, lorsque le traitement est susceptible de comprendre des informations dont la communication ne mettrait pas en cause les fins qui lui sont assignées, l'acte réglementaire autorisant le traitement peut prévoir que les droits d'accès, de rectification et d'effacement peuvent être exercés par la personne concernée auprès du responsable de traitement directement saisi dans les conditions prévues aux II à III du présent article.

**II.** - La personne concernée justifiant de son identité a le droit d'obtenir :

1° La confirmation que des données à caractère personnel la concernant font ou ne font pas l'objet de ce traitement ;

2° Des informations relatives aux finalités du traitement, aux catégories de données à caractère personnel traitées et aux destinataires ou aux catégories de destinataires auxquels les données sont communiquées ;

3° Le cas échéant, des informations relatives aux transferts de données à caractère personnel envisagés à destination d'un Etat non membre de l'Union européenne ;

4° La communication, sous une forme accessible, des données à caractère personnel qui la concernent ainsi que de toute information disponible quant à l'origine de celles-ci ;

5° Les informations permettant de connaître et de contester la logique qui sous-tend le traitement automatisé en cas de décision prise sur le fondement de celui-ci et produisant des effets juridiques à l'égard de l'intéressé.

Les demandes manifestement abusives, notamment par leur nombre, leur caractère répétitif ou systématique peuvent être rejetées.

**III.** - La personne concernée justifiant de son identité peut également exiger du responsable d'un traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite.

Lorsque l'intéressé en fait la demande, le responsable de traitement doit justifier, sans frais pour le demandeur, qu'il a procédé aux opérations exigées.

En cas de contestation, la charge de la preuve incombe au responsable de traitement auprès duquel est exercé le droit d'accès sauf lorsqu'il est établi que les données contestées ont été communiquées par l'intéressé ou avec son accord.

Si une donnée a été transmise à un tiers, le responsable du traitement doit accomplir les diligences utiles afin de lui notifier les opérations qu'il a effectuées conformément au premier alinéa du III.

#### **Article 120**

Aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour fondement un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de la personnalité de cette personne.

Aucune autre décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative ne peut être prise sur le seul fondement d'un traitement automatisé de données à caractère personnel destiné à prévoir ou évaluer certains aspects personnels relatifs à la personne concernée.

## **Chapitre II : Autres dispositions**

### **Section 1 : Obligations incombant au responsable de traitement**

#### **Article 121**

Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

### **Section 2 : Obligations incombant au sous-traitant**

#### **Article 122**

Les données à caractère personnel ne peuvent faire l'objet d'une opération de traitement de la part d'un sous-traitant, d'une personne agissant sous l'autorité du responsable du traitement ou de celle du sous-traitant, que sur instruction du responsable du traitement.

Le sous-traitant doit présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité mentionnées au 6° de l'article 4 et à l'article 121. Cette exigence ne décharge pas le responsable du traitement de son obligation de veiller au respect de ces mesures.

Le contrat liant le sous-traitant au responsable du traitement comporte l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et prévoit que le sous-traitant ne peut agir que sur instruction du responsable du traitement.

### **Section 3 : Transferts de données à caractère personnel vers des Etats n'appartenant pas à l'Union européenne ou vers des destinataires établis dans des Etats n'appartenant pas à l'Union européenne**

#### **Article 123**

Le responsable d'un traitement ne peut transférer des données à caractère personnel vers un Etat n'appartenant pas à l'Union européenne que si cet Etat assure un niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font l'objet ou peuvent faire l'objet.

Le caractère suffisant du niveau de protection assuré par un Etat s'apprécie en fonction notamment des dispositions en vigueur dans cet Etat, des mesures de sécurité qui y sont appliquées, des caractéristiques propres du traitement, telles que ses fins et sa durée, ainsi que de la nature, de l'origine et de la destination des données traitées.

#### **Article 124**

Toutefois, le responsable de traitement peut transférer des données à caractère personnel vers un Etat ne répondant pas aux conditions de l'article 123 si la personne à laquelle se rapportent les données a consenti expressément à leur transfert ou si le transfert est nécessaire à l'une des conditions suivantes :

1° A la sauvegarde de la vie de cette personne ;

2° A la sauvegarde de l'intérêt public ;

3° Au respect d'obligations permettant d'assurer la constatation, l'exercice ou la défense d'un droit en justice ;

4° A la consultation, dans des conditions régulières, d'un registre public qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation de celui-ci ou de toute personne justifiant d'un intérêt légitime ;

5° A l'exécution d'un contrat entre le responsable du traitement et l'intéressé, ou de mesures précontractuelles prises à la demande de celui-ci ;

6° A la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans

l'intérêt de la personne concernée, entre le responsable du traitement et un tiers.

Il peut également être fait exception à l'interdiction prévue à l'article 123 si un tel transfert est autorisé par décret, pris après avis motivé de la Commission nationale de l'informatique et des libertés, lorsque le traitement garantit un niveau de protection suffisant de la vie privée ainsi que des libertés et droits fondamentaux des personnes, notamment en raison des clauses contractuelles ou règles internes dont il fait l'objet. Lorsque les données transférées sont issues d'un traitement créé par un acte réglementaire dispensé de publication en application du III de l'article 31, le décret autorisant le transfert est lui-même dispensé de publication.

La commission se prononce dans un délai de deux mois à compter de la réception de la demande d'avis. Toutefois ce délai peut être renouvelé une fois sur décision motivée de son président. Lorsque la commission ne s'est pas prononcée dans ces délais, l'avis demandé à la commission sur le transfert est réputé favorable.

## **Titre V : Dispositions relatives à l'outre-mer**

### **Article 125**

La présente loi est applicable en Nouvelle-Calédonie, en Polynésie française, dans les îles Wallis et Futuna et dans les Terres australes et antarctiques françaises, dans sa rédaction résultant de l'ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel.

### **Article 126**

Pour l'application de la présente loi à Saint-Barthélemy, à Saint-Pierre-et-Miquelon, en Nouvelle-Calédonie, en Polynésie française, dans les îles Wallis et Futuna et dans les Terres australes et antarctiques françaises, la référence au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données est remplacée par la référence aux règles en vigueur en métropole en vertu du règlement (UE) 2016/679 du 27 avril 2016.

### **Article 127**

L'article 37 de la présente loi n'est pas applicable en Nouvelle-Calédonie et en Polynésie française en ce qu'il intéresse l'action de groupe devant les tribunaux de l'ordre judiciaire.

## **Article 128**

**I.** - Pour l'application de l'article 37 de la présente loi dans les îles Wallis et Futuna, les mots : “ des articles L. 2122-1, L. 2122-5 ou L. 2122-9 du code du travail ” sont remplacées par les mots : “ de l'arrêté pris en application de l'article 73 de la loi n° 52-1322 du 15 décembre 1952 instituant un code du travail dans les territoires et territoires associés relevant du ministère de la France d'outre-mer ”.

**II.** - Pour l'application des articles 65 à 77 de la présente loi en Nouvelle-Calédonie, en Polynésie française, dans les îles Wallis et Futuna et dans les Terres australes et antarctiques françaises, les références aux articles L. 1451-1, L. 1461-1, L. 1462-1, L. 6113-7 et L. 6113-8 du code de la santé publique sont remplacées par les dispositions ayant le même objet applicables localement.

**III.** - Pour l'application de l'article 67 de la présente loi en Nouvelle-Calédonie et en Polynésie française, la référence à la section 1 du chapitre III du titre Ier du livre IV de la première partie du code de la santé publique est remplacée par les dispositions ayant le même objet applicables localement.