JOURNAL OFFICIEL

DU GRAND-DUCHÉ DE LUXEMBOURG

MÉMORIAL A

N° 565 du 14 juin 2017

Règlement grand-ducal du 31 mai 2017 modifiant le règlement grand-ducal du 8 janvier 2015 relatif à la protection des mineurs dans les services des médias audiovisuels.

Nous Henri, Grand-Duc de Luxembourg, Duc de Nassau,

Vu la loi modifiée du 27 juillet 1991 sur les médias électroniques et notamment ses articles *27ter* et 28*quater*;

Vu la directive 2010/13/UE du Parlement européen et du Conseil du 10 mars 2010 visant à la coordination de certaines dispositions législatives, réglementaires et administratives des Etats membres relatives à la fourniture de services de médias audiovisuels;

Vu l'avis de la Chambre de commerce;

Notre Conseil d'Etat entendu;

Sur le rapport de Notre Ministre des Communications et des Médias et après délibération du Gouvernement en conseil;

Arrêtons :

Art. 1er.

A l'article 8, paragraphe 1er du règlement grand-ducal du 8 janvier 2015 relatif à la protection des mineurs dans les services des médias audiovisuels, le mot « équivalent » est supprimé.

Art. 2.

A l'article 9, paragraphe 1er du même règlement, le mot « équivalent » est supprimé.

Art. 3.

Notre Ministre des Communications et des Médias est chargé de l'exécution du présent règlement qui sera publié au Journal officiel du Grand-Duché de Luxembourg.

Le Ministre des Communications et des Médias,
Xavier Bettel

Cabasson, le 31 mai 2017.
Henri

JOURNAL OFFICIEL

DU GRAND-DUCHÉ DE LUXEMBOURG

MÉMORIAL A

N° 564 du 14 juin 2017

Avis de publication conformément à l'article 40 de la loi modifée du 15 décembre 2010 relative à la sécurité des jouets.

Il est porté à la connaissance de tous les intéressés ce qui suit:

L'annexe II, appendice C, de la directive 2009/48/CE du Parlement européen et du Conseil du 18 juin 2009 relative à la sécurité des jouets, déclarée obligatoire par la loi modifiéedu 15 décembre 2010 relative à la sécurité des jouets, est modifiée conformément à la directive (UE) 2017/898 de la Commission du 24 mai 2017 modifiant, aux fins de l'adoption de valeurs limites spécifiques pour les substances chimiques utilisées dans les jouets, l'annexe II, appendice C, de la directive 2009/48/CE du Parlement européen et du Conseil relative à la sécurité des jouets en ce qui concerne le bisphénol A, publiée au Journal officiel de l'Union européenne (JO L138 du 25.5.2017).

Luxembourg, le 12 juin 2017.

Pour le Ministre de l'Économie,
La Secrétaire d'État,
Francine Closener

JOURNAL OFFICIEL

DU GRAND-DUCHÉ DE LUXEMBOURG

MÉMORIAL A

N° 563 du 14 juin 2017

Règlement grand-ducal du 22 mai 2017 modifiant le règlement grand-ducal du 25 juillet 2015 portant exécution de l'article 4, paragraphe 1er, de la loi du 25 juillet 2015 relative à l'archivage électronique.

Nous Henri, Grand-Duc de Luxembourg, Duc de Nassau,

Vu la loi du 25 juillet 2015 relative à l'archivage électronique et notamment son article 4, paragraphe 1er;

Vu les avis de la Chambre de commerce et de la Chambre des métiers;

Notre Conseil d'État entendu;

Sur le rapport de Notre Ministre de l'Économie et après délibération du Gouvernement en conseil;

Arrêtons:

Art. 1er.

L'annexe du règlement grand-ducal du 25 juillet 2015 portant exécution de l'article 4, paragraphe 1er, de la loi du 25 juillet 2015 relative à l'archivage électronique est remplacée par l'annexe jointe au présent règlement grand-ducal.

Art. 2.

Notre Ministre de l'Économie est chargé de l'exécution du présent règlement qui sera publié au Journal officiel du Grand-Duché de Luxembourg.

Le Ministre de l'Économie,
Étienne Schneider

Palais de Luxembourg, le 22 mai 2017.
Henri

ANNEXE

Règle technique pour un système de management et mesures de sécurité pour les Prestataires de Services de Dématérialisation ou de Conservation.

Table des matières

0 Introduction

0.1 Contexte

La présente règle technique (ci-après « la Règle technique ») définit des exigences et des mesures permettant à une organisation d'établir une gestion de la sécurité de l'information et une gestion opérationnelle spécifiques aux processus de dématérialisation ou de conservation.

Du point de vue de la gestion de la sécurité de l'information, la Règle technique se base sur les Normes internationales ISO/IEC 27001:2013 et ISO/IEC 27002:2013 de manière à ce qu'une organisation puisse être en mesure de définir, d'implémenter, de maintenir et d'améliorer :

a) un Système de Management de la Sécurité de l'Information (ci-après « SMSI ») basé sur la Norme internationale ISO/IEC 27001:2013 et intégrant les processus de dématérialisation ou de conservation,
b) des objectifs et des mesures de la sécurité de l'information basés sur la Norme internationale ISO/IEC 27002:2013 et spécifiques aux processus de dématérialisation ou de conservation.

La Règle technique a été rédigée selon des exigences de la norme ISO/IEC 27009:2016.

La Règle technique est aussi utilisée pour les audits d'évaluation de la conformité d'une organisation exécutant des processus de dématérialisation ou de conservation.

Ces audits d'évaluation ne doivent pas uniquement porter sur les exigences et les mesures de sécurité, mais aussi sur les préconisations de mise en œuvre. Toute déviation par rapport à ces préconisations, qui n'est pas dûment argumentée, documentée ou évidente, peut donner lieu à une non-conformité mineure. Toute déviation par rapport aux mesures, sauf si l'exclusion de la mesure est dûment justifiée par le processus de traitement des risques ainsi que toute déviation par rapport aux exigences, doit donner lieu à une non-conformité mineure ou majeure telle que définie dans ISO/IEC 17021-1:2015.

L'Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (ci-après ILNAS) est la seule autorité nationale luxembourgeoise habilitée à conférer à une organisation un statut de prestataire de services de dématérialisation ou de conservation (ci-après statut de PSDC), si cette organisation a été certifiée conforme à la Règle technique par un organisme de certification accrédité pour cette activité selon les exigences de la Norme internationale ISO/IEC 17021-1:2015, « Évaluation de la conformité - Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management » ainsi que les exigences complémentaires de la Norme ISO/IEC 27006:2015 « Requirements for bodies providing audit and certification of information security management systems ». Ces normes définissent les exigences pour réaliser des certifications à reconnaissance internationale de systèmes de management selon la norme ISO/IEC 27001:2013 et la Règle technique.

La Règle technique ne se substitue pas aux règlements, lois, ou normes applicables aux organisations exécutant des processus de dématérialisation ou de conservation. En particulier, le règlement (UE) n °910/2014 du Parlement Européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (aussi appelé règlement « eIDAS ») doit être considéré comme une fondation pour l'établissement des propriétés de sécurité qui y sont exposées, notamment en matière de confidentialité, d'intégrité, de disponibilité, d'authenticité, de fiabilité et d'exploitabilité.

0.2 Structure du document

Ce document est structuré de la façon suivante :

- Le chapitre 1 précise le domaine d'application de la Règle technique.
- Le chapitre 2 cite des références normatives, c'est-à-dire les normes à respecter par les organisations mettant en application la Règle technique.
- Le chapitre 3 définit les termes utilisés dans ce texte.

- Le chapitre 4 cite des exigences spécifiques pour le système de management des prestataires de service de dématérialisation ou de conservation. Ce chapitre est à lire comme un complément à la norme ISO/IEC 27001:2013 « Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences », d'où la numérotation non linéaire des exigences : un complément à une section existante de la norme initiale garde le même numéro, les sections non modifiées ne sont pas incluses dans le présent document, et les nouvelles sections prennent des numéros qui ne sont pas utilisés dans la norme ISO/IEC 27001:2013.
- Le chapitre 5 définit des guidances spécifiques, en particulier des objectifs, des mesures de sécurité, des préconisations de mise en œuvre et des informations complémentaires. Ce chapitre est à lire comme un complément à la norme ISO/IEC 27002:2013 « Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information », d'où la numérotation non linéaire des exigences.
- L'Annexe A résume les objectifs spécifiques et les mesures de sécurité spécifiques énoncés au Chapitre 5 tout en rendant leur examen obligatoire dans le traitement des risques.

Les transitions requises par ISO/IEC 27009:2016 sont indiquées en *italique*.

1 Domaine d'application

La loi du 25 juillet 2015 relative à l'archivage électronique dispose qu'une personne peut, si elle détient une certification selon les exigences et les mesures définies dans la Règle technique d'exigences et de mesures pour la certification des Prestataires de Services de Dématérialisation ou de Conservation (ci-après PSDC), en regard de l'exécution de ses processus de dématérialisation ou de conservation, procéder à une notification auprès de l'ILNAS, en vue d'obtenir le statut de PSDC.

Si les critères de vérification établis par la loi relative à l'archivage électronique et par le système de qualité ad hoc du Département de la confiance numérique de l'ILNAS sont validés, l'ILNAS procèdera à l'inscription de la personne concernée dans la liste des PSDC, précisant les processus relatifs à la certification, établissant ainsi le statut de PSDC. Tout événement ou incident significatif détecté et tout changement majeur relatif à la portée de la certification, doit obligatoirement être notifié à l'ILNAS. Tout retrait, suspension ou non-renouvellement de la certification entraîne de facto le retrait du statut de PSDC.

Le statut de PSDC demeure volontaire, sauf disposition réglementaire ou sectorielle l'imposant.

La certification effective selon la Règle technique d'exigences et de mesures pour la certification des PSDC de toute personne permet la demande du statut de prestataire de services de dématérialisation ou de conservation délivré par le Département de la confiance numérique de l'ILNAS. L'ILNAS reconnaît formellement, via ce statut, la personne concernée en tant que PSDC.

La personne certifiée doit être en mesure de garantir les résultats de l'exécution des processus de dématérialisation ou de conservation pour lesquels elle a obtenu la certification. La certification garantit que les documents numériques résultants de la numérisation des documents analogiques et les archives numériques seront reconnus comme conformes aux exigences spécifiques liées à l'activité de dématérialisation respectivement de conservation, telles qu'établies dans ce document.

Ainsi une copie sera présumée être conforme à l'original si elle est produite par le processus ad hoc d'un PSDC. De même, une archive numérique est considérée comme équivalente aux originaux numériques, si elle est conservée par le processus ad hoc d'un PSDC.

Indépendamment de son type, de sa taille, de ses processus ou de ses activités, pour ses besoins internes ou dans le cadre de services proposés à ses clients, la Règle technique d'exigences et de mesures des PSDC est applicable à toute organisation publique ou privée.

La Règle technique a été définie à partir de Normes internationales publiées et maintenues par l'Organisation Internationale de Normalisation (ci-après « ISO »).

La Règle technique doit donc être considérée comme un supplément à ces normes[1] en amendant et complétant leur contenu spécifiquement aux processus de dématérialisation ou de conservation.

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application de la Règle technique.

Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

ISO/IEC 27000:2016, Technologies de l'information – Techniques de sécurité – Systèmes de gestion de la sécurité de l'information – Vue d'ensemble et vocabulaire

ISO/IEC 27001:2013, Technologies de l'information – Techniques de sécurité – Systèmes de gestion de la sécurité de l'information -- Exigences

ISO/IEC 27002:2013, Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour la gestion de la sécurité de l'information

3 Termes et définitions

Pour les besoins de la Règle technique, les abréviations suivantes s'appliquent :

DdA	Déclaration d'Applicabilité (terme anglais : Statement of Applicability (SoA), déclaration relative à l'applicabilité des objectifs et mesures de sécurité)
eIDAS	Règlement (UE) No 910/2014 du Parlement Européen de du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE
L2TP	Layer 2 Tunneling Protocol (terme anglais)
IPSec	Internet Protocol Security (terme anglais)
PPP	Point to Point Protocol (terme anglais)
PSDC	Prestataire de Services de Dématérialisation ou de Conservation
SDC	Système de Dématérialisation ou de Conservation
SFTP	SSH File Transfer Protocol (terme anglais)
SMSI	Système de Management de la Sécurité de l'Information
SSH	Secure SHell (terme anglais)
TLS	Transport Layer Security (terme anglais)
UTC	Temps Univers

Pour les besoins de la Règle technique, les termes et définitions fournis dans la norme ISO/IEC 27000:2016 ainsi que les définitions supplémentaires suivantes s'appliquent.

