

**Loi du 1<sup>er</sup> août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale et portant modification**

- 1° de la loi modifiée du 7 mars 1980 sur l'organisation judiciaire ;
- 2° de la loi modifiée du 29 mai 1998 portant approbation de la Convention sur la base de l'article K.3 du Traité sur l'Union européenne portant création d'un Office européen de police (Convention Europol), signée à Bruxelles, le 26 juillet 1995 ;
- 3° de la loi du 20 décembre 2002 portant approbation - de la Convention établie sur base de l'article K.3 du Traité sur l'Union européenne, sur l'emploi de l'informatique dans le domaine des douanes, signé à Bruxelles, le 26 juillet 1995 ; - de l'Accord relatif à l'application provisoire entre certains États membres de l'Union européenne de la Convention établie sur base de l'article K.3 du Traité sur l'Union européenne, sur l'emploi de l'informatique dans le domaine des douanes, signé à Bruxelles, le 26 juillet 1995 ;
- 4° de la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité ;
- 5° de la loi modifiée du 16 juin 2004 portant réorganisation du centre socio-éducatif de l'État ;
- 6° de la loi modifiée du 25 août 2006 relative aux procédures d'identification par empreintes génétiques en matière pénale et portant modification du Code d'instruction criminelle ;
- 7° de la loi du 24 juin 2008 ayant pour objet le contrôle des voyageurs dans les établissements d'hébergement ;
- 8° de la loi modifiée du 29 mars 2013 relative à l'organisation du casier judiciaire ;
- 9° de la loi modifiée du 19 décembre 2014 facilitant l'échange transfrontalier d'informations concernant les infractions en matière de sécurité routière ;
- 10° de la loi modifiée du 25 juillet 2015 portant création du système de contrôle et de sanction automatisés ;
- 11° de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État ;
- 12° de la loi du 23 juillet 2016 portant mise en place d'un statut spécifique pour certaines données à caractère personnel traitées par le Service de renseignement de l'État ;
- 13° de la loi du 22 février 2018 relative à l'échange de données à caractère personnel et d'informations en matière policière ;
- 14° de la loi du 18 juillet 2018 sur la Police grand-ducale ; et
- 15° de la loi du 18 juillet 2018 sur l'Inspection générale de la Police.

Nous Henri, Grand-Duc de Luxembourg, Duc de Nassau,  
Notre Conseil d'État entendu ;

De l'assentiment de la Chambre des Députés ;

Vu la décision de la Chambre des Députés du 26 juillet 2018 et celle du Conseil d'État du 27 juillet 2018 portant qu'il n'y a pas lieu à second vote ;

*Avons ordonné et ordonnons :*

## **Chapitre 1<sup>er</sup> - Dispositions générales**

### **Art.1<sup>er</sup>. Objet et champ d'application**

(1) La présente loi s'applique aux traitements de données à caractère personnel mis en oeuvre 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 ».

(2) La présente loi s'applique également aux traitements de données à caractère personnel effectués :

- a) par la Police grand-ducale dans l'exécution de missions à des fins autres que celles visées au paragraphe 1<sup>er</sup> et prévues par des lois spéciales,
- b) par le Service de renseignement de l'État dans l'exécution de ses missions prévues à l'article 3 de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État,
- c) par l'Autorité nationale de sécurité dans l'exécution de ses missions prévues à l'article 20 de la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité,
- d) par l'Armée luxembourgeoise dans l'exécution de ses missions prévues à l'article 2 de la loi modifiée du 23 juillet 1952 concernant l'organisation militaire,
- e) par la Cellule de renseignement financier dans l'exécution de ses missions prévues aux articles 74-1 à 74-6 de la loi modifiée du 7 mars 1980 sur l'organisation judiciaire, et
- f) par les autorités luxembourgeoises dans le cadre des activités qui relèvent du champ d'application du titre V, chapitre 2, du Traité sur l'Union européenne relatif à la politique étrangère et de sécurité commune.

(3) La présente loi s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier.

### **Art. 2. Définitions**

(1) Aux fins de la présente loi, on entend par :

- 1° « données à caractère personnel » : toute information se rapportant à une personne physique identifiée ou identifiable, ci-après dénommée « personne concernée » ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ;
- 2° « traitement » : toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ;
- 3° « limitation du traitement » : le marquage de données à caractère personnel conservées en vue de limiter leur traitement futur ;

- 4° « profilage » : toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne ;
- 5° « pseudonymisation » : le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable ;
- 6° « fichier » : 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 ;
- 7° « autorité compétente » :
- a) toute autorité publique compétente pour la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, ainsi que les fonctionnaires et agents des administrations et services publics auxquels des lois spéciales ont attribué certains pouvoirs de police administrative ou judiciaire, dans les conditions et dans les limites fixées par ces lois, ou
  - b) tout autre organisme ou entité à qui le droit d'un État membre confie l'exercice de l'autorité publique et des prérogatives de puissance publique 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 ;
- 8° « responsable du traitement » : l'autorité compétente qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel ; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union européenne ou le droit luxembourgeois, le responsable du traitement ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union européenne ou le droit luxembourgeois ;
- 9° « sous-traitant » : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ;
- 10° « destinataire » : la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication des données à caractère personnel, qu'il s'agisse ou non d'un tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément à la loi ne sont pas considérées comme des destinataires ; le traitement de ces données par les autorités publiques en question est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement ;
- 11° « violation de données à caractère personnel » : une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données ;
- 12° « données génétiques » : les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question ;
- 13° « données biométriques » : les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques ;
- 14° « données concernant la santé » : les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la fourniture de soins de santé, qui révèlent des informations sur l'état de santé de cette personne ;

15° « autorité de contrôle » :

- a) l'autorité de contrôle instituée par la loi du 1<sup>er</sup> août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, ci-après désignée comme la « Commission Nationale pour la Protection des Données », et
- b) l'autorité de contrôle judiciaire instituée par l'article 40 ;

16° « organisation internationale » : une organisation internationale et les organismes de droit public international qui en relèvent, ou tout autre organisme qui est créé par un accord entre deux pays ou plus, ou en vertu d'un tel accord, y compris l'Organisation internationale de police criminelle (OIPC - Interpol).

(2) Pour l'application de la présente loi, lorsque les notions utilisées ne sont pas définies au paragraphe 1<sup>er</sup>, les définitions de l'article 4 du 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), ci-après désigné comme « le règlement (UE) n° 2016/679 », sont applicables.

## Chapitre 2 - Principes

### Art. 3. Principes relatifs au traitement des données à caractère personnel

(1) Les données à caractère personnel visées par la présente loi sont :

- a) traitées de manière licite et loyale ;
- b) collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées d'une manière incompatible avec ces finalités ;
- c) adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées ;
- d) 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 ;
- e) 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 ;
- f) 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, à l'aide de mesures techniques ou organisationnelles appropriées.

(2) Les traitements effectués, par le même ou par un autre responsable du traitement, pour l'une des finalités énoncées à l'article 1<sup>er</sup> 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 par le présent chapitre et par les chapitres IV et V.

(3) Ces traitements, par le même ou par un autre responsable du traitement, peuvent comprendre l'archivage dans l'intérêt public, à des fins scientifiques, statistiques ou historiques, pour l'une des finalités énoncées à l'article 1<sup>er</sup>.

(4) Le responsable du traitement est responsable du respect des paragraphes 1<sup>er</sup>, 2 et 3 et est en mesure de démontrer que ces dispositions sont respectées.

### Art. 4. Délais de conservation et d'examen

(1) Le responsable du traitement fixe des délais appropriés pour l'effacement des données à caractère personnel ou pour la vérification régulière de la nécessité de conserver les données à caractère personnel. Les délais sont à fixer eu égard à la finalité du traitement.

(2) Le responsable du traitement établit des règles procédurales en vue d'assurer le respect de ces délais qui déterminent les personnes intervenant au nom et pour compte du responsable du traitement dans cette procédure, y compris le délégué à la protection des données, ainsi que les délais dans lesquelles ces personnes doivent accomplir leurs tâches respectives. Les règles procédurales sont mises à la disposition de la personne concernée conformément à l'article 11 et à l'autorité de contrôle compétente sur demande de celle-ci.

**Art. 5. Distinction entre différentes catégories de personnes concernées**

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

- a) 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 ;
- b) les personnes reconnues coupables d'une infraction pénale ;
- c) 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, et
- d) 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 visées aux lettres a) et b).

**Art. 6. Distinction entre les données à caractère personnel et vérification de la qualité des données à caractère personnel**

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

(2) 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 ne soient pas transmises ou mises à disposition. À 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 nécessaires permettant à l'autorité compétente destinataire de juger de l'exactitude, de l'exhaustivité, de la fiabilité, ainsi que du niveau de mise à jour des données à caractère personnel en cause.

(3) 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 16.

**Art. 7. Licéité du traitement**

(1) Le traitement n'est licite que si et dans la mesure où il est nécessaire à l'exécution des missions de l'autorité compétente définie à l'article 2, paragraphe 1<sup>er</sup>, point 7<sup>o</sup>, pour une des finalités énoncées à l'article 1<sup>er</sup> et lorsque cette mission est effectuée en application de dispositions législatives régissant l'autorité compétente visée.

(2) Le traitement assure 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 et faits concernés.

**Art. 8. Conditions spécifiques applicables au traitement**

(1) Les données à caractère personnel collectées par les autorités compétentes pour les finalités énoncées à l'article 1<sup>er</sup> ne peuvent être traitées à des fins autres que celles y énoncées, à moins qu'un tel traitement ne soit autorisé par le droit de l'Union européenne ou par une disposition du droit luxembourgeois. Dans ce cas, le traitement de ces données est effectué conformément aux dispositions du règlement (UE) n° 2016/679 ou de la loi du 1<sup>er</sup> août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données.

(2) Lorsque des autorités compétentes sont chargées d'exécuter des missions autres que celles énoncées à l'article 1<sup>er</sup>, le règlement (UE) n° 2016/679 ou, le cas échéant, la loi du 1<sup>er</sup> août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données s'appliquent au traitement des données 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.

(3) Lorsque le droit de l'Union européenne ou une disposition du droit luxembourgeois applicable à l'autorité compétente qui transmet les données soumet leur traitement 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.

(4) L'autorité compétente qui transmet les données n'applique pas aux destinataires dans les autres États membres 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 en vertu du paragraphe 3 différentes de celles applicables aux transferts de données similaires à d'autres autorités compétentes établies sur le territoire du Grand-Duché de Luxembourg.

#### **Art. 9. Traitement portant sur des catégories particulières de données à caractère personnel**

Le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, ou l'appartenance syndicale, et le traitement 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 sont autorisés uniquement en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et uniquement :

- a) lorsqu'ils sont autorisés par le droit de l'Union européenne ou en application de la présente loi ou d'une autre disposition du droit luxembourgeois ;
- b) pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne physique, ou
- c) lorsque le traitement porte sur des données manifestement rendues publiques par la personne concernée.

#### **Art. 10. Décision individuelle automatisée**

(1) Toute décision fondée exclusivement sur un traitement automatisé, y compris le profilage, qui produit des effets juridiques défavorables pour la personne concernée ou l'affecte de manière significative, est interdite, à moins qu'elle ne soit autorisée par une disposition légale nationale ou par le droit de l'Union européenne, et que le responsable du traitement fournit des garanties appropriées pour les droits et libertés de la personne concernée, et au minimum le droit d'obtenir une intervention humaine de la part du responsable du traitement.

(2) Les décisions visées au paragraphe 1<sup>er</sup> ne sont pas fondées sur les catégories particulières de données à caractère personnel visées à l'article 9, à moins que des mesures appropriées pour la sauvegarde des droits et des libertés et des intérêts légitimes de la personne concernée ne soient en place.

(3) Tout profilage qui entraîne une discrimination à l'égard des personnes physiques sur la base des catégories particulières de données à caractère personnel visées à l'article 9 est interdit.

### **Chapitre 3 - Droits de la personne concernée**

#### **Art. 11. Communication et modalités de l'exercice des droits de la personne concernée**

(1) Le responsable du traitement prend des mesures raisonnables pour fournir toute information visée à l'article 12 et procède à toute communication relative au traitement ayant trait à l'article 10, aux articles 13 à 17 et à l'article 30 à la personne concernée d'une façon concise, compréhensible et aisément accessible, en des termes clairs et simples. Les informations sont fournies par tout moyen approprié, y compris par voie électronique. De manière générale, le responsable du traitement fournit les informations sous la même forme que la demande.

(2) Le responsable du traitement facilite l'exercice des droits conférés à la personne concernée par l'article 10 et les articles 13 à 17.

(3) Le responsable du traitement informe par écrit, dans les meilleurs délais, la personne concernée des suites données à sa demande.

(4) Aucun paiement n'est exigé pour fournir les informations visées à l'article 12 et pour procéder à toute communication et prendre toute mesure au titre de l'article 10, des articles 13 à 17 et de l'article 30. Lorsque les demandes d'une personne concernée sont manifestement infondées ou excessives, notamment en raison de leur caractère répétitif, le responsable du traitement peut :

- a) soit exiger le paiement de frais raisonnables qui tiennent compte des coûts administratifs supportés pour fournir les informations, procéder à la communication ou prendre les mesures demandées,

b) soit refuser de donner suite à la demande.

Il incombe au responsable du traitement de démontrer le caractère manifestement infondé ou excessif de la demande.

(5) Lorsque le responsable du traitement a des doutes raisonnables quant à l'identité de la personne physique présentant la demande visée aux articles 13 ou 15, il peut demander que lui soient fournies des informations supplémentaires nécessaires pour confirmer l'identité de la personne concernée.

### **Art. 12. Informations à mettre à la disposition de la personne concernée ou à lui fournir**

(1) Le responsable du traitement met à la disposition de la personne concernée au moins les informations suivantes :

- a) l'identité et les coordonnées du responsable du traitement ;
- b) les coordonnées du délégué à la protection des données ;
- c) les finalités du traitement auquel sont destinées les données à caractère personnel ;
- d) le droit d'introduire une réclamation auprès d'une des deux autorités de contrôle visées aux articles 39 et 40 et les coordonnées de ladite autorité ;
- e) l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, leur rectification ou leur effacement, et la limitation du traitement des données à caractère personnel relatives à une personne concernée.

(2) En plus des informations visées au paragraphe 1<sup>er</sup>, le responsable du traitement fournit à la personne concernée, dans des cas particuliers, les informations additionnelles suivantes afin de lui permettre d'exercer ses droits :

- a) la base juridique du traitement ;
- b) la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;
- c) le cas échéant, les catégories de destinataires des données à caractère personnel, y compris dans les pays tiers ou au sein d'organisations internationales ;
- d) au besoin, des informations complémentaires, en particulier lorsque les données à caractère personnel sont collectées à l'insu de la personne concernée.

(3) Le responsable du traitement peut retarder ou limiter la fourniture des informations à la personne concernée en application du paragraphe 2, ou ne pas fournir ces informations, dès lors et aussi longtemps qu'une mesure de cette nature constitue une mesure nécessaire et proportionnée dans une société démocratique, eu égard à la finalité du traitement concerné, et en tenant dûment compte des droits fondamentaux et des intérêts légitimes de la personne physique concernée, pour :

- a) éviter de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires ;
- b) 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 ;
- c) protéger la sécurité publique ;
- d) protéger la sécurité nationale et la défense nationale ; ou
- e) protéger les droits et libertés d'autrui.

### **Art. 13. Droit d'accès par la personne concernée**

Sous réserve de l'article 14, la personne concernée a le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données ainsi que les informations suivantes :

- a) les finalités du traitement ainsi que sa base juridique ;
- b) les catégories de données à caractère personnel concernées ;
- c) les destinataires ou catégories de destinataires auxquels les données à caractère personnel ont été communiquées, en particulier les destinataires qui sont établis dans des pays tiers ou les organisations internationales ;
- d) lorsque cela est possible, la durée de conservation des données à caractère personnel envisagée ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;

- e) l'existence du droit de demander au responsable du traitement la rectification ou l'effacement des données à caractère personnel, ou la limitation du traitement des données à caractère personnel relatives à la personne concernée ;
- f) le droit d'introduire une réclamation auprès de l'une des deux autorités de contrôle compétentes visées aux articles 39 et 40 et les coordonnées de ladite autorité ;
- g) la communication des données à caractère personnel en cours de traitement, ainsi que toute information disponible quant à leur source.

#### **Art. 14. Limitations du droit d'accès**

(1) Le responsable du traitement peut limiter, entièrement ou partiellement, le droit d'accès de la personne concernée, dès lors et aussi longtemps qu'une telle limitation partielle ou complète constitue une mesure nécessaire et proportionnée dans une société démocratique, eu égard à la finalité du traitement concerné, et en tenant dûment compte des droits fondamentaux et des intérêts légitimes de la personne physique concernée, pour :

- a) éviter de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires ;
- b) 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 ;
- c) protéger la sécurité publique ;
- d) protéger la sécurité nationale et la défense nationale ; ou
- e) protéger les droits et libertés d'autrui.

(2) Dans les cas visés au paragraphe 1<sup>er</sup>, le responsable du traitement informe la personne concernée par écrit, 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 paragraphe 1<sup>er</sup>. Le responsable du traitement informe la personne concernée des possibilités d'introduire une réclamation auprès de l'autorité de contrôle compétente ou de former un recours juridictionnel.

(3) Le responsable du traitement consigne les motifs de fait ou de droit sur lesquels se fonde la décision. Ces informations sont mises à la disposition de l'autorité de contrôle compétente.

#### **Art. 15. Droit de rectification ou d'effacement des données à caractère personnel et limitation du traitement**

(1) Le responsable du traitement rectifie, dans les meilleurs délais, des données à caractère personnel de la personne concernée qui sont inexactes. Compte tenu des finalités du traitement, les données à caractère personnel incomplètes de la personne concernée sont complétées, y compris par une déclaration complémentaire fournie par la personne concernée fournie à cet effet.

(2) Le responsable du traitement efface dans les meilleurs délais les données à caractère personnel de la personne concernée lorsque le traitement de ces données constitue une violation des dispositions prévues par les articles 3, 7 ou 9, ou lorsque les données à caractère personnel doivent être effacées pour respecter une obligation légale à laquelle est soumis le responsable du traitement.

(3) Au lieu de procéder à l'effacement, le responsable du traitement limite le traitement lorsque :

- a) l'exactitude des données à caractère personnel est contestée par la personne concernée et qu'il ne peut être déterminé si les données sont exactes ou non, ou
- b) les données à caractère personnel doivent être conservées à des fins probatoires.

Lorsque le traitement est limité en vertu de l'alinéa 1<sup>er</sup>, lettre a), du présent paragraphe, le responsable du traitement informe la personne concernée avant de lever la limitation du traitement.

(4) Le responsable du traitement informe la personne concernée par écrit de tout refus de rectifier ou d'effacer des données à caractère personnel ou de limiter le traitement, ainsi que des motifs du refus. Le responsable du traitement peut limiter, en tout ou en partie, la fourniture de ces informations, dès lors qu'une telle limitation constitue une mesure nécessaire et proportionnée dans une société démocratique, eu égard à la finalité du traitement concerné, et en tenant dûment compte des droits fondamentaux et des intérêts légitimes de la personne physique concernée pour :



- a) éviter de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires ;
- b) 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 ;
- c) protéger la sécurité publique ;
- d) protéger la sécurité nationale et la défense nationale ; ou
- e) protéger les droits et libertés d'autrui.

Le responsable du traitement informe la personne concernée des possibilités d'introduire une réclamation auprès d'une autorité de contrôle ou de former un recours juridictionnel.

(5) Le responsable du traitement communique la rectification des données à caractère personnel inexactes à l'autorité compétente dont proviennent les données à caractère personnel inexactes.

(6) Lorsque des données à caractère personnel ont été rectifiées ou effacées ou que le traitement a été limité au titre des paragraphes 1, 2 et 3, le responsable du traitement adresse une notification aux destinataires afin que ceux-ci rectifient ou effacent les données à caractère personnel ou limitent le traitement des données à caractère personnel sous leur responsabilité.

#### **Art. 16. Exercice des droits de la personne concernée et vérification par l'autorité de contrôle**

(1) Dans les cas visés à l'article 12, paragraphe 3, à l'article 14, paragraphe 1<sup>er</sup>, et à l'article 15, paragraphe 4, les droits de la personne concernée peuvent être exercés par l'intermédiaire de l'autorité de contrôle compétente.

(2) Le responsable du traitement informe la personne concernée de la possibilité qu'elle a d'exercer ses droits par l'intermédiaire de l'autorité de contrôle compétente en application du paragraphe 1<sup>er</sup>.

(3) Lorsque le droit visé au paragraphe 1<sup>er</sup> est exercé, l'autorité de contrôle compétente informe au moins la personne concernée du fait qu'elle a procédé à toutes les vérifications nécessaires ou à un examen. L'autorité de contrôle informe également la personne concernée de son droit de former un recours juridictionnel.