3.1 actif

tout élément représentant de la valeur pour l'organisation

Note 1 : Il existe plusieurs sortes d'actifs, dont :

a) l'information,
b) les documents,
c) les archives,
d) les actifs techniques, par exemple un scanneur, un serveur ou des disques durs,
e) les actifs techniques immatériels, par exemple des unités de stockage virtuelles,
f) le personnel d'une organisation,
g) les actifs incorporels, par exemple la réputation et l'image,
h) les processus et services.

Note 2 : Définition adaptée de la norme ISO/IEC 30300:2011, définition 3.1.2.

3.2 analogique

non numérique

Note : Un support de stockage analogique est un support de stockage non numérique, par exemple le papier, le film argentique ou le disque vinyle.

3.3 archive

document conservé en l'état en vue d'une utilisation pérenne

Note : Définition adaptée de la norme ISO/IEC 30300:2011, définition 3.1.1.

3.4 archive numérique

archive sous forme de document numérique

3.5 authenticité

propriété selon laquelle une entité est ce qu'elle revendique être

[ISO/IEC 27000:2016]

3.6 confidentialité

propriété selon laquelle l'information n'est pas diffusée ni divulguée à des personnes, des entités ou des processus non autorisés

[ISO/IEC 27000:2016]

3.7 conservation (électronique)

l'activité qui consiste à conserver un original numérique ou une copie à valeur probante dans des conditions qui assurent des garanties fiables quant au maintien de l'intégrité du document conservé

[loi du 25 juillet 2015, art. 2 b]

Note : Dans la suite du document, le terme « conservation » est synonyme de « conservation électronique », sauf précision contraire

3.8 dématérialisation

l'activité qui consiste à créer une copie à valeur probante d'un original existant sous forme analogique dans des conditions qui assurent des garanties fiables quant à la conformité de la copie ainsi créée à l'original

[loi du 25 juillet 2015, art. 2 d]

3.9 disponibilité

propriété d'être accessible et utilisable à la demande par une entité autorisée

[ISO/IEC 27000:2016]

3.10 document

information ou objet documentaire enregistré qui peut être traité comme une unité

[ISO 15489 -1:2001]

3.11 fiabilité

propriété relative à un comportement et des résultats prévus et cohérents

[ISO/IEC 27000:2016]

3.12 gestion

définition, mise en œuvre ou en exploitation, opération, contrôle, révision, maintenance et amélioration

Note : De même, gérer est synonyme de « définir, mettre en œuvre ou en exploitation, opérer, contrôler, réviser, maintenir et améliorer ».

3.13 indexation

définition de points d'accès pour faciliter la recherche des documents

Note 1 : La génération de métadonnées liées aux documents numériques et aux archives numériques est généralement utilisée pour faciliter leur recherche.

Note 2 : Définition adaptée de la norme ISO 15489 -1:2001, définition 3.11.

3.14 intégrité

propriété d'exactitude et de complétude

[ISO/IEC 27000:2016]

3.15 métadonnées

données décrivant le contexte, le contenu ou la structure des documents ainsi que leur gestion dans le temps

Note : Définition adaptée de la norme ISO/IEC 30300:2011, définition 3.1.6.

3.16 non-répudiation

capacité à prouver l'occurrence d'un événement ou d'une action donnée(e) et des entités qui en sont à l'origine

[ISO/IEC 27000:2016]

3.17 organisme

personne ou groupe de personnes qui exerce ses propres fonctions associées aux responsabilités, pouvoirs et relations nécessaires pour atteindre ses objectifs

Note 1 : Le concept d'organisme inclut, sans s'y limiter, les travailleurs indépendants, compagnies, sociétés, firmes, entreprises, autorités, partenariats, œuvres de bienfaisance ou institutions, ou toute partie ou combinaison de ceux-ci, constituée en société de capitaux ou ayant un autre statut, de droit privé ou public.

[ISO/IEC 27000:2016]

Note 2 : Le terme organisme désigne le prestataire qui est ou qui veut être prestataire de service de dématérialisation ou de conservation.

3.18 prestataire de services de dématérialisation ou de conservation (PSDC)

toute personne qui exerce à titre principal ou accessoire, pour ses propres besoins ou pour compte d'autrui, des activités de dématérialisation ou de conservation électronique et qui est, dans les conditions et selon les modalités de la [loi 25 juillet 2015], certifiée à cette fin et inscrite sur la liste visée à l'article 4 (3) [de cette loi]

[loi du 25 juillet 2015, art. 2h]

Note : Les prestataires ne sont concernés que par les processus qu'ils gèrent. Dans tout ce document, le « ou » peut être inclusif ou exclusif selon le contexte opérationnel du prestataire.

3.19 preuve

document démontrant l'effectivité d'une opération

Note 1 : La preuve d'une opération signifie qu'il peut être démontré qu'elle a été créée dans le cadre normal de la conduite de l'activité de l'organisation et qu'elle est intacte et complète. Ne se limite pas au sens légal du terme.

Note 2 : Définition adaptée de la norme ISO/IEC 30300:2011, définition 3.1.5.

3.20 processus

ensemble d'activités corrélées ou interactives qui transforme des éléments d'entrée en éléments de sortie

[ISO 9000:2015]

3.21 sécurité de l'information

protection de la confidentialité, de l'intégrité et de la disponibilité de l'information

Note : En outre, d'autres propriétés, telles que l'authenticité, l'imputabilité, la non-répudiation et la fiabilité peuvent également être concernées.

[ISO/IEC 27000:2016]

Note pour les PSDC : les propriétés, telles que l'authenticité, l'imputabilité, la non-répudiation, la fiabilité et l'exploitabilité sont incluses dans la notion de sécurité.

3.22 système

ensemble d'actifs techniques corrélés ou interactifs

3.23 système de conservation

système composé d'un ensemble d'actifs techniques permettant le stockage temporaire des documents numériques en vue de leur conservation électronique, leur conversion en archives numériques, leur suppression et la conservation des archives numériques aussi longtemps que nécessaire, leur exploitation, leur restitution partielle ou totale, leur transfert et leur suppression

3.24 système de dématérialisation

système composé d'un ensemble d'actifs techniques permettant la création des documents numériques à partir des documents analogiques, le stockage temporaire des documents analogiques et numériques, leur restitution, leur transfert, la destruction éventuelle des documents analogiques et la suppression des documents numériques

3.25 système de dématérialisation ou de conservation (SDC)

système de dématérialisation, système de conservation, ou un système combinant les deux

4 Exigences spécifiques pour PSDC et complémentaires à la norme ISO/IEC 27001:2013

4.1 Structure de ce standard

Ce standard est un standard lié à la norme ISO/IEC 27001:2013. Il est spécifique aux PSDC au sens de la loi du 25 juillet 2015 relative à l'archivage électronique.

Les objectifs de sécurité et les mesures de sécurité spécifiques sont indiqués dans l'Annexe A.

4.2 Exigences spécifiques aux systèmes de management des PSDC

Toutes les exigences des chapitres 4 à 10 de la norme ISO/IEC 27001:2013 qui ne figurent pas ci-dessous restent applicables sans modification.

4 Contexte de l'organisation

Une exigence additionnelle à la norme ISO/IEC 27001:2013 est :

4.0 Système de Management des processus de dématérialisation ou de conservation

L'organisation doit gérer un système de management des processus de dématérialisation ou de conservation, intégré au SMSI ou répondant aux mêmes exigences, pour assurer le déroulement adéquat des processus de dématérialisation ou de conservation, la stabilité financière de l'organisation et sa capacité de couverture de responsabilités contractuelles, légales et réglementaires liés aux processus de dématérialisation ou de conservation.

Ce système de management des processus et le SMSI, ou le système de management intégrant ces deux aspects doit s'appliquer aux processus et activités liés à la prestation de services du PSDC et à tous les actifs supportant ces processus.

L'exigence 4.3 de la norme ISO/IEC 27002:2013 est complétée de la façon suivante.

4.3 Détermination du domaine d'applicabilité

Pour établir le domaine d'application du système de management des processus de dématérialisation ou de conservation, l'organisation doit en déterminer les limites et l'applicabilité.

Elle doit définir la nature des processus (dématérialisation ou conservation), le type des documents concernés et le type des clients (internes ou externes à l'organisation, secteurs concernés) qui peuvent bénéficier des services du PSDC.

Une exigence additionnelle à la norme ISO/IEC 27001:2013 est :

4.5 L'authenticité, la fiabilité, et l'exploitabilité

En complément des propriétés de sécurité de base qui sont:

a. la confidentialité,
b. l'intégrité, et

c. la disponibilité,

le système de management doit gérer les propriétés de sécurité complémentaires suivantes :

d. l'authenticité (souvent considéré comme un volet particulier de l'intégrité) :
   L'organisation doit pouvoir démontrer que toutes les activités effectuées dans le cadre de la gestion des processus de dématérialisation ou de conservation sont authentiques, à savoir :
   i. Les documents analogiques ou numériques ont bien été transmis par la personne qui est supposée les avoir transmis.
   ii. Le document numérique résultant de la numérisation d'un document analogique ou l'archive numérique a bien été créé par la personne ou le système au moment présumé.
   iii. Le document numérique ou l'archive numérique est bien ce qu'il est supposé être.

e. la fiabilité :
   L'organisation doit pouvoir démontrer que toutes les activités effectuées dans le cadre de la gestion des processus de dématérialisation ou de conservation sont fiables, à savoir :
   i. Toutes les activités effectuées dans le cadre de l'établissement des processus de dématérialisation ou de conservation sont exécutées conformément aux politiques et aux procédures définies et mises en œuvre par l'organisation en la matière.
   ii. Le document numérique ou l'archive numérique créé et exploité est conforme à son état original et non modifié par des modifications non autorisées.

f. l'exploitabilité :
   L'organisation doit pouvoir démontrer que l'exploitation des processus de dématérialisation ou de conservation crée un document numérique ou une archive numérique qui soit à tout moment localisable, lisible, intelligible, utilisable avec les informations nécessaires à la compréhension de son origine et disponible aussi longtemps que nécessaire.

Note : C'est en ajoutant ces propriétés dans l'envergure du SMSI qu'on généralise le système de management de la norme ISO/IEC 27001:2013 limité à la sécurité de l'information, à un système de management de toutes les propriétés requises aux activités de dématérialisation ou de conservation.

5 Leadership

Une exigence additionnelle à la norme ISO/IEC 27001:2013 est :

5.4 Rôles, responsabilités et autorités sur les processus de dématérialisation ou de conservation

La direction doit s'assurer que les responsabilités et autorités des rôles concernés par les processus de dématérialisation ou de conservation sont attribuées et communiquées au sein de l'organisation.

La direction doit désigner qui a la responsabilité et l'autorité de :

a. s'assurer que le système de management des processus de dématérialisation ou de conservation est conforme aux exigences du présent document ;
b. définir les critères de performances ;
c. rendre compte à la direction des performances du système de management des processus de dématérialisation ou de conservation ;
d. gérer la documentation (politiques, procédures) supportant ces processus ;
e. définir le système, son fonctionnement et sa sécurité au niveau opérationnel ;
f. superviser la mise en œuvre de la politique ;
g. émettre des recommandations en vue d'améliorer la gestion opérationnelle ;
h. définir et approuver les méthodes relatives à la gestion des risques pouvant impacter la stabilité financière et la capacité de couverture des responsabilités contractuelles, légales et réglementaires ;

i. gérer les risques pouvant impacter la stabilité financière de l'organisation et la capacité de couverture des responsabilités contractuelles, légales et réglementaires liées à la dématérialisation ou à la conservation ;
j. évaluer l'adéquation des mesures adoptées en vue de mitiger les risques pouvant impacter la stabilité financière et la capacité de couverture des responsabilités contractuelles, légales et réglementaires liées à la dématérialisation ou à la conservation, et jugées non acceptables par la direction de l'organisation ;
k. évaluer l'opportunité d'une couverture d'assurance pour garantir la continuité de l'exécution des processus de dématérialisation ou de conservation de l'organisation même en cas de cessation d'activité et pendant une période minimum de transition ;
l. identifier les changements en termes de risques pouvant impacter la stabilité financière et la capacité de couverture des responsabilités contractuelles, légales et réglementaires liées à la dématérialisation ou à la conservation ;
m. sensibiliser le personnel (de l'organisation et des tiers) concerné quant aux risques ;
n. identifier et évaluer les problèmes et les incidents ;
o. émettre des recommandations quant aux actions préventives et correctives à adopter en réponse aux problèmes et aux incidents évalués.