#### **Art. 17. Droits des personnes concernées lors des enquêtes judiciaires et des procédures pénales**

Lorsque les données à caractère personnel sont relatives à des faits qui font l'objet d'une enquête préliminaire, d'une instruction préparatoire, qui ont été renvoyés devant une juridiction de jugement, qui font l'objet d'une citation, ou lorsque l'autorité compétente sur base de la loi modifiée du 10 août 1992 relative à la protection de la jeunesse est saisie de ces faits, les droits visés aux articles 12, 13 et 15 sont exercés conformément aux dispositions du Code de procédure pénale ou à d'autres dispositions légales applicables.

### **Chapitre 4 - Responsable du traitement et sous-traitant**

#### *Section 1<sup>ère</sup> - Obligations générales*

#### **Art. 18. Obligations incombant au responsable du traitement**

(1) Le responsable du traitement, compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, met en œuvre les mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément à la présente loi. Ces mesures sont réexaminées et actualisées, si nécessaire.

(2) Lorsque cela est proportionné au regard des activités de traitement, les mesures visées au paragraphe 1<sup>er</sup> comprennent la mise en œuvre de politiques appropriées en matière de protection des données par le responsable du traitement.

#### **Art. 19. Protection des données dès la conception et protection des données par défaut**

(1) Compte tenu de l'état des connaissances, des coûts de la mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant lors de la détermination des moyens du traitement que lors du traitement proprement

dit, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires, afin de répondre aux exigences de la présente loi et de protéger les droits des personnes concernées.

(2) Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cette obligation s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne concernée.

#### **Art. 20. Responsables conjoints du traitement**

(1) Lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement. Les responsables conjoints du traitement définissent de manière transparente leurs obligations respectives aux fins d'assurer le respect de la loi, notamment en ce qui concerne l'exercice des droits de la personne concernée, et leurs obligations respectives quant à la communication des informations visées aux articles 11 et 12, par voie d'accord entre eux. Le point de contact unique pour les personnes concernées, afin que celles-ci puissent exercer leurs droits, est désigné dans l'accord.

(2) Indépendamment des termes de l'accord visé au paragraphe 1<sup>er</sup>, la personne concernée peut exercer les droits que lui confère la présente loi à l'égard de et contre chacun des responsables du traitement.

#### **Art. 21. Sous-traitant**

(1) Le responsable du traitement, lorsqu'un traitement doit être effectué pour son compte, fait uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière que le traitement réponde aux exigences de la présente loi et garantisse la protection des droits de la personne concernée.

(2) Le sous-traitant ne recrute pas un autre sous-traitant sans l'autorisation écrite préalable, spécifique ou générale, du responsable du traitement. Dans le cas d'une autorisation écrite générale, le sous-traitant informe le responsable du traitement de tout changement prévu concernant l'ajout ou le remplacement d'autres sous-traitants, donnant ainsi au responsable du traitement la possibilité d'émettre des objections à l'encontre de ces changements.

(3) Le traitement par un sous-traitant est régi par un contrat ou un autre acte juridique au titre du droit de l'Union européenne, du droit luxembourgeois ou du droit d'un autre État membre, qui lie le sous-traitant à l'égard du responsable du traitement et qui 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 et les obligations et les droits du responsable du traitement. Ce contrat ou cet autre acte juridique prévoit, notamment, que le sous-traitant :

- a) n'agit que sur instruction du responsable du traitement ;
- b) veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
- c) aide le responsable du traitement, par tout moyen approprié, à veiller au respect des dispositions relatives aux droits de la personne concernée ;
- d) selon le choix du responsable du traitement, supprime toutes les données à caractère personnel ou les renvoie au responsable du traitement au terme de la prestation des services de traitement des données, et détruit les copies existantes, à moins qu'une disposition légale n'exige la conservation des données à caractère personnel ;
- e) met à la disposition du responsable du traitement toutes les informations nécessaires pour apporter la preuve du respect du présent article ;
- f) respecte les conditions visées aux paragraphes 2 et 3 pour recruter un autre sous-traitant.

(4) Le contrat ou l'autre acte juridique visé au paragraphe 3 revêt la forme écrite, y compris la forme électronique.

(5) Si, en violation de la présente loi, un sous-traitant détermine les finalités et les moyens du traitement, il est considéré comme un responsable du traitement pour ce qui concerne ce traitement.

#### **Art. 22. Traitement effectué sous l'autorité du responsable du traitement ou du sous-traitant**

Le sous-traitant, et toute personne agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel ne les traite que sur instruction du responsable du traitement, à moins d'y être obligé par une disposition légale.

#### **Art. 23. Registre des activités de traitement**

(1) Les responsables du traitement tiennent un registre de toutes les catégories d'activités de traitement effectuées sous leur responsabilité. Ce registre comporte toutes les informations suivantes :

- a) le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement et du délégué à la protection des données ;
- b) les finalités du traitement ;
- c) les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales ;
- d) une description des catégories de personnes concernées et des catégories de données à caractère personnel ;
- e) le cas échéant, le recours au profilage ;
- f) le cas échéant, les catégories de transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale ;
- g) une indication de la base juridique de l'opération de traitement, y compris les transferts, à laquelle les données à caractère personnel sont destinées ;
- h) dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données à caractère personnel ;
- i) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 28, paragraphe 1<sup>er</sup>.

(2) Chaque sous-traitant tient un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement, comprenant :

- a) le nom et les coordonnées du ou des sous-traitants, de chaque responsable du traitement pour le compte duquel le sous-traitant agit et, le cas échéant, du délégué à la protection des données ;
- b) les catégories de traitements effectués pour le compte de chaque responsable du traitement ;
- c) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, lorsqu'il en est expressément chargé par le responsable du traitement, y compris l'identification de ce pays tiers ou de cette organisation internationale ;
- d) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 28, paragraphe 1<sup>er</sup>.

(3) Les registres visés aux paragraphes 1 et 2 se présentent sous une forme écrite, y compris la forme électronique. Le responsable du traitement et le sous-traitant mettent ces registres à la disposition de l'autorité de contrôle, sur demande.

#### **Art. 24. Journalisation**

(1) Des journaux sont établis au moins pour les opérations de traitement suivantes dans des systèmes de traitement automatisé : la collecte, la modification, la consultation, la communication, y compris les transferts, l'interconnexion et l'effacement. Les journaux des opérations de consultation et de communication permettent d'établir le motif, la date et l'heure de celles-ci et l'identification de la personne qui a consulté ou communiqué les données à caractère personnel, ainsi que l'identité des destinataires de ces données à caractère personnel.

(2) Les journaux sont utilisés uniquement à des fins de vérification de la licéité du traitement, d'autocontrôle, de garantie de l'intégrité et de la sécurité des données à caractère personnel et à des fins de procédures pénales.

(3) Le responsable du traitement et le sous-traitant mettent les journaux à la disposition de l'autorité de contrôle sur demande de celle-ci.

#### **Art. 25. Coopération avec l'autorité de contrôle compétente**

Le responsable du traitement et le sous-traitant coopèrent avec l'autorité de contrôle compétente, à la demande de celle-ci, dans l'exécution de ses missions.

#### **Art. 26. Analyse d'impact relative à la protection des données**

(1) Lorsqu'un type de traitement, en particulier par le recours aux nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques, le responsable du traitement effectue préalablement au traitement une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.

(2) L'analyse visée au paragraphe 1<sup>er</sup> contient au moins une description générale des opérations de traitement envisagées, une évaluation des risques pour les droits et libertés des personnes concernées, les mesures envisagées pour faire face à ces risques, les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect de la loi, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes touchées.

#### **Art. 27. Consultation préalable de l'autorité de contrôle compétente**

(1) Le responsable du traitement ou le sous-traitant consulte l'autorité de contrôle compétente préalablement au traitement des données à caractère personnel qui fera partie d'un nouveau fichier à créer :

- a) lorsqu'une analyse d'impact relative à la protection des données, telle qu'elle est prévue à l'article 26, indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque, ou
- b) 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.

(2) L'autorité de contrôle compétente est consultée dans le cadre de l'élaboration d'un projet de loi ou d'un projet de règlement grand-ducal qui se rapporte au traitement.

(3) L'autorité de contrôle peut établir une liste des opérations de traitement devant faire l'objet d'une consultation préalable conformément au paragraphe 1<sup>er</sup>.

(4) Le responsable du traitement fournit à l'autorité de contrôle l'analyse d'impact relative à la protection des données en vertu de l'article 26 et, sur demande, toute autre information afin de permettre à l'autorité de contrôle d'apprécier la conformité du traitement et, en particulier, les risques pour la protection des données à caractère personnel de la personne concernée et les garanties qui s'y rapportent.

(5) Lorsque l'autorité de contrôle compétente est d'avis que le traitement prévu visé au paragraphe 1<sup>er</sup> constituerait une violation de la présente loi, en particulier lorsque le responsable du traitement n'a pas suffisamment identifié ou atténué le risque, l'autorité de contrôle compétente fournit par écrit, dans un délai maximum de six semaines à compter de la réception de la demande de consultation, un avis écrit au responsable du traitement, et le cas échéant au sous-traitant, et elle peut faire usage des pouvoirs visés à l'article 14 de la loi du 1<sup>er</sup> août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données ou à l'article 43 de la présente loi, en fonction de l'autorité de contrôle compétente. Ce délai peut être prolongé d'un mois, en fonction de la complexité du traitement prévu. L'autorité de contrôle informe le responsable du traitement et, le cas échéant, le sous-traitant de toute prorogation dans un délai d'un mois à compter de la réception de la demande de consultation, ainsi que des motifs du retard.

## Section 2 - Sécurité des données

### Art. 28. Sécurité du traitement

(1) Compte tenu de l'état des connaissances, des coûts de la mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles 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 visées à l'article 9.

(2) En ce qui concerne le traitement automatisé, le responsable du traitement ou le sous-traitant met en œuvre, à la suite d'une évaluation des risques, des mesures destinées à :

- a) empêcher toute personne non autorisée d'accéder aux installations utilisées pour le traitement (contrôle de l'accès aux installations) ;
- b) empêcher que des supports de données puissent être lus, copiés, modifiés ou supprimés de façon non autorisée (contrôle des supports de données) ;
- c) 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 (contrôle de la conservation) ;
- d) empêcher que les systèmes de traitement automatisé puissent être utilisés par des personnes non autorisées à l'aide d'installations de transmission de données (contrôle des utilisateurs) ;
- e) 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 (contrôle de l'accès aux données) ;
- f) 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 (contrôle de la transmission) ;
- g) 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 (contrôle de l'introduction) ;
- h) 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 (contrôle du transport) ;
- i) garantir que les systèmes installés puissent être rétablis en cas d'interruption (restauration) ;
- j) garantir que les fonctions du système opèrent, que les erreurs de fonctionnement soient signalées (fiabilité) et que les données à caractère personnel conservées ne puissent pas être corrompues par un dysfonctionnement du système (intégrité).