La direction doit attribuer chaque rôle et responsabilité à une personne ou à une entité dont les membres et le mode de fonctionnement sont documentés, et réviser régulièrement cette attribution.

Une exigence additionnelle à la norme ISO/IEC 27001:2013 est :

5.5 Leadership et engagement de PSDC

La direction doit faire preuve de leadership et affirmer son engagement en faveur du système de management en :

a. s'assurant qu'une politique et des objectifs sont établis en matière de processus de dématérialisation ou de conservation et qu'ils sont compatibles avec l'orientation stratégique de l'organisation dûment documentée et avec la politique de sécurité de l'information ;
   Note : Une politique dédiée aux processus de dématérialisation et une politique dédiée au processus de conservation peuvent être établies par l'organisation. Si un des processus n'est pas dans le domaine d'applicabilité, cette politique et toutes les exigences y relatives ne sont évidemment pas requises.
b. s'assurant que les exigences de cette politique sont intégrées aux processus ;
c. s'assurant que les ressources nécessaires pour le système de management des processus de dématérialisation ou de conservation sont disponibles (en particulier pour fournir les éléments probants quant à l'intégrité et la fiabilité) ;
d. communiquant sur l'importance de disposer d'un management des processus de dématérialisation ou de conservation efficace et de se conformer à ses exigences ;
e. s'assurant que le système de management des processus de dématérialisation ou de conservation produit le ou les résultats escomptés ;
f. orientant et soutenant les personnes pour qu'elles contribuent à l'efficacité du processus de dématérialisation ou de conservation ;
g. promouvant l'amélioration continue ;
h. aidant les autres managers concernés à faire également preuve de leadership dès lors que cela s'applique à leurs domaines de responsabilités ;
i. fournissant la preuve de l'existence légale de l'organisation ;
j. fournissant la preuve d'une situation financière suffisante et d'une situation stable pour répondre aux attentes des parties intéressées à l'activité de PSDC ;
   Note : L'organisation peut mener une étude sur le coût d'un transfert d'activités ou d'une restitution à tous les clients des documents y inclus toutes les informations requises pour maintenir la valeur probante d'un document dématérialisé et d'une archive numérique. L'étude pourra montrer que ce coût est inférieur aux provisions, aux réserves, ou au capital disponible de l'organisation, et que ces

paramètres sont stables. L'organisation peut mettre en place un processus de monitoring de ces paramètres qui assure une gestion d'incident en cas de dégradation de la stabilité financière.

Note : Une organisation de droit privé pourra par exemple fournir les informations suivantes :

- □ une étude sur le coût d'un transfert d'activités et la justification de pouvoir le réaliser à tout moment, compte tenu de son capital, de ses réserves, ou de ses provisions,
- □ les bilans et comptes de résultat des 3 dernières années fiscales, pour autant que l'ancienneté de l'organisation le permette,
- □ rapport ou avis financier émis par une autorité de surveillance luxembourgeoise,
- □ niveau d'exposition des activités métiers aux facteurs externes à l'organisation,
- □ rapport d'auditeurs financiers.

k. fournissant la garantie de continuité d'exécution (c'est-à-dire, pendant une période de transition minimum permettant d'assurer un transfert) des processus de dématérialisation ou de conservation, en particulier pour les cas suivants :
   1. processus de dématérialisation exécuté par l'organisation pour le compte d'un tiers,
   2. processus de conservation électronique exécuté par l'organisation pour le compte d'un tiers,
   3. sous-processus de restitution, transfert et suppression des archives numériques exécuté par l'organisation pour son propre compte.

   Cette garantie de continuité doit être gérée par l'organisation et couvrir le risque économique de cessation d'activités.

   Note : Un moyen pour l'organisation de garantir cette continuité d'exécution pendant une période de transition minimum est par exemple de contracter une assurance spécifique ou d'obtenir un engagement formel d'un actionnaire institutionnel ou privé majoritaire se portant garant.

6 Planification

Une exigence additionnelle à la norme ISO/IEC 27001:2013 est :

6.1.4 Risques liés à l'activité PSDC

L'organisation doit:

a. intégrer les risques de sécurité de l'information et opérationnels associés à la gestion des processus de dématérialisation ou de conservation dans son processus d'identification (6.1.2 c) d'analyse (6.1.2.d) et d'évaluation des risques (6.1.2.e), y intégrer également les risques pouvant impacter la stabilité financière de l'organisation et sa capacité de couverture de responsabilités contractuelles, légales et réglementaires liées à ces processus ;
b. appliquer son processus de traitement des risques de sécurité aux risques déterminés au point précédent ;
c. comparer les objectifs et les mesures déterminés en 6.1.3 b) avec celles de l'Annexe A du présent document et vérifier qu'aucune mesure nécessaire n'a été omise ;
d. compléter la déclaration d'applicabilité déterminée en 6.1.3 d) avec les mesures de l'Annexe A de la Règle technique et la justification de leur insertion ou de leur exclusion, ainsi que, le cas échéant, l'indication de leur mise en œuvre ;
e. porter à connaissance des clients et à l'ILNAS la déclaration d'applicabilité, notamment si elle contient des exclusions.

Une exclusion doit être rejetée si elle crée une non-conformité avec une exigence légale, réglementaire ou contractuelle.

7 Support

Une exigence additionnelle à la norme ISO/IEC 27001:2013 est :

7.4 Sensibilisation à la politique de dématérialisation ou de conservation

Les personnes effectuant un travail sous le contrôle de l'organisation doivent :

1. être sensibilisées à la politique de dématérialisation ou de conservation et respecter toute la documentation relative à cette politique ;
2. avoir conscience de leur contribution à l'efficacité du système de management, y compris aux effets positifs d'une amélioration des performances ;
3. avoir conscience des implications de toute non-conformité aux exigences requises par le système de management ;
4. connaitre leurs responsabilités en vertu de la loi luxembourgeoise en matière de dématérialisation ou de conservation et concernant les processus de dématérialisation ou de conservation.

Une exigence additionnelle à la norme ISO/IEC 27001:2013 est :

7.5.4 La non-répudiation des informations documentées

L'organisation doit mettre en place un environnement documentaire permettant de démontrer envers un tiers le respect des propriétés de sécurité indiquées au chapitre 4.5 du présent document et l'intégrité de la documentation.

8 Fonctionnement

Une exigence additionnelle à la norme ISO/IEC 27001:2013 est :

8.4 Acceptation des risques

L'organisation doit faire accepter par la direction l'appréciation des risques, le plan de traitement des risques incluant une indication des ressources requises, le niveau du risque actuel et celui après traitement.

L'organisation doit conserver la preuve de cette acceptation et la documentation de la délibération par la direction.

9 Évaluation des performances

L'exigence 9.1 de la norme ISO/IEC 27001:2013 est complétée de la façon suivante.

9.1 Surveillance, mesures, analyse et évaluation

De la même façon que pour le système de management de la sécurité de l'information, l'organisation doit évaluer les performances de son SDC, ainsi que l'efficacité du système de management des processus de dématérialisation et de conservation.

L'exigence 9.2 de la norme ISO/IEC 27001:2013 est complétée de la façon suivante.

9.2 Audit interne

De la même façon que pour le système de management de la sécurité de l'information, l'organisation doit réaliser des audits internes à des intervalles planifiés afin de recueillir des informations permettant de déterminer si le système de management des processus de dématérialisation et de conservation

a. est conforme :
    1. aux exigences propres de l'organisation concernant son système de management de processus de dématérialisation ou de conservation
    2. à cette règle technique ;
b. est efficacement mis en œuvre et tenu à jour.

L'organisation doit donc inclure ces audits dans le ou les programmes d'audit, définir les critères d'audit et le périmètre de chaque audit, sélectionner des auditeurs et réaliser des audits qui assurent l'objectivité et l'impartialité du processus d'audit, s'assurer qu'il est rendu compte des résultats des audits à la direction concernée, et conserver des informations documentées comme preuves de la mise en œuvre du ou des programme(s) d'audit et des résultats d'audit.

L'exigence 9.3 de la norme ISO/IEC 27001:2013 est complétée de la façon suivante.

9.3 Revue de direction

De la même façon que pour le système de management de la sécurité de l'information, la direction doit procéder à la revue du système de management des processus de dématérialisation ou de conservation mis en place par l'organisation, afin de s'assurer qu'il est toujours approprié, adapté et efficace.

La revue de direction doit prendre en compte :

g. les résultats de l'analyse de risques pouvant impacter la stabilité financière de l'organisation et sa capacité de couverture de responsabilités contractuelles, légales et réglementaires liées aux processus de dématérialisation ou de conservation de manière régulière.

La revue de direction doit avoir lieu au moins une fois par an et suite à des changements significatifs :

1. impactant le fonctionnement de l'organisation,
2. issus des besoins actuels de l'organisation,
3. de nature légale et réglementaire ayant un impact sur les activités et les processus de l'organisation.

10 Amélioration

L'exigence 10.2 de la norme ISO/IEC 27001:2013 est complétée de la façon suivante.

10.2 Amélioration continue

L'organisation doit continuellement améliorer la pertinence, l'adéquation et l'efficacité du système de management des processus de dématérialisation ou de conservation.

5 Code de bonnes pratiques spécifiques aux PSDC en relation avec ISO/IEC 27002:2013

Toutes les catégories de mesures, objectifs de sécurité, mesures, préconisations de mise en œuvre, et informations supplémentaires de la norme ISO/IEC 27002:2013 qui ne figurent pas ci-dessous restent applicables sans modification.

L'Annexe A résume les objectifs spécifiques et les mesures de sécurité spécifiques énoncés dans ce chapitre tout en les rendant leur examen obligatoire dans le traitement des risques.

5 Politiques de sécurité de l'information

Une catégorie de mesures additionnelles à la norme ISO/IEC 27002:2013 est :

5.2 Orientations de la direction en matière de politique de dématérialisation ou de conservation

Objectif : Apporter à la gestion des processus de dématérialisation ou de conservation une orientation et un soutien de la part de la direction, conformément aux exigences métier et aux lois et règlements en vigueur.

5.2.1 Politiques de dématérialisation ou de conservation

Mesure

Il convient de définir une « politique de dématérialisation ou de conservation », de la faire approuver par la direction, de la mettre en application, de la diffuser et de la communiquer aux salariés et aux tiers concernés.

Préconisations de mise en œuvre

Il convient que la politique de dématérialisation ou de conservation définisse le domaine d'application des processus de dématérialisation ou de conservation, la gestion de la sécurité de l'information et la gestion opérationnelle appliqués à ce processus.

Il convient que ce document contienne les éléments suivants :

a. une présentation de l'organisation, de son historique et de ses activités métiers ;
b. le lien avec la stratégie ou la motivation d'implémenter cette activité ;
c. une définition du domaine d'application des processus de dématérialisation ou de conservation ;
d. une description générale organisationnelle et technique des processus suivants sous-jacents
    1. au processus de dématérialisation :
        i. collecte des documents analogiques,
        ii. création et stockage temporaire des documents numériques,
        iii. stockage temporaire des documents analogiques,
        iv. restitution, transfert, destruction éventuelle des documents analogiques et suppression des documents numériques,
        v. le nom des fournisseurs dès qu'une activité du processus est sous-traitée ;
    2. au processus de conservation :
        i. collecte des documents numériques,
        ii. création et conservation des archives numériques,
        iii. restitution, transfert, suppression des archives numériques,

iv. le nom des fournisseurs dès qu'une activité du processus est sous-traitée ;

e. une description générale technique du SDC et de son niveau de conformité à des normes et des référentiels reconnus ;
f. les rôles et les responsabilités spécifiques au processus de dématérialisation ou de conservation et aux processus sous-jacents exécutés par l'organisation et en matière de gestion de la sécurité de l'information et de gestion opérationnelle ;
g. les grands principes de sécurité de l'information appliqués au processus de dématérialisation ou de conservation exécuté par l'organisation, notamment en matière d'authenticité, de fiabilité et d'exploitabilité ;
h. les références aux lois et aux règlements applicables à l'organisation et spécifiques au processus de dématérialisation ou de conservation ;
i. la gestion de la documentation supportant le processus de dématérialisation ou de conservation ;
j. des références aux documents, comme les procédures d'administration, d'opérations et de sécurité, supportant la politique de dématérialisation ou de conservation ;
k. les modalités de revue de la politique de dématérialisation ou de conservation.

5.2.2 Revue de la politique de dématérialisation ou de conservation

Mesure

Pour garantir la constance de la pertinence, de l'adéquation et de l'efficacité de la politique de dématérialisation ou de conservation, il convient de revoir ces politiques et les processus y relatifs à intervalles programmés et en cas de changements majeurs.

Préconisations de mise en œuvre

Les mêmes préconisations que pour la politique de sécurité de l'information s'appliquent à cette politique.

La catégorie « 6 Organisation de la sécurité de l'information » est complétée de la façon suivante.

6 Organisation de la sécurité de l'information et des processus de dématérialisation ou de conservation

6.1 Organisation interne

Objectif : Établir un cadre de gestion pour engager, puis vérifier la mise en œuvre et le fonctionnement de la sécurité de l'information et des processus de dématérialisation ou de conservation au sein de l'organisation.

6.1.1 Fonctions et responsabilités liées à la sécurité de l'information et aux processus de dématérialisation ou de conservation

Mesure

Il convient de définir et d'attribuer toutes les responsabilités en matière de sécurité de l'information, en particulier celles liées à l'exécution des processus de dématérialisation ou de conservation et celles qui consistent à s'assurer de la conformité des processus et de la gestion opérationnelle aux politiques et aux documents applicables.

Préconisations de mise en œuvre

Il convient d'attribuer les responsabilités conformément à la politique de sécurité de l'information (voir 5.1.1 de l'ISO/IEC 27002:2013) et à la politique de dématérialisation ou de conservation (voir 5.2.1 du présent document).

Il convient de déterminer les responsabilités relatives à la protection des actifs et la mise en œuvre de processus de sécurité spécifiques et des processus de dématérialisation ou de conservation.

Il convient de déterminer les responsabilités liées aux activités de gestion des risques en matière de sécurité de l'information et d'exploitation des processus de dématérialisation ou de conservation et en particulier, celles liées à l'acceptation des risques résiduels. Si nécessaire, il convient de compléter ces responsabilités de directives détaillées, appropriées à certains sites et moyens de traitement de l'information.

Il convient de préciser les domaines de responsabilité de chacun et notamment de prendre les mesures suivantes :

a. il convient d'identifier et de déterminer les actifs et les processus de sécurité ainsi que les processus de dématérialisation ou de conservation ;
b. il convient d'affecter une personne ou une entité responsable à chaque actif ou processus et de documenter ses responsabilités dans le détail (voir 8.1.2) ;
c. il convient de définir et de documenter les différents niveaux d'autorisation ;
d. pour être à même d'assurer les responsabilités, il convient que les personnes désignées soient compétentes dans ce domaine et qu'elles bénéficient de facilités pour se tenir au courant des évolutions ;
e. Il convient d'identifier et de documenter les activités de coordination et de supervision liées aux relations avec les fournisseurs.

Il convient de désigner pour chaque processus de dématérialisation ou de conservation une personne pour chacune des responsabilités suivantes :

a. la gestion de la documentation (politiques, procédures) supportant ces processus,
b. leur définition au niveau opérationnel, incluant le SDC et les mécanismes de sécurité associés,
c. la supervision de leur mise en œuvre,
d. la définition de leurs critères de performances,
e. leur évaluation selon les critères de performances,
f. l'émission de recommandations en vue d'améliorer leur gestion opérationnelle.

Informations supplémentaires

Les personnes auxquelles ont été attribuées des responsabilités peuvent déléguer des tâches. Néanmoins, elles demeurent responsables et il convient qu'elles s'assurent de la bonne exécution de toute tâche déléguée.

6.1.2 Séparation des tâches

Préconisations de mise en œuvre

Il convient de s'assurer que les personnes assumant des rôles et des responsabilités dans la gestion de processus ou d'activités de la sécurité de l'information ou opérationnels liés à la dématérialisation ou la conservation, n'assument pas également la revue de l'efficacité de l'exécution de ces rôles et responsabilités ainsi que l'évaluation de leur conformité à des objectifs définis.

Il convient d'assurer une séparation effective des activités d'administration, d'opérations et de sécurité non seulement dans la description des rôles, mais aussi dans l'attribution des privilèges pour les comptes des utilisateurs autorisés à accéder au SDC, de manière à réduire les risques de conflits d'intérêts et d'accès non autorisés.

Pour respecter le principe de non-répudiation, il convient de pouvoir démontrer que les privilèges d'accès établis pour l'ensemble des utilisateurs du SDC, y compris les accès à travers des comptes techniques, respectent le principe de séparation effective des activités d'administration, d'opérations et de sécurité du système de conservation.

6.1.5 La sécurité de l'information dans la gestion de projet

Préconisations de mise en œuvre

Il convient de rédiger et d'approuver les procédures de gestion du SDC dans la définition et la mise en œuvre des projets de dématérialisation ou de conservation.

Une catégorie de mesures additionnelles à la norme ISO/IEC 27002:2013 est :

6.3 Organisation interne spécifique aux processus de dématérialisation et de conservation

Objectif : Établir un cadre de gestion pour assurer le respect des exigences légales spécifiques des processus de dématérialisation ou de conservation au sein de l'organisation.

6.3.1 Vérification des documents numériques après dématérialisation

Mesure

Il convient d'exercer une vérification du contenu des documents numériques par rapport aux documents analogiques correspondants.

Préconisations de mise en œuvre

En ce qui concerne le processus de dématérialisation, il convient d'implémenter des

a. mécanismes de vérification de l'adéquation du nombre de documents analogiques en entrée (ou du nombre de pages composant ces documents) avec le nombre de documents (ou de pages) en sortie (numériques et analogiques rejetés), et des
b. mécanismes de vérification du contenu des documents numériques résultant de la numérisation de documents analogiques pour s'assurer de la reproduction conforme à l'original.

6.3.2 Principes du double contrôle pour la modification ou la suppression d'archives numériques

Mesure

Il convient de s'assurer que toute modification ou suppression des archives numériques créées, qui n'étaient pas programmées lors de la définition du projet de conservation, nécessitent l'approbation de deux utilisateurs autorisés à exécuter ces opérations.

6.3.3 Gestion des preuves

Mesure

Il convient d'établir une procédure et de mettre en œuvre une gestion adéquate des preuves du fonctionnement du SDC et des activités effectuées par le personnel concerné.

Préconisations de mise en œuvre

Il convient de s'assurer que l'intégrité du fonctionnement du SDC, des documents numériques et des archives numériques gérées par le SDC est vérifiée de manière régulière et suite à une modification significative du SDC et du processus de conservation.

6.3.4 Relations avec l'autorité nationale

Mesure

Il convient de mettre en application des procédures pour notifier aux autorités compétentes, en particulier l'ILNAS, les prévisions de changements significatifs pouvant impacter la sécurité de l'information et les activités opérationnelles ainsi que, dans les meilleurs délais et en tout état de cause dans un délai de vingt-quatre heures après en avoir eu connaissance, toute atteinte à la sécurité ou toute perte d'intégrité ayant une incidence potentiellement importante sur le service de dématérialisation ou de conservation.

Préconisations de mise en œuvre

Il convient notamment de considérer comme changements significatifs :

a. un changement de direction de l'organisation,
b. une modification du SDC impactant les processus associés,
c. une modification du périmètre d'activités gérées par des fournisseurs impactant les processus de dématérialisation ou de conservation exécutés par l'organisation.

Une catégorie de mesures additionnelles à la norme ISO/IEC 27002:2013 est :

6.4 Organisation des processus de dématérialisation et de conservation impliquant les clients

Objectif : Clarifier les responsabilités entre le PSDC et ses clients et assurer la transparence en matière de sécurité et d'exploitation des processus de dématérialisation ou de conservation envers les clients.

6.4.1 La sécurité dans les accords avec le client

Mesure

Il convient d'établir les conditions d'exécution des processus de dématérialisation ou de conservation, ainsi que les besoins de sécurité de l'information associés à ces processus avec le client dans un document contractuel approuvé par le client et le PSDC.

Préconisations de mise en œuvre

Si le client est interne à l'organisation ou appartient à la même entité juridique, le document contractuel peut être remplacé par un document interne établi et validé selon les pratiques de gestion documentaire de l'organisation.

Il convient d'établir avec le client les éléments suivants dans le cadre de la gestion d'un projet de dématérialisation ou de conservation :

a. le besoin en informations du client liées aux processus de dématérialisation ou de conservation ;
b. la description détaillée du projet de dématérialisation ou de conservation, en prenant en compte les aspects techniques, opérationnels, sécuritaires, légaux et réglementaires ;
c. la base de référence des mesures de sécurité et les mesures additionnelles mises en exploitation pour sassurer l'authenticité, la fiabilité et l'exploitation des documents collectés (analogiques et numériques), des documents numériques et des archives numériques du client pendant l'exécution des processus de dématérialisation ou de conservation ;

d. les niveaux de service liés à l'exécution du SDC ;
e. la gestion des changements organisationnels et techniques pouvant impacter les processus de dématérialisation ou de conservation, ainsi que le SDC ;
f. la gestion des incidents (majeurs) impactant les processus de dématérialisation ou de conservation, ainsi que le SDC ;
g. le processus et les modalités à appliquer pour l'évaluation des services ainsi que l'acceptation des services par le client ;
h. les rôles et responsabilités du client et de l'organisation dans le cadre de la mise en œuvre du projet et les conséquences en cas de non-respect de ces rôles et de ces responsabilités ;
i. les points de contacts du client et de l'organisation, d'un point de vue contractuel, opérationnel et de la sécurité de l'information ;
j. l'implication du client dans l'appréciation et le traitement des risques.

La base de référence des mesures de sécurité et les mesures additionnelles mises en exploitation peuvent être documentées dans la déclaration d'applicabilité (voir ISO/IEC 27001) ou dans un document appelé « exigences d'assurance de sécurité » selon les Critères Communs (voir ISO 15408).

Il convient que le client s'engage en particulier à fournir et maintenir une liste de personnes autorisées à :

a. soumettre et à récupérer des documents analogiques ;
b. accéder aux documents numériques résultants de la numérisation des documents analogiques ou aux archives numériques ;
c. utiliser le SDC ;
d. demander la destruction et la suppression des documents collectés (analogiques et numériques), des documents numériques résultants de la numérisation des documents analogiques ou des archives numériques.

Informations supplémentaires

Un changement d'un document contractuel nécessite l'accord des parties contractantes.

C'est à ce niveau que des mesures de sécurité particulières exigées par le client et complémentaires à celles que le PSDC établit de sa propre initiative peuvent être spécifiées.

6.4.2 Obligation d'information préalable du client

Mesure

Préalablement à toute relation contractuelle avec un détenteur, il convient de mettre à disposition, sur un support durable et dans des termes aisément compréhensibles, les informations relatives aux conditions de prestation de service, en particulier toutes les informations légalement requises pour assurer un service transparent.

Préconisations de mise en œuvre

Il convient que le PSDC inclue dans les informations données à ses clients avant d'établir un contrat :

a. la procédure suivie pour la dématérialisation ou pour la conservation,
b. la procédure suivie afin de restituer les copies à valeur probante sous une forme lisible en garantissant la fidélité à l'original,
c. les modalités et conditions d'une éventuelle sous-traitance y compris le lieu de stockage des données,
d. les obligations légales que le PSDC doit observer,
e. les conditions contractuelles de réalisation des prestations, y compris les limites éventuelles de responsabilité du PSDC,
f. les normes et procédures mises en œuvre ainsi que les caractéristiques techniques essentielles des installations utilisées pour la réalisation des prestations,
g. les modalités d'information du client en cas de changement.

Il convient de convenir avec les clients (internes ou externes à l'organisation) qui sont impactés le déroulement détaillé et les règles à suivre dans le cadre de l'exécution et des processus de dématérialisation et de conservation.

Il convient d'inclure ce déroulement détaillé et ces règles dans les procédures d'exploitation des processus de dématérialisation et de conservation, et de les faire approuver par les clients concernés.

Il convient d'impliquer le client dans les changements des procédures qu'il a approuvées.

Il convient d'inclure dans ces procédures le déroulement détaillé :

a. de la collecte des documents analogiques (pour le processus de dématérialisation seulement),
b. de la collecte des documents numériques (pour la conservation),
c. du stockage temporaire des documents numériques,
d. de la création et la conservation des archives numériques (pour la conservation),
e. de la restitution, le transfert et la suppression des archives numériques (pour la conservation).

Il convient de notifier le client d'une suppression programmée d'une archive numérique du client si un calendrier de suppression spécifique à cette archive a été rédigé lors de la définition du projet de conservation.

En cas d'absence de calendrier de suppression pour une archive numérique, il convient de demander au préalable au client l'autorisation de la supprimer.

6.4.3 Classification des actifs du client

Mesure

Il convient que le client définisse avec le PSDC pour tous ses documents analogiques ou numériques et toutes ses archives numériques le niveau de classification, la durée de rétention, ainsi que les éventuelles autres exigences de sécurité comme les droits d'accès particuliers.