### Art. 29. Notification à l'autorité de contrôle d'une violation de données à caractère personnel

(1) En cas de violation de données à caractère personnel, le responsable du traitement notifie la violation en question à l'autorité de contrôle compétente dans les meilleurs délais et, si possible, dans un délai de 72 heures au plus tard après en avoir pris connaissance, à moins qu'il soit peu probable que la violation en question n'engendre des risques pour les droits et les libertés d'une personne physique. Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.

(2) Le sous-traitant notifie au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance.

(3) La notification visée aux paragraphes 1 et 2 doit au moins :

- a) décrire la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- b) communiquer le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- c) décrire les conséquences probables de la violation de données à caractère personnel, et

d) décrire les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

(4) Si et dans la mesure où il n'est pas possible de fournir toutes les informations en même temps, les informations peuvent être communiquées de manière échelonnée sans autre retard indu.

(5) Le responsable du traitement documente toute violation de données à caractère personnel visée au paragraphe 1<sup>er</sup> en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier, afin que la documentation ainsi constituée permet à l'autorité de contrôle de vérifier le respect du présent article.

(6) Lorsque la violation de données à caractère personnel porte sur des données à caractère personnel qui ont été transmises par le responsable du traitement d'un autre État membre ou à celui-ci, les informations visées au paragraphe 3 sont communiquées au responsable du traitement de cet État membre dans les meilleurs délais.

### **Art. 30. Communication à la personne concernée d'une violation de données à caractère personnel**

(1) Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et les libertés d'une personne physique, le responsable du traitement communique la violation à la personne concernée dans les meilleurs délais.

(2) La communication à la personne concernée visée au paragraphe 1<sup>er</sup> décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins les informations et les mesures visées à l'article 29, paragraphe 3, lettres b), c) et d).

(3) La communication à la personne concernée visée au paragraphe 1<sup>er</sup> n'est pas nécessaire si l'une ou l'autre des conditions suivantes est remplie :

- a) le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et ces dernières ont été appliquées aux données à caractère personnel affectées par ladite violation, en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement ;
- b) le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et les libertés des personnes concernées visé au paragraphe 1<sup>er</sup> n'est plus susceptible de se matérialiser ;
- c) elle exigerait des efforts disproportionnés. Dans ce cas, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace.

(4) Si le responsable du traitement n'a pas déjà communiqué à la personne concernée la violation de données à caractère personnel la concernant, l'autorité de contrôle peut, après avoir examiné si cette violation est susceptible d'engendrer un risque élevé, exiger du responsable du traitement qu'il procède à cette communication ou décider que l'une ou l'autre des conditions visées au paragraphe 3 est remplie.

(5) La communication à la personne concernée visée au paragraphe 1<sup>er</sup> peut être retardée, limitée ou omise, sous réserve des conditions et pour les motifs visés à l'article 12, paragraphe 3.

### *Section 3 - Délégué à la protection des données*

#### **Art. 31. Désignation du délégué à la protection des données**

(1) Le responsable du traitement désigne un délégué à la protection des données.

(2) Le délégué à la protection des données est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à exercer les missions visées à l'article 33.

(3) Un seul délégué à la protection des données peut être désigné pour plusieurs autorités compétentes, compte tenu de leur structure organisationnelle et de leur taille.

(4) Le responsable du traitement publie les coordonnées du délégué à la protection des données et les communique à l'autorité de contrôle.

### **Art. 32. Fonction du délégué à la protection des données**

(1) Le responsable du traitement veille à ce que le délégué à la protection des données soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel.

(2) Le responsable du traitement aide le délégué à la protection des données à exercer les missions visées à l'article 33 en fournissant les ressources nécessaires pour exercer ces missions ainsi que l'accès aux données à caractère personnel et aux traitements, et lui permettant d'entretenir ses connaissances spécialisées.

### **Art. 33. Missions du délégué à la protection des données**

Le responsable du traitement confie au délégué à la protection des données au moins les missions suivantes :

- a) informer et conseiller le responsable du traitement et les employés qui procèdent au traitement sur les obligations qui leur incombent en vertu de la présente loi et d'autres dispositions du droit de l'Union européenne ou du droit luxembourgeois en matière de protection des données ;
- b) contrôler le respect de la présente loi, d'autres dispositions du droit de l'Union européenne ou du droit luxembourgeois en matière de protection des données et des règles internes du responsable du traitement en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant à des opérations de traitement, et les audits s'y rapportant ;
- c) dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci en vertu de l'article 26 ;
- d) coopérer avec l'autorité de contrôle compétente ;
- e) faire office de point de contact pour la personne concernée et l'autorité de contrôle sur les questions relatives au traitement, y compris la consultation préalable visée à l'article 27, et mener des consultations, le cas échéant, sur tout autre sujet en relation avec ses missions.

## **Chapitre 5 - Transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales**

### **Art. 34. Principes généraux applicables aux transferts de données à caractère personnel**

(1) Un transfert, par des autorités compétentes, de données à caractère personnel qui font ou sont destinées à faire l'objet d'un traitement après leur transfert vers un pays tiers ou à une organisation internationale, y compris des transferts ultérieurs vers un autre pays tiers ou à une autre organisation internationale, n'a lieu, sous réserve du respect des autres dispositions de la présente loi, que lorsque les conditions définies dans le présent chapitre sont respectées, à savoir :

- a) le transfert est nécessaire aux fins énoncées à l'article 1<sup>er</sup> ;
- b) les données à caractère personnel sont transférées à un responsable du traitement dans un pays tiers ou à une organisation internationale qui est une autorité compétente aux fins visées à l'article 1<sup>er</sup> ;
- c) en cas de transmission ou de mise à disposition de données à caractère personnel provenant d'un autre État membre, celui-ci a préalablement autorisé ce transfert conformément à son droit national ;
- d) la Commission européenne a adopté une décision d'adéquation en application de l'article 35 ou, en l'absence d'une telle décision, des garanties appropriées ont été prévues ou existent en application de l'article 36 ou, en l'absence de décision d'adéquation au titre de l'article 35 et de garanties appropriées conformément à l'article 36, des dérogations pour des situations particulières s'appliquent en vertu de l'article 37 ;
- e) en cas de transfert ultérieur vers un autre pays tiers ou à une autre organisation internationale, l'autorité compétente qui a procédé au transfert initial ou une autre autorité compétente du même État membre autorise le transfert ultérieur, après avoir dûment pris en considération l'ensemble des facteurs pertinents, y compris la gravité de l'infraction pénale, la finalité pour laquelle les données à caractère personnel ont

été transférées initialement et le niveau de protection des données à caractère personnel dans le pays tiers ou au sein de l'organisation internationale vers lequel ou laquelle les données à caractère personnel sont transférées ultérieurement.

(2) Les transferts effectués sans l'autorisation préalable d'un autre État membre prévue au paragraphe 1<sup>er</sup>, lettre c), sont autorisés uniquement lorsque le transfert de données à caractère personnel est nécessaire aux fins de la prévention d'une menace grave et immédiate pour la sécurité publique d'un État membre ou d'un pays tiers ou pour les intérêts essentiels d'un État membre et si l'autorisation préalable ne peut pas être obtenue en temps utile. L'autorité à laquelle il revient d'accorder l'autorisation préalable est informée sans retard.

(3) Toutes les dispositions du présent chapitre sont appliquées de manière que le niveau de protection des personnes physiques assuré par la présente loi ne soit pas compromis.

### **Art. 35. Transferts sur la base d'une décision d'adéquation**

(1) Un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale peut avoir lieu lorsque la Commission européenne, en application de l'article 36 de la directive (UE) n° 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, ci-après désignée comme « la directive (UE) n° 2016/680 », a constaté par voie de décision que le pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou l'organisation internationale en question assure un niveau de protection adéquat. Un tel transfert ne nécessite pas d'autorisation spécifique.

(2) Une décision adoptée en vertu de l'article 36, paragraphe 5, de la directive (UE) n° 2016/680 est sans préjudice des transferts de données à caractère personnel vers le pays tiers, le territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou à l'organisation internationale en question, effectués en application des articles 36 et 37.

### **Art. 36. Transferts moyennant des garanties appropriées**

(1) En l'absence de décision en vertu de l'article 35, un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale peut avoir lieu lorsque :

- a) des garanties appropriées en ce qui concerne la protection des données à caractère personnel sont fournies dans un instrument juridiquement contraignant, ou
- b) le responsable du traitement a évalué toutes les circonstances du transfert et estime qu'il existe des garanties appropriées au regard de la protection des données à caractère personnel.

(2) Le responsable du traitement informe l'autorité de contrôle compétente des catégories de transferts relevant du paragraphe 1<sup>er</sup>, lettre b).

(3) Lorsqu'un transfert est effectué sur la base du paragraphe 1<sup>er</sup>, lettre b), ce transfert est documenté et la documentation est mise à la disposition de l'autorité de contrôle compétente, sur demande, et comporte la date et l'heure du transfert, des informations sur l'autorité compétente destinataire, la justification du transfert et les données à caractère personnel transférées.

### **Art. 37. Dérogations pour des situations particulières**

(1) En l'absence de décision d'adéquation en vertu de l'article 35 ou de garanties appropriées en vertu de l'article 36, un transfert ou une catégorie de transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale ne peut avoir lieu qu'à condition que le transfert soit nécessaire :

- a) à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne ;
- b) à la sauvegarde des intérêts légitimes de la personne concernée ;
- c) pour prévenir une menace grave et immédiate pour la sécurité publique d'un État membre ou d'un pays tiers ;
- d) dans des cas particuliers, aux fins énoncées à l'article 1<sup>er</sup>, ou



e) dans un cas particulier, à la constatation, à l'exercice ou à la défense de droits en justice en rapport avec les fins énoncées à l'article 1<sup>er</sup>.

(2) Les données à caractère personnel ne sont pas transférées si l'autorité compétente qui transfère les données estime que les libertés et droits fondamentaux de la personne concernée l'emportent sur l'intérêt public dans le cadre du transfert visé au paragraphe 1<sup>er</sup>, lettres d) et e).