Préconisations de mise en œuvre

Il convient que le client assume le rôle du propriétaire pour les informations qui lui appartiennent et qui sont gérées par l'organisation.

Il convient de sensibiliser le client au fait qu'il est responsable des exigences de classification définies et appliquées à ses documents (documents collectés, documents numériques ou archives numériques).

6.4.4 Obligation d'information du client en cas de changements ou d'incidents

Mesure

Il convient d'informer, avant la mise en application ou dans les plus brefs délais, les clients internes ou externes concernés de tout changement des informations préalables et des informations liées aux obligations contractuelles, ainsi que de tout incident pouvant mettre en danger les informations du client, tout en donnant les justifications nécessaires.

Préconisations de mise en œuvre

Il convient d'informer dans les plus brefs délais le client :

a. en cas de survenance d'incidents pouvant impacter :
    1. les documents du client,
    2. les processus de dématérialisation ou de conservation utilisés par le client ou pour son compte,
    3. le SDC utilisé par le client ou pour son compte ;

b. en cas de tentatives d'accès aux documents du client gérés par l'organisation avec les identifiants de connexion du client et hors des conditions normales de leur utilisation, par exemple hors des heures normales de bureau.

Il convient de considérer comme changements significatifs les changements signalés à l'autorité nationale (voir 6.3.4).

Il convient d'appliquer une conversion d'une archive numérique dans un format différent de son format initial que sur confirmation écrite du client (interne à l'organisation et externe) concerné par cette archive.

Il convient d'informer le client sur l'effet du changement sur l'appréciation des risques.

Il convient de garder une preuve que cette information a eu lieu, et si le temps avant la mise en application est court, de demander l'approbation du client.

7 La sécurité des ressources humaines

7.2 Pendant la durée du contrat

Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :

7.2.4 Engagement envers les politiques

Mesure

Il convient que le personnel interne et celui des fournisseurs, s'ils sont impliqués dans la gestion opérationnelle de la sécurité ou des processus de dématérialisation ou de conservation, comprennent et s'engagent par écrit à respecter la politique de sécurité et la politique de dématérialisation ou de conservation.

Préconisations de mise en œuvre

Il convient que le personnel interne et celui des fournisseurs impliqués dans la gestion opérationnelle de la sécurité ou des processus de dématérialisation ou de conservation :

1. soient correctement informés de leurs rôles et responsabilités liés aux processus de dématérialisation ou de conservation ;
2. s'engagent par écrit à respecter les politiques de dématérialisation ou de conservation et la politique de sécurité de l'information ;
3. assistent à une formation initiale sous forme de sensibilisation pour présenter les politiques, les attentes et les besoins de l'organisation en la matière, afin de s'assurer d'une compréhension commune de ces éléments ;
4. assistent à une formation continue de manière à rappeler les exigences liées à la dématérialisation ou à la conservation et à présenter les procédures associées à ces exigences et les récentes modifications apportées à l'ensemble de la documentation liée aux domaines concernés.

8 Gestion des actifs

8.1 Responsabilités relatives aux actifs

Des préconisations de mise en œuvre additionnelles sont :

8.1.1 Inventaire des actifs

Préconisations de mise en œuvre

Il convient d'identifier :

a. les processus de dématérialisation ou de conservation,
b. les composants des systèmes de dématérialisation ou de conservation,
c. les clients,
d. les documents collectés (analogiques et numériques) des clients,
e. les documents numériques résultants de la numérisation des documents analogiques des clients,
f. les archives numériques des clients.

8.1.2 Propriété des actifs

Préconisations de mise en œuvre

Il convient que le propriétaire de chaque actif processus de dématérialisation ou de conservation :

d. approuve l'évaluation des aspects opérationnels du SDC au moins une fois par an et suite à une modification significative ;
e. revoie la description détaillée du SDC et les spécifications des mécanismes de sécurité du système de conservation de manière régulière (au moins une fois par an) et suite à une modification significative du SDC.

Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :

8.1.4 Cloisonnement d'informations secrètes ou d'informations à caractère personnel

Mesure

Il convient de cloisonner d'éventuelles informations secrètes ou informations à caractère personnel de façon suffisante pour notamment pouvoir donner suite à la demande du propriétaire de les détruire sans mettre en danger d'autres informations archivées ou les preuves de la bonne gestion pour d'autres informations dématérialisées ou conservées.

Préconisations de mise en œuvre

En vue de respecter le règlement européen sur la protection des données à caractère personnel, en particulier le droit à l'oubli, il convient que le client ou le PSDC s'abstienne de mettre dans les métadonnées des informations à caractère personnel, si ces métadonnées font partie du système de traçabilité des opérations.

8.2 Classification de l'information

Des préconisations de mise en œuvre additionnelles sont :

8.2.1 Classification des informations

Préconisations de mise en œuvre

Il convient de définir des niveaux de classification et de les attribuer aux actifs inventoriés en intégrant les exigences relatives à l'authenticité, à la fiabilité et à l'exploitation aussi longtemps que nécessaire.

Il convient d'assurer une revue de ces lignes directrices en cas de changement des spécificités du SDC et en cas de changement des attentes des clients.

Informations supplémentaires

Un critère « fiabilité » peut être défini en complément d'autres critères. Il peut contenir plusieurs niveaux de précision d'une dématérialisation (couleur versus noir et blanc, encodage de la couleur, résolution) et attribuer un tel niveau spécifiquement aux documents collectés des clients et aux archives numériques des clients.

Le critère d'intégrité peut être utilisé pour inclure les exigences liées à l'authenticité.

Le critère de disponibilité peut être utilisé pour inclure les exigences liées à l'exploitabilité.

8.3 Manipulation des supports

Des préconisations de mise en œuvre additionnelles sont :

8.3.2 Mise au rebut des supports

Préconisations de mise en œuvre

Il convient d'envisager :

a. la destruction des éléments suivants, par des mécanismes sécurisés :
   1. les documents analogiques des clients selon les conditions définies dans les documents contractuels établis entre les clients et l'organisation,
   2. tout support de stockage de l'organisation contenant les informations des clients (incluant les documents et archives numériques) ou de nature confidentielle à l'organisation,
   3. la suppression de toutes les informations des clients, contenues dans les supports de stockage de l'organisation par des mécanismes sécurisés si ces supports ne peuvent pas être détruits de manière sécurisée ;
b. l'évaluation par un tiers pouvant attester l'effectivité de la destruction et de la suppression ;
c. en cas de recours à un fournisseur, la production d'une attestation de ce fournisseur stipulant que :
   1. les supports de stockage remis au tiers par l'organisation en vue de leur destruction sont bien ceux qui ont été détruits,
   2. les informations stockées dans les supports de stockage remis par l'organisation en vue de leur suppression ont bien été supprimées,
   3. la destruction des documents analogiques et des supports de stockage et la suppression des informations stockées dans ces supports ont été respectivement effectuées par une méthode sécurisée basée sur les bonnes pratiques en la matière.

9 Contrôle d'accès

9.1 Exigences métier en matière de contrôle d'accès

Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :

9.1.3 Ségrégation effective liée aux droits d'accès

Mesure

Il convient d'impliquer trois personnes différentes dans la gestion d'un droit d'accès : une pour l'autorisation de l'accès, une pour la vérification du respect des exigences de sécurité, et finalement une pour l'attribution de l'accès sur les systèmes.

Préconisations de mise en œuvre

Il convient qu'un administrateur de droits d'accès sur un SDC n'attribue ce droit que si le droit a été formellement autorisé selon la politique des droits d'accès pour une autre personne et que le respect des exigences de sécurité avec ce droit a été validé par une personne différente.

10 Cryptographie

10.1 Mesures cryptographiques

Des préconisations de mise en œuvre additionnelles sont :

10.1.1 Politique d'utilisation des mesures cryptographiques

Préconisations de mise en œuvre

Lors de l'élaboration d'une politique cryptographique, il convient de prendre en compte le point suivant :

h. l'application des services de confiance qualifiés conformes au règlement eIDAS pour assurer la sécurité des documents dématérialisés et archives numériques.

Informations supplémentaires

La norme ETSI TS 102 176-1 énumère des algorithmes cryptographiques et recommande une durée de validité de leur utilisation.

Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :

10.1.3 Authentification à deux facteurs

Mesure

Pour les personnes qui interagissent avec les actifs techniques du système de conservation ou qui accèdent aux documents numériques et aux archives numériques, il convient d'assurer une authentification appropriée et sécurisée basée sur des mécanismes cryptographiques et, si l'accès est possible à partir de locaux ne requérant pas d'authentification à deux facteurs à l'entrée, une authentification à deux facteurs.

Préconisations de mise en œuvre

Il convient d'utiliser un dispositif sécurisé, par exemple une carte à puce ou une clé USB cryptographique contenant un certificat électronique d'authentification, un dispositif physique d'authentification ou des techniques de biométrie pour s'assurer de l'authentification sécurisée d'un utilisateur aux actifs techniques du système de conservation, aux documents numériques et aux archives numériques gérés par le système de conservation.

Il convient d'utiliser un dispositif de filtrage d'adresses IP associé à un moyen cryptographique, par exemple un certificat SSL, pour s'assurer de l'authentification sécurisée d'un actif technique du système de conservation aux autres actifs du système de conservation, aux documents numériques et aux archives numériques gérés par le système de conservation.

Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :

10.1.4 Protection de l'intégrité des documents numériques ou des archives numériques

Mesure

Il convient de protéger l'intégrité des documents numériques collectés par le système de conservation et des archives numériques générées par le système de conservation avec des algorithmes et techniques cryptographiques appropriés.

Préconisations de mise en œuvre

Il convient de protéger l'intégrité des documents numériques collectés par le système de conservation et des archives numériques générées par le système de conservation pour s'assurer que ces documents sont correctement stockés, traités et supprimés et que ces archives sont correctement créées, exploitées, restituées, transférées ou supprimées.

Il convient que pour chaque document numérique à archiver, son empreinte digitale soit calculée par l'émetteur de ce document et transmise de manière sécurisée à l'organisation qui vérifiera l'intégrité du document numérique reçu en calculant et en obtenant une empreinte digitale identique à celle transmise par l'émetteur du document.

Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :

10.1.5 Protection de l'intégrité des documents internes

Mesure

Il convient de protéger l'intégrité des documents internes au SDC et aux processus y liés, en particulier les journaux d'événements du SDC, avec des protocoles utilisant des algorithmes et techniques cryptographiques appropriés.

Préconisations de mise en œuvre

Il convient de protéger l'intégrité des documents internes dans le temps, en particulier des journaux d'événements ou des opérations de vérification.

Il convient en particulier de s'assurer de :

a. l'établissement d'un schéma de liaison pour lier les événements enregistrés d'un journal entre eux permettant de détecter toute suppression d'événements survenus par le passé,

b. l'horodatage régulier, par exemple une fois par jour, des journaux d'événements par une autorité d'horodatage qualifiée.

Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :

10.1.6 Signature électronique des documents internes

Mesure

Il convient que les utilisateurs du SDC utilisent une signature qualifiée ou un mécanisme apportant une garantie équivalente pour valider les documents internes nécessaires à prouver le bon fonctionnement du SDC et des processus y liés.

Préconisations de mise en œuvre

Il convient d'utiliser un dispositif sécurisé pour permettre :

a. à un utilisateur du système de conservation de signer électroniquement des rapports d'activités d'administration, d'opérations et de sécurité du système de conservation de manière à s'assurer de l'authenticité des activités effectuées,
b. à une personne de l'organisation de signer électroniquement les transmissions d'informations, de documents numériques et d'archives numériques à destination des clients (internes ou externes à l'organisation) et des autorités compétentes de manière à s'assurer de l'authenticité des envois.

Le dispositif sécurisé de création de signatures électroniques et le certificat électronique qualifié utilisé doivent répondre aux exigences définies par l'Union européenne en la matière.

Il convient également d'utiliser des formats de signatures électroniques comme CAdES [5], XAdES [6] et PAdES [7] pour maintenir une pérennité de la signature électronique, des informations, des documents numériques et des archives numériques attachés à cette signature.

Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :

10.1.7 Protection des transmissions de documents

Mesure

Il convient de protéger la transmission d'informations et de documents numériques avec des protocoles utilisant des algorithmes et techniques cryptographiques appropriés.

Préconisations de mise en œuvre

Il convient d'utiliser un protocole sécurisé (SFTP, TLS, PPP, L2TP et IPSec…) pour sécuriser la transmission d'informations, de documents numériques et d'archives numériques entre les éléments suivants :

a. les actifs techniques du système de conservation, même pour ceux appartenant à un même réseau ;
b. les parties concernées par le processus de conservation comme l'organisation, les clients (internes ou externes à l'organisation) et les autorités compétentes.

Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :

10.1.8 Conservation des signatures électroniques

Mesure

Si l'intégrité d'un document numérique à archiver repose sur une signature électronique, il convient de conserver le document avec la preuve que la signature a été vérifiée au plus tard au moment de l'archivage.

Préconisations de mise en œuvre

Il convient de démontrer l'intégrité du document en démontrant :

a. qu'au moment de l'archivage, la signature électronique était correcte, le certificat électronique qualifié y apposé était valide et issu d'une autorité de certification reconnue ;
b. que le système d'archivage conserve l'intégrité des documents archivés aussi longtemps que nécessaire.

Informations supplémentaires

Plusieurs techniques sont possibles à cette fin comme :

a. l'utilisation du protocole de vérification en ligne de certificats (OCSP) de l'autorité de certification émettrice du certificat électronique qualifié,
b. l'horodatage du rapport d'activités signé et récupération de la liste de révocation des certificats (CRL) publiée régulièrement par l'autorité de certification émettrice du certificat électronique qualifié.

11 Sécurité physique et environnementale

11.1 Zones sécurisées

Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :

11.1.7 Accompagnement des visiteurs

Mesure

Il convient qu'un membre de l'organisation habilité accompagne de manière permanente tous les visiteurs de l'organisation, même si l'accès à ces zones leur a déjà été autorisé.

Préconisations de mise en œuvre

Il convient d'assurer que les visiteurs n'accèdent pas aux zones associées au processus de dématérialisation, notamment en cas d'activités de traitement de documents analogiques de clients pour réduire les risques de divulgation non autorisée d'informations.

Il convient de prendre les mesures nécessaires pour s'assurer que les visiteurs ne puissent pas voir des informations des clients.

Il convient d'assurer une surveillance effective des tiers autorisés de manière permanente à accéder aux zones sécurisées de l'organisation dès qu'ils accèdent aux actifs techniques du SDC et aux documents des clients.

Il convient de protéger les actifs techniques du SDC contre des accès non autorisés :

a. en cas d'évacuation des zones hébergeant ces actifs,

b. au cas où ils sont situés dans des sites multioccupants.

11.2 Matériels

Des préconisations de mise en œuvre additionnelles sont :

11.2.1 Emplacement et protection du matériel

Préconisations de mise en œuvre

Il convient de considérer les documents analogiques des clients comme des actifs nécessitant une protection spéciale (au sens de 11.2.1.d de la norme ISO/IEC 27002:2013) au niveau des conditions ambiantes et des autres menaces liées.

11.2.5 Sortie des actifs

Préconisations de mise en œuvre

Il convient de ne pas sortir de l'organisation sans autorisation préalable du client des documents analogiques du processus de dématérialisation, excepté pour prévenir la destruction de ces actifs en cas de catastrophe.

12 Sécurité liée à l'exploitation

12.1 Procédures et responsabilités liées à l'exploitation

Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :

12.1.5 Procédures d'exploitation du SDC

Mesure

Il convient de définir, mettre en œuvre, et faire suivre par le personnel concerné (de l'organisation et des fournisseurs) des procédures d'administration, d'opérations du SDC, d'exploitation du processus de dématérialisation ou de conservation, et de contrôle de la sécurité du SDC et des processus incluant toutes les règles à suivre nécessaires pour assurer les propriétés de confidentialité, d'intégrité, de disponibilité, d'authenticité, de fiabilité et d'exploitabilité.

Préconisations de mise en œuvre

Il convient d'inclure dans les procédures de gestion du SDC les activités suivantes :

a. la gestion des accès au SDC et des privilèges associés aux comptes du SDC ;
b. la gestion des fonctionnalités d'administration, d'opérations et de sécurité du SDC et des instructions pour les exécuter ;
c. la gestion de la configuration du SDC ;
d. l'instruction du fonctionnement du SDC en mode dégradé, de son redémarrage et de sa récupération ;
e. la gestion des mécanismes de surveillance du SDC ;
f. la gestion des journaux d'événements du SDC et des instructions pour leur exploitation ;
g. la gestion des mécanismes cryptographiques de sécurité du SDC, comme les suivants :
    1. les mécanismes d'authentification et de signature des utilisateurs du SDC,
    2. les protocoles sécurisés de transmission d'informations, de documents numériques et d'archives numériques,
    3. les mécanismes d'intégrité des documents numériques, des archives numériques et des journaux d'événements, ainsi que

4. le remplacement de ces mécanismes en cas de découverte de vulnérabilités sans altérer l'exploitabilité et l'intégrité des archives ;

h. si c'est convenu dans l'accord avec les clients, la gestion des mécanismes de détection et de suppression de codes malveillants ;
i. gestion des mécanismes de contrôle régulier d'intégrité du SDC ;
j. gestion des mécanismes de suppression des documents numériques et des archives numériques gérées par le SDC ;
k. gestion des supports de stockage du SDC, de leur remplacement et de leur mise au rebut ;
l. gestion des sauvegardes du SDC, des sauvegardes des documents numériques et des archives numériques gérées par le SDC et de leur restauration respective ;
m. gestion de la continuité et de la reprise du SDC même en cas de désastre ;
n. gestion des changements du SDC ;
o. gestion des incidents pouvant impacter le SDC ;
p. maintenance des actifs techniques avec gestion du support des fournisseurs en cas de dysfonctionnement du SDC ;
q. gestion des métadonnées de description et de contrôle associées aux archives numériques ;

et en plus pour les processus de dématérialisation :

r. la gestion des mécanismes de vérification de l'adéquation du nombre de documents analogiques (ou du nombre de pages composant ces documents) numérisés ;
s. la gestion des mécanismes de vérification du contenu des documents numériques.

Des préconisations de mise en œuvre additionnelles sont :

12.4 Journalisation et surveillance

12.4.1 Journalisation des événements

Préconisations de mise en œuvre

Il convient d'identifier et d'enregistrer dans des journaux tous les événements en lien avec le SDC, en particulier :

a. les événements système des actifs du SDC,
b. les erreurs et dysfonctionnements des actifs du SDC,
c. les erreurs et dysfonctionnements liés à la génération de journaux d'événements,
d. les événements liés aux documents analogiques, aux documents numériques et aux archives numériques traitées par le SDC.

12.4.3 Journaux administrateur et opérateur

Préconisations de mise en œuvre

Il convient d'identifier et d'enregistrer dans des journaux toutes les activités effectuées par les comptes des utilisateurs du SDC, incluant les activités effectuées hors de conditions normales d'utilisation du SDC en lien avec le SDC, en particulier :

a. les tentatives de connexion d'utilisateurs hors des heures normales de bureau,
b. les activités effectuées par les utilisateurs dans un laps de temps plus court que la normale, pouvant conduire à suspecter qu'elles sont réalisées par des actifs techniques et non des personnes physiques,
c. la duplication de sessions utilisateurs.

12.4.4 Synchronisation des horloges

Préconisations de mise en œuvre

Il convient d'assurer que :

a. les actifs techniques supportant le SDC soient synchronisés avec le temps universel coordonné (UTC), *via* une source de temps faisant autorité,
b. les événements liés à la synchronisation régulière de l'horloge système des actifs techniques du SDC soient enregistrés et conservés aussi longtemps que nécessaire,
c. un unique format de la date et de l'heure soit adopté pour la génération des événements du SDC pour faciliter la traçabilité des actions effectuées,
d. une synchronisation avec l'horloge maîtresse soit faite de façon suffisamment régulière pour s'assurer que la variation entre l'horloge maître et l'horloge des systèmes dans le périmètre reste en dessous du seuil d'une seconde,
e. toute variation supérieure à la variation tolérée soit détectée dans les plus brefs délais afin que des actions correctrices puissent être adoptées,
f. des éléments de vérification de l'exactitude de l'horloge, comme des jetons d'horodatage sont générés dans le cadre du fonctionnement du SDC.

Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :

12.4.5 Exploitabilité des journaux d'événements

Mesure

Il convient de conserver les journaux d'événements générés sous une forme exploitable et protégée contre toute manipulation et suppression non autorisées pour assurer une traçabilité aussi longtemps que nécessaire de tous les événements enregistrés par ces mécanismes.

Préconisations de mise en œuvre

Il convient de centraliser l'information journalisée en lien avec le SDC.

Il convient d'utiliser des supports de stockage pérennes pour une conservation appropriée aussi longtemps que nécessaire des journaux d'événements.

Une catégorie de mesures additionnelle à la norme ISO/IEC 27002:2013 est :

12.8 Gestion correcte et sécurisée du SDC

Objectif : assurer la gestion correcte et sécurisée des documents analogiques à dématérialiser, des documents numériques et des archives numériques dans le cadre du processus de dématérialisation ou de conservation.

12.8.1 Adéquation du SDC

Mesure

Il convient de démontrer que le SDC est composé d'actifs techniques et de mécanismes de sécurité répondant aux besoins des clients et permettant de garantir l'authenticité, la fiabilité et l'exploitation des documents analogiques à dématérialiser, des documents numériques et des archives numériques gérées par ce système.

12.8.2 Description détaillée du SDC

Mesure

Il convient de définir et de maintenir une description détaillée et compréhensible du SDC comprenant les actifs techniques, les aspects fonctionnels et opérationnels ainsi que les flux et les dépendances entre les différentes composantes.

Préconisations de mise en œuvre

Il convient de définir et de maintenir une description détaillée et compréhensible du SDC :

a. en identifiant et en documentant les actifs techniques supportant les processus sous-jacents au processus de dématérialisation ou de conservation, à savoir :
   1. la collecte des documents analogiques ou numériques,
   2. le stockage temporaire de ces documents,
   3. la création de documents numériques ou des archives numériques,
   4. la restitution, le transfert, la destruction éventuelle des documents analogiques, et la suppression des archives numériques ;

b. en identifiant, en évaluant et en documentant de manière régulière les aspects fonctionnels et opérationnels du SDC, comme les suivants :
   1. pour le système de dématérialisation, pour chaque scanneur :
      i. les nombres minimum et maximum de couleurs et les niveaux de gris,
      ii. les nombres minimum et maximum de dpi, de bits par pixel,
      iii. la possibilité de dématérialisation recto/verso ou uniquement verso,
      iv. les différents formats à l'entré, comme A3, A4 et A5,
      v. les méthodes de correction d'images, comme le redressement, la suppression de points isolés, et la suppression des marges,
      vi. les méthodes de compression des images,
      vii. le nombre de documents analogiques ou nombre de pages composant les documents analogiques pouvant être numérisés dans un laps de temps donné ;
   2. pour le système de conservation :
      i. le nombre maximum ou la taille maximum de documents numériques pouvant être transmis en un lot,
      ii. le débit de transmission des documents numériques ou de restitution d'archives numériques,
      iii. les délais de réponse,
      iv. la fréquence d'émission des lots ou de restitutions d'archives numériques,
      v. les protocoles sécurisés de transmission d'informations, de documents numériques et d'archives numériques supportées, comme SFTP, TLS, PPP, L_2TP et IPSec.

c. en documentant sur des schémas l'architecture du réseau, les flux de données entre les actifs, les dépendances entre les actifs.

12.8.3 Mécanismes de sécurité du SDC

Mesure

Il convient de gérer et de documenter les mécanismes de sécurité du SDC permettant d'assurer l'authenticité, la fiabilité et l'exploitation des documents analogiques, des documents numériques et des archives numériques gérés par ce système.

Préconisations de mise en œuvre

Il convient en particulier de gérer les mécanismes de sécurité suivants :

a. Mécanismes de gestion des accès au SDC.

Il convient de protéger les accès aux actifs techniques du SDC, aux documents analogiques, aux documents numériques et aux archives numériques gérés par le SDC en :

1. s'assurant que les conditions d'accès à ces actifs s'appliquent à toute personne physique et à tout actif tentant d'y accéder,
2. assurant une gestion adéquate des comptes des utilisateurs autorisés à accéder au SDC et des comptes techniques des actifs techniques du SDC, avec une capacité de révocation immédiate de ces comptes,
3. en identifiant sans ambigüité les activités et les actions système effectuées et en pouvant les attribuer de façon incontestable à un auteur, par exemple en attribuant des comptes personnels à chaque utilisateur,
4. gérant des mécanismes d'authentification appropriés et sécurisés pour les comptes des utilisateurs autorisés et les comptes techniques des actifs techniques du SDC.

b. Mécanismes de gestion des privilèges.
Il convient d'assurer une gestion des privilèges pour l'ensemble des comptes des utilisateurs du SDC et des comptes techniques des actifs techniques du SDC (voir 6.1.2 et 6.1.6).
c. Mécanismes de surveillance (voir 12.4.3).
d. Mécanismes cryptographiques de sécurité (voir 10.1).
e. Mécanismes de détection et de suppression de codes malveillants contenus dans des documents numériques collectés en vue de leur conservation électronique, si c'est demandé par le client.