(3) Lorsqu'un transfert est effectué sur la base du paragraphe 1<sup>er</sup>, lettre b), ce transfert est documenté et la documentation est mise à la disposition de l'autorité de contrôle, sur demande, et indique la date et l'heure du transfert, donne des informations sur l'autorité compétente destinataire, indique la justification du transfert et les données à caractère personnel transférées.

### **Art. 38. Transferts de données à caractère personnel à des destinataires établis dans des pays tiers**

(1) Par dérogation à l'article 34, paragraphe 1<sup>er</sup>, lettre b), et sans préjudice de tout accord international visé au paragraphe 2, les autorités compétentes au sens de l'article 2, point 7), lettre a), peuvent, dans certains cas particuliers, transférer des données à caractère personnel directement aux destinataires établis dans des pays tiers, uniquement lorsque les autres dispositions de la présente loi sont respectées et que toutes les conditions ci-après sont remplies :

- a) le transfert est strictement nécessaire à l'exécution de la mission de l'autorité compétente qui transfère les données ainsi que le prévoit le droit de l'Union européenne ou aux fins énoncées à l'article 1<sup>er</sup> ;
- b) l'autorité compétente qui transfère les données établit qu'il n'existe pas de libertés ni de droits fondamentaux de la personne concernée qui prévalent sur l'intérêt public nécessitant le transfert dans le cas en question ;
- c) l'autorité compétente qui transfère les données estime que le transfert à une autorité qui est compétente aux fins visées à l'article 1<sup>er</sup> dans le pays tiers est inefficace ou inapproprié, notamment parce que le transfert ne peut pas être effectué en temps opportun ;
- d) l'autorité qui est compétente aux fins visées à l'article 1<sup>er</sup> dans le pays tiers est informée dans les meilleurs délais, à moins que cela ne soit inefficace ou inapproprié, et
- e) l'autorité compétente qui transfère les données informe le destinataire de la finalité ou des finalités déterminées pour lesquelles les données à caractère personnel ne doivent faire l'objet d'un traitement que par cette dernière, à condition qu'un tel traitement soit nécessaire.

(2) Par accord international visé au paragraphe 1<sup>er</sup>, on entend tout accord international bilatéral ou multilatéral en vigueur entre le Grand-Duché de Luxembourg et des pays tiers dans le domaine de la coopération judiciaire en matière pénale et de la coopération policière.

(3) L'autorité compétente qui transfère les données informe l'autorité de contrôle des transferts relevant du présent article.

(4) Lorsqu'un transfert est effectué sur la base du paragraphe 1<sup>er</sup>, ce transfert est documenté.

## **Chapitre 6 - Autorités de contrôle indépendantes**

### *Section 1<sup>ère</sup> - Autorité de contrôle administrative*

#### **Art. 39. Compétence de la Commission nationale pour la protection des données**

L'autorité de contrôle instituée par l'article 3 de la loi du 1<sup>er</sup> août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données est compétente pour contrôler et vérifier le respect des dispositions de la présente loi.

### *Section 2 - Autorité de contrôle judiciaire*

#### **Art. 40. Création, compétence et composition de l'autorité de contrôle judiciaire**

(1) Il est créé une autorité de contrôle de la protection des données judiciaires, ci-après désignée comme « autorité de contrôle judiciaire ».

(2) Par dérogation à l'article 39, les opérations de traitement de données à caractère personnel effectuées par les juridictions de l'ordre judiciaire, y compris le ministère public, et de l'ordre administratif dans l'exercice

de leurs fonctions juridictionnelles, que ce soit pour les finalités visées à l'article 1<sup>er</sup> de la présente loi ou pour celles visées par le règlement (UE) n° 2016/679, sont soumises au contrôle de l'autorité de contrôle judiciaire.

(3) L'autorité de contrôle judiciaire est composée de six membres effectifs et de leurs suppléants comme suit :

- 1) le Président de la Cour supérieure de Justice ou son délégué ;
- 2) un représentant des autres juridictions de l'ordre judiciaire ;
- 3) le Président de la Cour administrative ou son délégué ;
- 4) le Procureur général d'État ou son délégué ;
- 5) un représentant du Parquet de l'arrondissement de Luxembourg ou de l'arrondissement de Diekirch, et
- 6) un représentant de la Commission nationale pour la protection des données.

Un fonctionnaire ou employé de l'administration judiciaire assume le rôle de secrétaire de l'autorité de contrôle judiciaire. Un ou plusieurs autres fonctionnaires ou employés de l'administration judiciaire peuvent être nommés en tant que membres du secrétariat de l'autorité de contrôle judiciaire, dont un en tant que secrétaire suppléant.

(4) Les membres effectifs et leurs suppléants ainsi que les fonctionnaires et employés assurant le secrétariat de l'autorité de contrôle judiciaire sont nommés par arrêté du ministre ayant la justice dans ses attributions sur proposition :

- 1) du président de la Cour supérieure de Justice pour les membres suppléants visés au paragraphe 3, alinéa 1<sup>er</sup>, points 1) et 2), et pour les fonctionnaires et employés visés au paragraphe 3, alinéa 2 ;
- 2) du procureur général d'État pour les membres effectifs et suppléants visés au paragraphe 3, points 4) et 5), et
- 3) du président de la Commission nationale pour la protection des données pour le membre visé au paragraphe 3, point 6).

(5) Ne peuvent être nommés que des membres effectifs et suppléants qui disposent d'une ancienneté d'au moins trois ans au sein respectivement de la magistrature de l'ordre judiciaire, des juridictions administratives ou de la Commission nationale pour la protection des données. La durée du mandat des membres effectifs et de leurs suppléants est de six ans et est renouvelable une fois. Les mandats prennent encore fin en cas de démission en tant que membre de l'autorité de contrôle judiciaire ou en tant que membre de la magistrature de l'ordre judiciaire, des juridictions administratives ou de la Commission nationale pour la protection des données, ou en cas de mise ou de départ à la retraite. Un membre ne peut être démis de son mandat que s'il a commis une faute grave ou s'il ne remplit plus les conditions nécessaires à l'exercice de ses fonctions. En cas de vacance d'un mandat effectif ou suppléant, il est pourvu à son remplacement par la nomination d'un nouveau membre, désigné conformément au paragraphe 4, qui achève le mandat de celui qu'il remplace.

(6) Pendant la durée de leur mandat, les membres effectifs de l'autorité de contrôle judiciaire bénéficient chacun d'une prime mensuelle non pensionnable de cinquante points indiciaires. Cette prime est de trente points pour les membres suppléants de l'autorité de contrôle judiciaire et de vingt points pour les membres de son secrétariat.

En cas de nomination d'un délégué au sens des paragraphes 3 et 4, le titulaire ayant procédé à la délégation ne pourra bénéficier de la prime visée à l'alinéa 1<sup>er</sup> pendant la durée de cette délégation.

#### **Art. 41. Fonctionnement de l'autorité de contrôle judiciaire**

(1) La présidence de l'autorité de contrôle judiciaire est assurée par le Président de la Cour supérieure de Justice ou son délégué et sa vice-présidence est assurée par le Président de la Cour administrative ou son délégué.

(2) L'autorité de contrôle judiciaire ne peut valablement délibérer que lorsque au moins trois de ses membres effectifs ou suppléants, dont au moins un membre effectif, sont présents. Le membre effectif qui est empêché de participer à une réunion en informe son suppléant.

L'autorité de contrôle judiciaire peut s'adjoindre des experts qui peuvent assister, à sa demande, aux réunions avec voix consultative.

(3) L'autorité de contrôle judiciaire se réunit, sur convocation de son président, toutes les fois que l'exigent les affaires comprises dans ses attributions. Les réunions de l'autorité de contrôle judiciaire sont présidées

par son président ou, en cas d'absence, par son vice-président, sinon conformément aux dispositions de son règlement interne visé au paragraphe 10.

Hormis le cas d'urgence, la convocation, contenant l'ordre du jour et mentionnant le lieu, le jour et l'heure de la réunion, est envoyée par voie postale ou par voie électronique au moins huit jours de calendrier avant la date fixée pour la réunion aux adresses indiquées par les membres effectifs.

(4) Le président ouvre et clôt la réunion et dirige les débats. Lorsque le président constate que l'autorité de contrôle judiciaire n'est pas en nombre pour délibérer valablement, il clôt la réunion. Dans ce cas il convoque à nouveau, dans un délai de huit jours de calendrier, l'autorité de contrôle judiciaire avec le même ordre du jour. L'autorité de contrôle judiciaire siège et délibère alors valablement quel que soit le nombre et la qualité des membres présents.

(5) Le président et les autres membres de l'autorité de contrôle judiciaire disposent chacun d'une voix. Ils votent à main levée. Les décisions sont prises à la majorité des voix exprimées, hormis les abstentions. En cas de partage des voix, celle du président de la réunion est prépondérante.

(6) Le secrétaire établit après chaque réunion un procès-verbal indiquant le nom des membres présents ou excusés, l'ordre du jour de la réunion ainsi que les décisions prises et, le cas échéant, les motifs à leur base. Le procès-verbal est signé par le président et le secrétaire et communiqué aux membres de l'autorité de contrôle judiciaire.

(7) L'autorité de contrôle judiciaire agit en toute indépendance dans l'exercice de ses missions et des pouvoirs dont elle est investie conformément à la présente loi. Dans l'exercice de leurs missions et de leurs pouvoirs, les membres de l'autorité de contrôle judiciaire demeurent libres de toute influence extérieure, qu'elle soit directe ou indirecte, et ne sollicitent ni n'acceptent d'instructions de quiconque.

(8) Les membres de l'autorité de contrôle judiciaire s'abstiennent de tout acte incompatible avec leurs fonctions et, pendant la durée de leur mandat, n'exercent aucune activité professionnelle incompatible, rémunérée ou non.

(9) Les membres de l'autorité de contrôle judiciaire sont soumis au secret professionnel au sens de l'article 458 du Code pénal concernant toute information confidentielle dont ils ont eu connaissance dans l'exercice de leurs missions ou de leurs pouvoirs, y compris après la cessation de leurs mandats.

(10) L'autorité de contrôle judiciaire adopte un règlement interne afin de déterminer ses procédures et modalités de travail nécessaires non prévues par la présente loi. Ce règlement est publié au Journal officiel du Grand-Duché de Luxembourg.

#### **Art. 42. Missions de l'autorité de contrôle judiciaire**

(1) Dans les limites de ses compétences prévues à l'article 40, paragraphe 2, et lorsque le traitement de données à caractère personnel concerné par les autorités y visées relève du champ d'application de la présente loi, l'autorité de contrôle judiciaire :

- a) contrôle l'application des dispositions de la présente loi et veille au respect de celles-ci ;
- b) favorise la sensibilisation du public et sa compréhension des risques, des règles, des garanties et des droits relatifs au traitement ;
- c) conseille la Chambre des députés, le Gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement ;
- d) encourage la sensibilisation des responsables du traitement et des sous-traitants des traitements de données relevant de sa compétence aux obligations qui leur incombent en vertu de la présente loi ;
- e) fournit, sur demande, à toute personne concernée, des informations sur l'exercice de ses droits découlant de la présente loi et, le cas échéant, coopère à cette fin avec la Commission nationale pour la protection des données et les autorités de contrôle étrangères ;
- f) traite les réclamations introduites par une personne concernée ou par un organisme, une organisation ou une association conformément à l'article 47, 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 ;

- g) vérifie la licéité du traitement en vertu de l'article 16 et informe la personne concernée dans un délai raisonnable de l'issue de la vérification, conformément au paragraphe 3 du même article, ou des motifs ayant empêché sa réalisation ;
- h) coopère avec d'autres autorités de contrôle, y compris en partageant des informations, et leur fournit une assistance mutuelle dans ce cadre en vue d'assurer une application cohérente de la présente loi pour en assurer le respect ;
- i) effectue des enquêtes sur l'application de la présente loi, y compris sur la base d'informations reçues d'une autre autorité de contrôle ou d'une autre autorité publique ;
- j) suit les évolutions pertinentes, dans la mesure où elles ont une incidence sur la protection des données à caractère personnel, notamment dans le domaine des technologies de l'information et de la communication ;
- k) fournit des conseils sur les opérations de traitement visées à l'article 27.

L'autorité de contrôle judiciaire facilite l'introduction des réclamations visées au paragraphe 1<sup>er</sup>, lettre f), par des mesures telles que la fourniture d'un formulaire de réclamation qui peut être rempli également par voie électronique, sans que d'autres moyens de communication ne soient exclus.

L'accomplissement des missions de l'autorité de contrôle judiciaire est gratuit pour la personne concernée et pour les délégués à la protection des données compétents pour les traitements de données relevant du champ d'application de la présente loi.

Lorsqu'une demande est manifestement infondée ou excessive en raison, notamment, de son caractère répétitif, l'autorité de contrôle judiciaire peut exiger le paiement de frais raisonnables basés sur ses coûts administratifs ou refuser de donner suite à la demande. Il incombe à l'autorité de contrôle judiciaire de démontrer le caractère manifestement infondé ou excessif de la demande.

(2) Lorsque le traitement de données à caractère personnel effectué par les autorités visées à l'article 40, paragraphe 2, relève du champ d'application du règlement (UE) n° 2016/679, les missions de l'autorité de contrôle judiciaire sont celles visées à l'article 57 de ce règlement.

#### **Art. 43. Pouvoirs de l'autorité de contrôle judiciaire**

(1) Lorsque le traitement de données à caractère personnel effectué par les autorités visées à l'article 40, paragraphe 2, relève du champ d'application de la présente loi, l'autorité de contrôle judiciaire dispose des pouvoirs correctifs suivants :

- a) avertir un responsable du traitement ou un sous-traitant du fait que les opérations de traitement envisagées sont susceptibles de violer les dispositions de la présente loi ;
- b) ordonner au responsable du traitement ou au sous-traitant de mettre les opérations de traitement en conformité avec les dispositions adoptées en vertu de la présente loi, le cas échéant de manière spécifique et dans un délai déterminé, en particulier en ordonnant la rectification ou l'effacement de données à caractère personnel ou la limitation du traitement en application de l'article 15 ;
- c) limiter temporairement ou définitivement, y compris interdire, un traitement.

L'autorité de contrôle judiciaire obtient du responsable du traitement ou du sous-traitant accès à toutes les données à caractère personnel qui sont traitées et à toutes les autres informations nécessaires à l'exercice de ses missions.

L'autorité de contrôle judiciaire conseille le responsable du traitement conformément à la procédure de consultation préalable visée à l'article 27 et émet, de sa propre initiative ou sur demande, des avis à l'attention de la Chambre des députés et du Gouvernement ou d'autres institutions et organismes, ainsi que du public, sur toute question relative à la protection des données à caractère personnel relevant de sa compétence.

L'autorité de contrôle judiciaire a le pouvoir de porter les violations des dispositions de la présente loi à la connaissance des autorités judiciaires en vue de faire respecter les dispositions de la présente loi.

(2) Lorsque le traitement de données à caractère personnel effectué par les autorités visées à l'article 40, paragraphe 2, relève du champ d'application du règlement (UE) n° 2016/679, les pouvoirs de l'autorité de contrôle judiciaire sont ceux visés à l'article 58 de ce règlement.

## Chapitre 7 - Voies de recours, responsabilité et sanctions

### Art. 44. Droit d'introduire une réclamation auprès d'une autorité de contrôle

(1) Toute personne concernée peut introduire auprès de la Commission nationale pour la protection des données une réclamation contre des opérations de traitement de données à caractère personnel si elle considère que le traitement des données à caractère personnel la concernant constitue une violation des dispositions de la présente loi.

(2) Par dérogation au paragraphe 1<sup>er</sup>, les réclamations contre des opérations de traitement de données à caractère personnel effectuées par les juridictions de l'ordre judiciaire, y compris le ministère public, et de l'ordre administratif dans l'exercice de leurs fonctions juridictionnelles sont traitées comme incident de procédure devant la juridiction qui est compétente pour statuer sur le litige auquel la personne concernée est partie, conformément aux dispositions procédurales applicables au litige concerné.

(3) Pour toutes les réclamations contre des opérations de traitement de données à caractère personnel effectuées par les juridictions de l'ordre judiciaire, y compris le ministère public, et de l'ordre administratif dans l'exercice de leurs fonctions juridictionnelles qui ne peuvent être traitées conformément au paragraphe 2, la personne concernée peut saisir l'autorité de contrôle judiciaire.

(4) Si la réclamation n'est pas introduite auprès de l'autorité de contrôle compétente, l'autorité de contrôle auprès de laquelle la réclamation a été introduite la transmet dans les meilleurs délais à l'autorité de contrôle compétente. La personne concernée est informée de cette transmission.

(5) La personne concernée est informée par l'autorité de contrôle compétente de l'état d'avancement et de l'issue de la réclamation, y compris de la possibilité d'un recours juridictionnel en vertu de l'article 45.

### Art. 45. Droit à un recours juridictionnel contre une décision de l'autorité de contrôle

(1) Contre les décisions prises par l'autorité de contrôle judiciaire en application de l'article 44, paragraphe 3, lorsque le traitement de données à caractère personnel visé par la réclamation relève du champ d'application de la présente loi, un recours juridictionnel peut être introduit par la personne concernée devant la chambre du conseil de la cour d'appel.

La requête y afférente est consignée sur un registre tenu à cet effet au greffe de la chambre du conseil de la cour d'appel. Sous peine d'irrecevabilité, la requête doit être déposée au greffe de la chambre du conseil de la cour d'appel dans le délai d'un mois qui court à partir du jour de la notification de la décision en cause par l'autorité de contrôle judiciaire à la personne concernée, ou, lorsque l'autorité de contrôle judiciaire n'a pas statué sur la réclamation de la personne concernée, à partir de l'expiration d'un délai de trois mois à partir du jour de la saisine de l'autorité de contrôle judiciaire par la personne concernée. Le greffier avertit la personne concernée et le responsable du traitement au moins huit jours avant les jour et heure de l'audience.

Le responsable du traitement ou son représentant et la personne concernée et, le cas échéant, son mandataire ont seul le droit d'assister à l'audience et de fournir tels mémoires et de faire telles réquisitions, verbales ou écrites, qu'ils jugent convenables. L'audience de la chambre du conseil n'est pas publique.

Les notifications et avertissements visés au présent paragraphe se font dans les formes prévues pour les notifications en matière répressive. Ni le délai de recours, ni la saisine de la chambre du conseil de la cour d'appel en application du présent paragraphe n'ont d'effet suspensif.

(2) Contre les décisions prises par la Commission nationale pour la protection des données sur base de l'article 44, paragraphe 1<sup>er</sup>, et contre les décisions prises par l'autorité de contrôle judiciaire sur base de l'article 44, paragraphe 3, lorsque le traitement de données à caractère personnel visé par la réclamation relève du champ d'application du règlement (UE) n° 2016/679, la personne concernée peut introduire un recours devant le tribunal administratif qui statue comme juge du fond.

### Art. 46. Représentation des personnes concernées

(1) Sans préjudice des dispositions légales relatives à la représentation des parties devant les juridictions de l'ordre judiciaire et de l'ordre administratif, la personne concernée a le droit de mandater une personne morale, remplissant les conditions prévues au paragraphe 2, pour qu'elle exerce en son nom les droits visés aux articles 44 et 45.

(2) Afin de pouvoir représenter valablement la personne concernée, et sous peine d'irrecevabilité de la réclamation ou du recours, la personne morale visée au paragraphe 1<sup>er</sup> doit remplir les conditions suivantes :

- a) être valablement constituée en tant qu'association ou fondation conformément aux dispositions de la loi modifiée du 21 avril 1928 sur les associations et les fondations sans but lucratif ;
- b) s'il s'agit d'une association sans but lucratif, avoir été reconnue d'utilité publique conformément à l'article 26-2 de la loi visée à la lettre a) ;
- c) la protection des droits et libertés de la personne concernée dans le cadre de la protection des données à caractère personnel doit figurer aux statuts de l'association ou de la fondation comme l'objet ou l'un des objets en vue desquels l'association ou la fondation a été créée ;
- d) disposer de la personnalité juridique au moment de l'introduction de la réclamation ou de l'action en justice au nom de la personne concernée ;
- e) avoir été mandatée par écrit et préalablement à l'exercice des droits de la personne visés aux articles 44 et 45.

(3) Le mandat délivré en application du présent article ayant comme objet la défense de l'intérêt général est nul.

#### **Art. 47. Sanctions**

(1) La violation des articles 3 à 15, 18 à 30, et 34 à 38 de la présente loi sont passibles d'une amende administrative de 500 à 250 000 euros qui est prononcée, par voie de décision, par l'autorité de contrôle. Un recours contre cette décision est ouvert devant le Tribunal administratif qui statue comme juge du fond.

(2) L'autorité de contrôle compétente peut, par voie de décision, prononcer une astreinte de 100 euros par jour de retard afin de contraindre le responsable du traitement de se conformer aux injonctions soit émises par la Commission nationale pour la protection des données en application de l'article 14, points 1°, 3° et 4° de la loi du 1<sup>er</sup> août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, soit émises par l'autorité de contrôle judiciaire en application de l'article 43, lettres b) et c).