Il convient d'utiliser au minimum un antivirus pour vérifier que tous les documents numériques collectés en vue de leur conservation électronique ne contiennent pas de codes malveillants, comme des virus, des chevaux de Troie et des vers de réseau.

Il convient de l'utiliser dès la réception par le SDC des documents numériques et avant le démarrage du processus de création des archives numériques.

f. Mécanismes de suppression sécurisée des documents et archives numériques, comme une réécriture multiple sur les informations ne permettant plus de les retrouver en l'état.
g. Mécanismes de conversion (si nécessaire) des archives numériques dans un format différent de leur format original.

12.8.4 Supervision des aspects opérationnels du SDC

Mesure

Il convient d'évaluer de manière régulière les aspects opérationnels du SDC comme l'espace disponible et les taux d'échecs de composants redondants.

Préconisations de mise en œuvre

Il convient :

a. de définir une liste avec les aspects opérationnels du SDC à contrôler ;
b. de l'inclure dans la liste des éléments nécessaires de surveiller selon les exigences de l'évaluation des performances du système de management (voir ISO/IEC 27001 2013, chapitre 9.1) ;
c. d'établir des indicateurs de disponibilité des caractéristiques opérationnelles, comme les durées de vie des disques.

12.8.5 Contrôle régulier de l'intégrité du SDC

Mesure

Il convient d'implémenter des mécanismes de contrôle régulier de l'intégrité du SDC et des informations nécessaires pour assurer la traçabilité.

Préconisations de mise en œuvre

En ce qui concerne le SDC, il convient de s'assurer que :

a. le fonctionnement du SDC n'a pas été altéré suite à des :
   1. opérations de maintenance ou des mises à jour,
   2. remplacements d'actifs du SDC comme les scanneurs, la plateforme de conservation électronique ou des composants de ces actifs comme les supports de stockage ;

b. les fichiers de configurations du SDC n'ont pas été modifiés de manière non autorisée ;
c. l'intégrité est préservée en ce qui concerne les
   1. documents numériques stockés,
   2. métadonnées associées,
   3. archives numériques,
   4. journaux d'événements.

13 Sécurité des communications

Les objectifs, mesures, préconisations de mise en œuvre et informations supplémentaires de la norme ISO/IEC 27001:2013 s'appliquent sans modification.

14 Acquisition, développement et maintenance des systèmes d'information

14.1 Exigences de sécurité applicables aux systèmes d'information

Des préconisations de mise en œuvre additionnelles sont :

14.1.1 Analyse et spécification des exigences de sécurité de l'information

Préconisations de mise en œuvre

Il convient de s'assurer et de pouvoir démontrer que les applications critiques et les systèmes d'information supportant le SDC sont réalisés en respectant des méthodes de développement sécurisé reconnues.

Il convient d'évaluer et le cas échéant d'instaurer le principe de dépôts des codes source chez un tiers pour toute application du SDC fournie par un fournisseur et nécessaire à assurer l'intégrité et la disponibilité des informations.

15 Relations avec les fournisseurs

15.1 Sécurité de l'information dans les relations avec les fournisseurs

Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :

15.1.4 Conditions contractuelles pour les fournisseurs intervenant dans le processus de dématérialisation et de conservation

Mesure

Il convient d'inclure dans les contrats établis avec chaque fournisseur intervenant dans le processus de dématérialisation et de conservation les conditions assurant le respect de la politique de sécurité et de la politique de dématérialisation et de conservation.

Préconisations de mise en œuvre

Pour tous les fournisseurs supportant les processus de dématérialisation ou de conservation exécutés par l'organisation, il convient d'étudier les conditions suivantes, puis d'inclure les conditions nécessaires pour maitriser les risques liés à l'activité du fournisseur, dans le document contractuel établi avec ce fournisseur :

a. des dispositions quant à la propriété des produits et des services, comme des documents et des applications, fournis par le fournisseur dans le cadre de son support aux processus de dématérialisation ou de conservation exécutés par l'organisation ;
b. des dispositions quant à la continuité de la délivrance des produits et des services fournis par le fournisseur dans le cadre de son support aux processus de dématérialisation ou de conservation exécutés par l'organisation, même en cas de désastre ;
c. le respect de la politique de dématérialisation ou de la politique de conservation de l'organisation ;
d. des mesures garantissant :
    1. une notification dans les plus brefs délais des changements sécuritaires appliqués aux actifs du fournisseur et de ses fournisseurs pouvant impacter les processus de dématérialisation ou de conservation exécutés par l'organisation,
    2. que les informations de l'organisation seront utilisées exclusivement pour les finalités pour lesquelles elles ont été rendues accessibles au fournisseur et à ses fournisseurs,
    3. que les changements de fournisseurs du fournisseur impliqués dans le support des processus de dématérialisation ou de conservation exécutés par l'organisation seront sujets à approbation préalable de l'organisation ;
e. l'engagement du fournisseur à coopérer avec l'organisation dans le cadre d'investigations effectuées par l'organisation pour la résolution d'un incident pouvant impacter les services ou produits fournis à l'organisation par le fournisseur et dont l'origine présumée ou avérée est autre que le fournisseur ou ses fournisseurs ;
f. le droit d'auditer les fournisseurs du fournisseur de manière équivalente à ce dernier et dans le périmètre de leur implication au niveau des processus de dématérialisation ou de conservation exécutés par l'organisation ;
g. la conformité du fournisseur et de ses fournisseurs aux lois et aux règlements en vigueur au Luxembourg ;
h. les points de contact de chaque partie concernée par le document contractuel, d'un point de vue contractuel, opérationnel et de la sécurité de l'information.

16 Gestion des incidents liés à la sécurité de l'information

16.1 Gestion des incidents liés à la sécurité de l'information et améliorations

Des préconisations de mise en œuvre additionnelles sont :

16.1.1 Responsabilités et procédures

Préconisations de mise en œuvre

Il convient de documenter dans une procédure les instructions précisant à partir de quel moment la gestion d'incidents est activée, la restauration est entamée et les autorités ou les clients concernés (internes ou externes à l'organisation) sont avertis de cet incident.

Informations supplémentaires

Voir mesure 6.1.6.

17 Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité

Une catégorie de mesures additionnelle à la norme ISO/IEC 27002:2013 est :

17.3 Continuité de l'activité et du SDC

Objectif : assurer la gestion correcte de la continuité du SDC et des processus de dématérialisation ou de conservation.

17.3.1 Organisation de la continuité

Mesure

Il convient de déterminer les exigences pour la continuité des processus de dématérialisation ou de conservation en cas de situation défavorable, comme lors d'une crise ou d'un sinistre.

Préconisations de mise en œuvre

Il convient de définir pour les actifs dans le périmètre la durée maximale d'interruption admissible (DMIA) (anglais : Return Time on Objective – RTO) et la perte de données maximale admissible (PDMA) (anglais : Recovery Point Objective – RPO) en tenant compte des exigences des clients et de l'obligation de restitution des documents.

Informations supplémentaires

La Norme internationale ISO/IEC 22301:2014 relative à la « Sécurité sociétale – Systèmes de management de la continuité d'activité – Exigences » spécifie les exigences pour planifier, établir, mettre en place et en œuvre, opérer, contrôler, réviser, maintenir et améliorer de manière continue un système de management documenté afin de se protéger des incidents perturbateurs, réduire leur probabilité de survenance, s'y préparer, y répondre et de s'en rétablir lorsqu'ils surviennent. Elle permet à toute organisation, y compris à un PSDC, de concevoir un système de management de la continuité des activités qui soit adapté à ses besoins et qui satisfasse aux exigences des parties intéressées.

17.3.2 Mise en œuvre de la continuité

Mesure

Il convient d'établir, de documenter, de mettre en œuvre et de maintenir les processus, procédures et mesures pour assurer le niveau requis de continuité pendant une situation défavorable.

Préconisations de mise en œuvre

Il convient de définir un processus de reprise d'activé qui inclut les processus de dématérialisation ou de conservation et qui tient compte des exigences des clients, de l'obligation de restitution des documents, et des scénarios de risques qui peuvent interrompre le bon fonctionnement d'une activité.

Il convient de gérer des plans de continuité pour les processus de dématérialisation ou de conservation permettant d'adresser les situations défavorables selon les conditions définies.

Il convient de gérer un plan de reprise de l'activité du SDC permettant d'adresser les situations défavorables selon les conditions définies.

17.3.3 Vérifier, revoir et évaluer la continuité

Mesure

Il convient de vérifier la mise en œuvre des mesures liées à la continuité du SDC à intervalles réguliers pour s'assurer qu'elles sont toujours valides et en vigueur pendant une situation défavorable.

Préconisations de mise en œuvre

Il convient de tester les éléments clés des plans de continuité et des plans de reprises.

18 Conformité

18.1 Conformité aux obligations légales et réglementaires

Des préconisations de mise en œuvre additionnelles sont :

18.1.3 Protection des enregistrements

Préconisations de mise en œuvre

Il convient de conserver les preuves de la conformité des activités effectuées par le personnel concerné par rapport aux politiques et aux procédures liées au processus de dématérialisation ou de conservation exécuté par l'organisation en utilisant des supports de stockage appropriés une conservation aussi longtemps que nécessaire.

En particulier il convient de conserver les preuves suivantes :

a. les rapports d'activités des utilisateurs du SDC,
b. les rapports de mises à jour ou de changement du SDC,
c. les rapports d'événements et d'incidents lié aux processus de dématérialisation ou de conservation,
d. les rapports de revue des journaux d'événements du SDC ;
e. en cas de processus de dématérialisation :
    1. les bordereaux de récupération ou de livraison de documents analogiques ;
f. en cas de processus d'archivage :
    1. les rapports de conversion de documents numériques en archives numériques,
    2. les rapports de conversion d'archives numériques en cas de changements de format.

Il convient qu'une preuve liée aux activités effectuées par le personnel concerné contienne en particulier les informations suivantes :

a. les auteurs des activités effectuées,
b. les dates et heures des activités effectuées,
c. les lieux des activités effectuées,
d. les actifs utilisés pour la réalisation de ces activités,
e. les actifs visés par ces activités,
f. le descriptif des activités effectuées,
g. les problèmes ou erreurs rencontrés pendant la réalisation de ces activités,
h. les clients (interne ou externe) concernés.

18.2 Revue de la sécurité de l'information

Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :

18.2.4 Revue indépendante de la conformité du système et des processus de dématérialisation ou de conservation

Mesure

Il convient de réaliser un audit interne de conformité du SDC afin d'attester de la conformité de son fonctionnement et des activités effectuées par le personnel concerné par rapport à la description détaillée du SDC, par rapport aux spécifications des mécanismes de sécurité, par rapport à la politique de dématérialisation et de conservation, par rapport aux procédures et aux règles définies dans ces procédures et par rapport aux lois et aux règlements en vigueur.

Préconisations de mise en œuvre

Il convient que cette évaluation s'assure :

a. par échantillonnage que les documents analogiques collectés ont été correctement transformés en documents numériques et par la suite détruits ou restitués, et que les documents numériques ont été correctement maintenus, restitués ou entrés dans un processus d'archivage ;
b. par échantillonnage que les documents numériques collectés ont été correctement conservés sous la forme d'archives numériques et par la suite supprimés, et que ces archives ont été correctement créées, maintenues, restituées, transférées ou supprimées ;
c. que les actifs critiques du SDC et les mécanismes de sécurité, comme les mécanismes cryptographiques, ont été évalués et certifiés par des organismes indépendants spécialisés dans ce type de revues ou qu'ils sont conformes à des normes ou des référentiels reconnus et qu'ils sont utilisés conformément aux bonnes pratiques en la matière ;
d. par échantillonnage que les procédures d'administration, d'opérations et de sécurité et des procédures d'exploitation du processus et les règles définies dans ces procédures sont respectées.

Informations supplémentaires

La norme ISO/IEC 27007 intitulé « Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information » fournit des préconisations sur la réalisation des audits de SMSI, ainsi que des lignes directrices sur les compétences des auditeurs, en complément des lignes directrices figurant dans l'ISO 19011, qui sont applicables aux systèmes de management en général.