L'astreinte court à compter de la date fixée dans la décision prononçant l'astreinte. Cette date ne peut être antérieure à la date de la notification de la décision. Un recours contre cette décision est ouvert devant le Tribunal administratif qui statue comme juge du fond.

(3) Par ailleurs, la violation des articles 9, 10 et 29 de la présente loi avec une intention frauduleuse ou à dessein de nuire est punie d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125 000 euros ou d'une de ces peines seulement. La juridiction saisie prononce la cessation du traitement contraire aux dispositions des articles précités sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

(4) La Commission nationale pour la protection des données et le procureur d'État coopèrent pour la répression administrative ou pénale des violations ou des infractions aux dispositions de la présente loi et à celles de la loi du 1<sup>er</sup> août 2018 portant organisation de la Commission nationale pour la protection des données et au régime général sur la protection des données. À cette fin, la Commission nationale pour la protection des données, le procureur d'État et la Police grand-ducale peuvent échanger toute information qu'ils jugent utile ou nécessaire.

(5) Si des indices peuvent justifier l'ouverture par la Commission nationale pour la protection des données d'une procédure administrative susceptible d'aboutir à l'imposition d'une sanction administrative pour un ou plusieurs faits constituant une violation du paragraphe 8 ou des articles 48 et 49 de la loi du 1<sup>er</sup> août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, elle en informe le procureur d'État qui décide, endéans les deux mois de la réception de cette information, s'il exerce l'action publique. Dans ce cas, il en informe la Commission nationale pour la protection des données.

Si le procureur d'État décide de poursuivre, la Commission nationale pour la protection des données ne procède pas. En cas de décision négative ou en l'absence d'une réponse du procureur d'État après le délai de deux mois, la Commission nationale pour la protection des données procède conformément à la loi du 1<sup>er</sup> août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données.

Lorsqu'au cours de la procédure la Commission nationale pour la protection des données constate l'existence d'indices que les personnes suspectées sont susceptibles d'avoir contrevenu aux dispositions du paragraphe 8 ou des articles 48 et 49 de la loi du 1<sup>er</sup> août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, elle se dessaisit du dossier et le transmet au procureur d'État qui procède conformément au Code de procédure pénale.

Si le procureur d'État estime au cours de son enquête et avant qu'il ne cite à comparaître que les conditions d'une poursuite pénale ne sont pas remplies mais que des sanctions administratives sont susceptibles de s'appliquer, il transmet le dossier à la Commission nationale pour la protection des données qui procède conformément à la loi du 1<sup>er</sup> août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données.

(6) Lorsque le procureur d'État est saisi sur base d'une plainte de faits susceptibles de constituer une infraction au paragraphe 8 ou aux articles 48 et 49 de la loi du 1<sup>er</sup> août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données et qu'il décide d'exercer l'action publique, il en informe la Commission nationale pour la protection des données. Dans ce cas, la Commission nationale pour la protection des données ne procède pas. Si le procureur d'État décide de ne pas poursuivre, la Commission nationale pour la protection des données procède conformément à la loi du 1<sup>er</sup> août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données.

Si le procureur d'État estime au cours de son enquête et avant qu'il ne cite à comparaître que les conditions d'une poursuite pénale ne sont pas remplies mais que des sanctions administratives sont susceptibles de s'appliquer, il transmet le dossier à la Commission nationale pour la protection des données qui procède conformément à la loi du 1<sup>er</sup> août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données.

(7) Les dispositions des paragraphes 4 à 6 s'appliquent également à l'autorité de contrôle judiciaire lorsqu'elle exerce les missions et dispose des pouvoirs prévus par le règlement (UE) n° 2016/679.

(8) Quiconque empêche ou entrave sciemment, de quelque manière que ce soit, l'accomplissement des missions incombant à l'autorité de contrôle judiciaire est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125 000 euros ou d'une de ces peines seulement.

(9) Les dispositions des articles 51 à 53 de la loi du 1<sup>er</sup> août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données sont applicables à l'autorité de contrôle judiciaire lorsqu'elle agit dans la cadre de ses compétences relatives au règlement (UE) n° 2016/679 ou prévues par la présente loi. Le recouvrement des amendes ou astreintes qu'elle prononce est confié à l'Administration de l'enregistrement et des domaines. Il se fait comme en matière d'enregistrement.

## **Chapitre 8 - Dispositions finales**

### *Section 1<sup>ère</sup> - Dispositions modificatives*

#### **Art. 48. Loi modifiée du 7 mars 1980 sur l'organisation judiciaire**

L'article 75-8 de la loi modifiée du 7 mars 1980 sur l'organisation judiciaire est remplacé comme suit :

« Art. 75-8.

Le droit de toute personne d'avoir accès aux données à caractère personnel la concernant qui sont traitées par Eurojust, tel que prévu par l'article 19 de la décision précitée du Conseil du 28 février 2002 se fait suivant les modalités du droit d'accès au Luxembourg telles qu'elles sont prévues par les articles 13, 14 et 16 de la loi du 1<sup>er</sup> août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale.

»

**Art. 49. Loi modifiée du 29 mai 1998 portant approbation de la Convention sur la base de l'article K.3 du Traité sur l'Union européenne portant création d'un Office européen de police (Convention Europol), signée à Bruxelles, le 26 juillet 1995**

L'article 3 de la loi modifiée du 29 mai 1998 portant approbation de la Convention sur la base de l'article K.3 du Traité sur l'Union européenne portant création d'un Office européen de police (Convention Europol), signée à Bruxelles, le 26 juillet 1995 est remplacé comme suit :

« Art. 3.

L'autorité de contrôle prévue à l'article 2, paragraphe 1<sup>er</sup>, point 15) a), de la loi du 1<sup>er</sup> août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale est désignée comme l'autorité de contrôle nationale prévue à l'article 23 de la Convention avec mission de contrôler le respect des dispositions en matière de protection des données à caractère personnel dans le cadre de l'exploitation du système d'information Europol.

»

**Art. 50. Loi du 20 décembre 2002 portant approbation - de la Convention établie sur base de l'article K.3 du Traité sur l'Union européenne, sur l'emploi de l'informatique dans le domaine des douanes, signé à Bruxelles, le 26 juillet 1995; - de l'Accord relatif à l'application provisoire entre certains États membres de l'Union européenne de la Convention établie sur base de l'article K.3 du Traité sur l'Union européenne, sur l'emploi de l'informatique dans le domaine des douanes, signé à Bruxelles, le 26 juillet 1995**

L'article 2 de la loi du 20 décembre 2002 portant approbation - de la Convention établie sur base de l'article K.3 du Traité sur l'Union européenne, sur l'emploi de l'informatique dans le domaine des douanes, signé à Bruxelles, le 26 juillet 1995; - de l'Accord relatif à l'application provisoire entre certains États membres de l'Union européenne de la Convention établie sur base de l'article K.3 du Traité sur l'Union européenne, sur l'emploi de l'informatique dans le domaine des douanes, signé à Bruxelles, le 26 juillet 1995 est remplacé comme suit :

« Art. 2.

L'autorité de contrôle prévue à l'article 2, paragraphe 1<sup>er</sup>, point 15) a), de la loi du 1<sup>er</sup> août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale est désignée comme l'autorité de contrôle nationale prévue à l'article 17 de la Convention, avec mission de contrôler le respect des dispositions en matière de protection des données à caractère personnel dans le cadre de l'exploitation du système d'information des douanes.

»

**Art. 51. Loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité**

À l'article 23 de la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité, l'alinéa 1<sup>er</sup> est remplacé comme suit :

« Le traitement, par l'Autorité nationale de Sécurité, des informations collectées dans le cadre de ses missions est mis en œuvre conformément aux dispositions de la loi du 1<sup>er</sup> août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale.

»



**Art. 52. Loi modifiée du 16 juin 2004 portant réorganisation du centre socio-éducatif de l'État**

La loi modifiée du 16 juin 2004 portant réorganisation du centre socio-éducatif de l'État est modifiée comme suit :

1° À l'article 11*bis*, paragraphe 4, alinéa 2, la première phrase est remplacée comme suit :

« Le procureur général d'État est considéré, en ce qui concerne le traitement des données à caractère personnel, comme responsable du traitement au sens de l'article 4, point 7), du règlement (UE) n° 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), ci-après désigné comme le « règlement (UE) n° 2016/279 ». »

2° À l'article 11*bis*, paragraphe 4, alinéa 3, la première phrase est remplacée comme suit :

« Le directeur du centre est considéré, en ce qui concerne le traitement des données à caractère personnel dans le cadre de l'hébergement et de l'encadrement du pensionnaire, comme responsable du traitement au sens de l'article 4, point 7), du règlement (UE) n° 2016/679. »

**Art. 53. Loi modifiée du 25 août 2006 relative aux procédures d'identification par empreintes génétiques en matière pénale et portant modification du Code d'instruction criminelle**

La loi modifiée du 25 août 2006 relative aux procédures d'identification par empreintes génétiques en matière pénale et portant modification du Code d'instruction criminelle est modifiée comme suit :

1° À l'article 1<sup>er</sup>, la deuxième phrase est remplacée comme suit :

« Le traitement de ces données est soumis aux prescriptions de l'article 9 de la loi du 1<sup>er</sup> août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale. »

2° À l'article 13, le paragraphe 2 est remplacé comme suit :

« (2) Un profil d'ADN établi est à considérer comme donnée à caractère personnel, au sens de la loi du 1<sup>er</sup> août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, à partir du moment où le code alphanumérique de l'analyse d'ADN a été associé à une information relative à la personne physique en cause permettant de l'identifier. »

**Art. 54. Loi du 24 juin 2008 ayant pour objet le contrôle des voyageurs dans les établissements d'hébergement**

À l'article 3 de la loi du 24 juin 2008 ayant pour objet le contrôle des voyageurs dans les établissements d'hébergement, la première phrase est remplacée comme suit :

« Le logeur est obligé de communiquer à la Police grand-ducale la fiche d'hébergement concernant les personnes hébergées aux fins de la prévention et de la 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. »

**Art. 55. Loi modifiée du 29 mars 2013 relative à l'organisation du casier judiciaire**

À l'article 8 de la loi modifiée du 29 mars 2013 relative à l'organisation du casier judiciaire, la deuxième phrase du point 2 est remplacée comme suit :

« Le SRE transmet sur une base trimestrielle la liste de ses demandes de délivrance et les motifs de ces demandes à l'autorité de contrôle judiciaire prévue à l'article 40 de la loi du 1<sup>er</sup> août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale ; »

**Art. 56. Loi modifiée du 19 décembre 2014 facilitant l'échange transfrontalier d'informations concernant les infractions en matière de sécurité routière**

L'article 6 de la loi modifiée du 19 décembre 2014 facilitant l'échange transfrontalier d'informations concernant les infractions en matière de sécurité routière est remplacé comme suit :

« Art. 6.

(1) Le traitement des données à caractère personnel dans le cadre de la présente loi est effectué à des fins de prévention, de recherche et de constatation des infractions pénales ou administratives relevant de son champ d'application et se fait conformément aux articles 24 à 32 de la décision 2008/615/JAI précitée et aux dispositions, y non contraires, de la loi du 1<sup>er</sup> août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale.

(2) Toute personne concernée a le droit d'obtenir des informations sur les données à caractère personnel transmises dans le cadre de la présente loi, y compris la date de la demande et l'autorité compétente de l'État membre de l'infraction, conformément aux articles 11 à 17 de la loi du 1<sup>er</sup> août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale.

»

**Art. 57. Loi modifiée du 25 juillet 2015 portant création du système de contrôle et de sanction automatisés**

L'article 10 de la loi modifiée du 25 juillet 2015 portant création du système de contrôle et de sanction automatisés est remplacé comme suit :

« Art. 10.

Le Centre procède au traitement des données à caractère personnel qui est nécessaire à l'accomplissement de ses missions qui est effectué conformément aux dispositions de la loi du 1<sup>er</sup> août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale.

»

**Art. 58. Loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État**

La loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État est modifiée comme suit :

1° À l'article 9, paragraphe 4, la dernière phrase est remplacée comme suit :

« Sous réserve des conditions définies à l'alinéa 1<sup>er</sup>, le SRE peut échanger directement des données à caractère personnel avec des services de renseignement étrangers, y compris au moyen d'installations communes de transmission, conformément aux articles 34 et 38 de la loi du 1<sup>er</sup> août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale. »

2° À l'article 10, le paragraphe 1<sup>er</sup> est remplacé comme suit :

« (1) Le SRE procède au traitement de données à caractère personnel qui sont nécessaires à l'accomplissement de ses missions légales qui est effectué conformément aux dispositions de la loi du 1<sup>er</sup> août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale. »

3° À l'article 10, paragraphe 2, l'alinéa 3 est remplacé comme suit :

« Le SRE transmet sur une base trimestrielle la liste de ses demandes de délivrance et les motifs de ces demandes à l'autorité de contrôle judiciaire prévue à l'article 40 de la loi du 1<sup>er</sup> août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale. »

4° À l'article 10, paragraphe 3, l'alinéa 1<sup>er</sup> est remplacé comme suit :

« Le directeur est responsable du traitement des données visées aux paragraphes 1<sup>er</sup> et 2. Il désigne un chargé de la protection des données qui est compétent sous son autorité de l'application conforme de la loi du 1<sup>er</sup> août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale et de la mise en œuvre des mesures de sécurité des traitements auxquels procède le SRE. »

**Art. 59. Loi du 23 juillet 2016 portant mise en place d'un statut spécifique pour certaines données à caractère personnel traitées par le Service de renseignement de l'État**

La loi du 23 juillet 2016 portant mise en place d'un statut spécifique pour certaines données à caractère personnel traitées par le Service de renseignement de l'État est modifiée comme suit :

1° À l'article 3, le paragraphe 11 est remplacé comme suit :

« (11) Pendant l'exercice de la mission des experts, le directeur du Service de renseignement de l'État est le responsable du traitement des données au sens de l'article 2, point 8), de la loi du 1<sup>er</sup> août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, et les Archives nationales sont considérées comme sous-traitant du Service de renseignement de l'État au sens de l'article 2, point 9), de la même loi. »

2° À l'article 3, paragraphe 15, la première est remplacée comme suit :

« Le rapport final ne peut contenir aucune donnée à caractère personnel ni aucun élément susceptible permettant l'identification d'une personne sauf consentement exprès de la personne concernée, conformément à l'article 6, paragraphe 1, lettre a), du règlement (UE) n° 2016/679. »

3° À l'article 4, paragraphe 2, le point 1 est remplacé comme suit :

« 1. les banques de données historiques recensées au sens de l'article 3, paragraphe 6, point 2, sont versées définitivement aux Archives nationales tel que prévu à l'article 7 de la loi modifiée du 25 juin 2004 portant réorganisation des instituts culturels de l'État et sous réserve des dispositions du règlement (UE) n° 2016/679. Les Archives nationales deviennent responsables de traitement de ces données à partir de la date de versement définitif ; »

4° À l'article 5, les paragraphes 1 et 2 sont remplacés comme suit :

« (1) L'accès d'une personne concernée à des données la concernant pendant l'exercice de la mission des experts s'effectue conformément aux dispositions des articles 13, 14 et 16 de la loi du 1<sup>er</sup> août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale.  
(2) Des données à caractère personnel, constatées au cours de la mission des experts et couvrant des personnes qui ont déjà introduit une demande d'accès, sont communiquées à la personne concernée conformément aux dispositions visées au paragraphe 1<sup>er</sup>. »

5° À l'article 5, le paragraphe 5 est remplacé comme suit :

« (5) Dans l'exercice de leur mission, les experts disposent d'un accès intégral aux banques de données historiques du Service de renseignement de l'État ainsi qu'un accès aux données à caractère personnel et traitent ces données conformément au principe de légitimité au sens de l'article 5, paragraphe 1<sup>er</sup>, lettre b), du règlement (UE) n° 2016/679. »

**Art. 60. Loi du 22 février 2018 relative à l'échange de données à caractère personnel et d'informations en matière policière**

La loi du 22 février 2018 relative à l'échange de données à caractère personnel et d'informations en matière policière est modifiée comme suit :

1° À l'article 1<sup>er</sup>, point 3), les mots « des articles 18 et 19 de la loi modifiée du 2 août 2002 relative à la protection des données à l'égard du traitement des données à caractère personnel » sont remplacés par les mots « du chapitre V de la loi du 1<sup>er</sup> août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale ».

2° À l'article 25, le paragraphe 2 est remplacé comme suit :

« (2) La transmission des données et informations se fait dans une forme permettant à la Commission nationale pour la protection des données de vérifier si toutes les conditions requises par la loi étaient remplies au moment de la transmission. La documentation de la transmission est conservée pendant une durée de deux ans. »

3° À l'article 26, le paragraphe 1<sup>er</sup> est remplacé comme suit :

« (1) Les données et informations transmises à l'administration de l'État concernée font partie du traitement des données à caractère personnel dont l'administration ou son représentant est le responsable du traitement au sens de l'article 4, point 7), du règlement (UE) n° 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données). La Commission nationale pour la protection des données est compétente pour vérifier l'application des dispositions du règlement précité et de la loi du 1<sup>er</sup> août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale. »

4° L'article 28 est remplacé comme suit :

« La Commission nationale pour la protection des données contrôle et surveille le respect des conditions d'accès prévues par la présente loi. Le rapport à transmettre au ministre ayant la Protection des données dans ses attributions, en exécution de l'article 10 de la loi du 1<sup>er</sup> août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, contient une partie spécifique ayant trait à l'exécution de sa mission de contrôle exercée au titre de la présente loi. »

**Art. 61. Loi du 18 juillet 2018 sur la Police grand-ducale**

À l'article 43 de la loi du 18 juillet 2018 sur la Police grand-ducale, l'alinéa 6 est remplacé comme suit :

« L'autorité de contrôle prévue à l'article 2, paragraphe 1<sup>er</sup>, point 15), lettre a), de la loi du 1<sup>er</sup> août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale contrôle et surveille le respect des conditions d'accès prévues par le présent article. Le rapport à transmettre au ministre ayant la Protection des données dans ses attributions, en exécution de l'article 10 de la loi du 1<sup>er</sup> août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, contient une partie spécifique ayant trait à l'exécution de sa mission de contrôle exercée au titre du présent article. »

**Art. 62. Loi du 18 juillet 2018 sur l'Inspection générale de la Police**

L'article 15 de la loi du 18 juillet 2018 sur l'Inspection générale de la Police est modifié comme suit :

1° Le paragraphe 3 est remplacé comme suit :

« (3) Dans le cadre des missions énoncées aux articles 4, 7 et 9, l'IGP a accès aux données retraçant les accès aux traitements des données à caractère personnel dont le responsable du traitement est le directeur général de la Police. »

2° Le paragraphe 6 est remplacé comme suit :

« (6) L'autorité de contrôle prévue à l'article 2, paragraphe 1<sup>er</sup>, point 15), lettre a), de la loi du 1<sup>er</sup> août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale contrôle et surveille le respect des conditions d'accès prévues par le présent article. Le rapport à transmettre au ministre ayant la Protection des données dans ses attributions, en exécution de l'article 10 de la loi du 1<sup>er</sup> août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, contient une partie spécifique ayant trait à l'exécution de sa mission de contrôle exercée au titre du présent article. »

*Section 2 - Dispositions transitoires, mise en conformité et intitulé de citation*

**Art. 63. Dispositions transitoires et mise en conformité**

(1) À titre exceptionnel et lorsque cela exige des efforts disproportionnés, les systèmes de traitements de données à caractère personnel automatisés installés avant le 6 mai 2016 sont mis en conformité avec l'article 24 au plus tard le 6 mai 2023.

(2) Par dérogation au paragraphe 1<sup>er</sup>, et dans des circonstances exceptionnelles, un système donné de traitement de données à caractère personnel automatisé visé au paragraphe 1<sup>er</sup> peut être mis en conformité avec l'article 24 jusqu'à une date butoir à déterminer par une décision du Gouvernement en conseil et située après le 6 mai 2023 lorsque, à défaut de cela, de graves difficultés se posent pour le fonctionnement du système de traitement automatisé en question. La date butoir ne peut être fixée au-delà du 6 mai 2026.

**Art. 64. Intitulé de citation**

La référence à la présente loi se fait sous la forme suivante : « Loi du 1<sup>er</sup> août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale. »

Mandons et ordonnons que la présente loi soit insérée au Journal officiel du Grand-Duché de Luxembourg pour être exécutée et observée par tous ceux que la chose concerne.

*Le Ministre de la Justice,*  
**Félix Braz**

Cabasson, le 1<sup>er</sup> août 2018.  
**Henri**

---

Doc. parl. 7168, sess. ord. 2016-2017 et 2017-2018 ; Dir. (UE) 2016/680.

---