Une mesure additionnelle à la norme ISO/IEC 27002:2013 est :

18.2.5 Revue indépendante de la sécurité du SDC

Mesure

Il convient de réaliser un audit technique du SDC et des mécanismes de sécurité afin d'attester de la sécurité adéquate du SDC et du fonctionnement correct de ses mécanismes de sécurité indiqué dans la description détaillée du SDC.

Préconisations de mise en œuvre

Il convient que cet audit technique inclut des tests, en particulier des tests d'intrusion et des tests d'escalade de privilèges et une conclusion par une personne expérimentée en test d'intrusion.

Informations supplémentaires

Le rapport technique ISO/IEC TR 27008 intitulé « Lignes directrices pour les auditeurs des contrôles de sécurité de l'information » fournit des préconisations pour la revue de la mise en œuvre et de l'exploitation des mesures de sécurité, y compris le contrôle de la conformité technique des mesures de sécurité. Il explique des techniques pouvant être utilisées pour un tel audit technique. L'audit est en général composé d'un audit de la configuration des systèmes et de l'activité du système pour vérifier le fonctionnement correct de chaque mécanisme de sécurité, d'un test d'intrusion externe, et d'un test d'escalade de privilège.

(1) ISO/IEC 27001:2013 et ISO/IEC 27002:2013.

Annexe A (normative) : Objectifs et mesures de référence spécifiques aux PSDC

Tableau A.1 - Objectifs et mesures

A.5 Politique de sécurité de l'information		
A.5.1 Orientation de la direction en matière de sécurité de l'information		
Objectif: Apporter à la sécurité de l'information une orientation et un soutien de la part de la direction, conformément aux exigences métier et aux lois et règlements en vigueur.		
A.5.1.1	Politiques de sécuirité de l'information	*Mesure* Un ensemble de politiques de sécurité de l'information doit être défini, approuvé par la direction, diffusé et communiqué aux salariés et aux tiers concernés.
QA.5.1.2	Revue des politiques de sécurité de l'informa-	*Mesure* Les politiques de sécurité doivent être revues à intervalles

Les objectifs et les mesures énumérés dans le Tableau A.1 découlent directement de ceux qui sont répertoriés dans le chapitre 5, avec lesquels ils sont en adéquation, et doivent être utilisés dans le contexte du paragraphe 6.1.4. La déclaration d'applicabilité doit justifier, en utilisant la méthode retenue pour l'appréciation et de traitement des risques, l'exclusion de toutes mesures.

Il y a 4 objectifs spécifiques et 34 mesures spécifiques au PSDC dont aucune obligatoire, donc qui ne peuvent pas être exclues par le processus de traitement des risques.

5 Politiques de sécurité de l'information

5.2 Orientations de la direction en matière de politique de dématérialisation ou de conservation

Objectif : Apporter à la gestion des processus de dématérialisation ou de conservation une orientation et un soutien de la part de la direction, conformément aux exigences métier et aux lois et règlements en vigueur.

5.2.1 Politiques de dématérialisation ou de conservation

Une politique de dématérialisation ou de conservation doit être définie, approuvée par la direction, mise en application, diffusée et communiquée aux salariés et aux tiers concernés.

5.2.2 Revue de la politique de dématérialisation ou de conservation

Pour garantir la constance de la pertinence, de l'adéquation et de l'efficacité de politiques des processus de dématérialisation ou de conservation, ces politiques doivent être revues à intervalles programmés et en cas de changements majeurs.

6 Organisation de la sécurité de l'information et des processus de dématérialisation ou de conservation

6.1 Organisation interne

Objectif : Établir un cadre de gestion pour engager, puis vérifier la mise en œuvre et le fonctionnement de la sécurité de l'information et des processus de dématérialisation ou de conservation au sein de l'organisation.

6.1.1 Fonctions et responsabilités liées à la sécurité de l'information et aux processus de dématérialisation ou de conservation

Toutes les responsabilités en matière de sécurité de l'information et des processus de dématérialisation ou de conservation, en particulier celles liées à l'exécution des processus de dématérialisation ou de conservation et celles qui consistent à s'assurer de la conformité des processus et de la gestion opérationnelle aux politiques et aux documents applicables, doivent être établies et d'attribuées.

6.3 Organisation interne spécifique aux processus de dématérialisation et de conservation

Objectif : Établir un cadre de gestion pour assurer le respect des exigences légales spécifiques des processus de dématérialisation ou de conservation au sein de l'organisation.

6.3.1 Vérification des documents numériques avant destruction des documents analogiques correspondants

Une vérification du contenu des documents numériques par rapport aux documents analogiques doit être exercée si la destruction de ces derniers est programmée à la suite de leur numérisation.

6.3.2 Principes du double contrôle pour la modification ou la suppression d'archives numériques

L'organisation doit s'assurer que toute modification ou suppression des archives numériques créées qui n'était pas programmée lors de la définition du projet de conservation nécessite l'approbation de deux utilisateurs autorisés à exécuter ces opérations.

6.3.3 Gestion des preuves

Une gestion adéquate des preuves du fonctionnement du SDC et des activités effectuées par le personnel concerné doit être établie dans une procédure et mise en œuvre.

6.3.4 Relations avec l'autorité nationale

Des procédures doivent être mises en application pour notifier aux autorités compétentes, en particulier l'ILNAS, les prévisions de changements significatifs pouvant impacter la sécurité de l'information et les activités opérationnelles ainsi que, dans les meilleurs délais et en tout état de cause dans un délai de vingt-quatre heures après en avoir eu connaissance, toute atteinte à la sécurité ou toute perte d'intégrité ayant une incidence importante sur le service de dématérialisation ou de conservation.

6.4 Organisation des processus de dématérialisation et de conservation impliquant les clients

Objectif : Clarifier les responsabilités entre le PSDC et ses clients et assurer la transparence en matière de sécurité et d'exploitation des processus de dématérialisation ou de conservation envers les clients.

6.4.1 La sécurité dans les accords avec les clients

Le PSDC doit définir les conditions d'exécution des processus de dématérialisation ou de conservation, ainsi que les besoins de sécurité de l'information associés à ces processus avec le client dans un document contractuel approuvé par le client et le PSDC.

6.4.2 Obligation d'information préalable du client

Préalablement à toute relation contractuelle avec un détenteur, le PSDC doit mettre à disposition, sur un support durable et dans des termes aisément compréhensibles, les informations relatives aux conditions de prestation de service, en particulier toutes les informations légalement requises pour assurer un service transparent.

6.4.3 Classification des actifs du client

Le client doit définir avec le PSDC pour tous ses documents analogiques ou numériques et toutes ses archives numériques le niveau de classification, la durée de rétention, ainsi que les éventuelles autres exigences de sécurité comme les droits d'accès particuliers.

6.4.4 Obligation d'information du client en cas de changements ou d'incidents

Le PSDC doit informer, avant la mise en application ou dans les plus brefs délais, les clients internes ou externes concernés de tout changement des informations préalables et des informations liées aux obligations contractuelles, ainsi que de tout incident pouvant mettre en danger les informations du client, tout en donnant les justifications nécessaires.

7 La sécurité des ressources humaines

7.2 Pendant la durée du contrat

7.2.4 Engagement envers les politiques

Le personnel interne et celui des fournisseurs, s'il est impliqué dans la gestion opérationnelle de la sécurité ou des processus de dématérialisation ou de conservation, doivent comprendre et s'engager par écrit à respecter la politique de sécurité et la politique de dématérialisation ou de conservation.

8. Gestion des actifs

8.1 Responsabilités relatives aux actifs

8.1.4 Cloisonnement d'informations secrètes ou d'informations à caractère personnel

D'éventuelles informations secrètes ou informations à caractère personnel doivent être cloisonnées de façon suffisante pour pouvoir donner suite à la demande du propriétaire de les détruire sans mettre en danger d'autres informations archivées ou les preuves de la bonne gestion pour d'autres informations dématérialisées ou conservées.

9 Contrôle d'accès

9.1 Exigences métier en matière de contrôle d'accès

9.1.3 Ségrégation effective liée aux droits d'accès

Trois personnes différentes doivent être impliquées dans la gestion d'un droit d'accès: une pour l'autorisation de l'accès, une pour la vérification du respect des exigences de sécurité, et finalement une pour l'attribution de l'accès sur les systèmes.

10 Cryptographie

10.1.3 Mesures d'authentification à deux facteurs

Pour les personnes qui interagissent avec les actifs techniques du système de conservation ou qui accèdent aux documents numériques et aux archives numériques, le PSDC doit assurer une authentification appropriée et sécurisée basée sur des mécanismes cryptographiques et, si l'accès est possible à partir de locaux ne requérant pas d'authentification à deux facteurs à l'entrée, une authentification à deux facteurs.

10.1.4 Protection de l'intégrité des documents numériques ou des archives numériques

L'intégrité des documents numériques collectés par le système de conservation et des archives numériques générées par le système de conservation doit être protégée avec des algorithmes et techniques cryptographiques appropriés.

10.1.5 Protection de l'intégrité des documents internes

L'intégrité des documents internes au SDC et aux processus y liés, en particulier les journaux d'événement du SDC, doit être protégée avec des protocoles utilisant des algorithmes et techniques cryptographiques appropriés.

10.1.6 Signature électronique des documents internes

Les utilisateurs du SDC doivent utiliser une signature qualifiée ou un mécanisme apportant une garantie équivalente pour valider les documents internes nécessaires à prouver le bon fonctionnement du SDC et des processus y liés.

10.1.7 Protection des transmissions de documents

La transmission d'informations et de documents numériques doit être protégée avec des protocoles utilisant des algorithmes et techniques cryptographiques appropriés.

10.1.8 Conservation des signatures électroniques

Si l'intégrité d'un document numérique à archiver repose sur une signature électronique, le document doit être conservé avec la preuve que la signature a été vérifiée au plus tard au moment de l'archivage.

11 Sécurité physique et environnementale

11.1 Zones sécurisées

11.1.7 Accompagnement des visiteurs

Un membre du PSDC habilité doit accompagner de manière permanente tous les visiteurs du PSDC, même si l'accès à ces zones leur a déjà été autorisé.

12 Sécurité liée à l'exploitation

12.1 Procédures et responsabilités liées à l'exploitation

12.1.5 Procédures d'exploitation du SDC

Des procédures d'administration, d'opérations du SDC, d'exploitation du processus de dématérialisation ou de conservation, et de contrôle de la sécurité du SDC et des processus incluant toutes les règles à suivre nécessaires pour assurer les propriétés de confidentialité, d'intégrité, de disponibilité, d'authenticité, de fiabilité et l'exploitabilité doivent être définies, mises en œuvre, et suivies par le personnel concerné (du PSDC et des fournisseurs).

12.4.5 Exploitabilité des journaux d'événements

Les journaux d'événements générés doivent être conservés sous une forme exploitable et protégée contre toute manipulation et suppression non autorisées pour assurer une traçabilité aussi longtemps que nécessaire de tous les événements enregistrés par ces mécanismes.

12.8 Gestion correcte et sécurisée du SDC

Objectif : assurer la gestion correcte et sécurisée des documents analogiques à dématérialiser, des documents numériques et des archives numériques dans le cadre du processus de dématérialisation ou de conservation.

12.8.1 Adéquation du SDC

Le PSDC doit démontrer que le SDC est composé d'actifs techniques et de mécanismes de sécurité répondant aux besoins des clients et permettant de garantir l'authenticité, la fiabilité et l'exploitation des documents analogiques à dématérialiser, des documents numériques et des archives numériques gérées par ce système.

12.8.2 Description détaillée du SDC

Une description détaillée et compréhensible du SDC comprenant les actifs techniques, les aspects fonctionnels et opérationnels ainsi que les flux et les dépendances entre les différentes composantes doit être définie et maintenue.

12.8.3 Mécanismes de sécurité du SDC

Le PSDC doit gérer et documenter les mécanismes de sécurité du SDC permettant d'assurer l'authenticité, la fiabilité et l'exploitation des documents analogiques, des documents numériques et des archives numériques gérés par ce système.

12.8.4 Supervision des aspects opérationnels du SDC

Les aspects opérationnels du SDC comme l'espace disponible et les taux d'échecs de composants redondants doivent être évalués de manière régulière.

12.8.5 Contrôle régulier de l'intégrité du SDC

Des mécanismes de contrôle régulier de l'intégrité du SDC et des informations nécessaires pour assurer la traçabilité doivent être implémentés.

15 Relations avec les fournisseurs

15.1 Sécurité de l'information dans les relations avec les fournisseurs

15.1.4 Conditions contractuelles pour les fournisseurs intervenant dans le processus de dématérialisation et de conservation

Le PSDC doit inclure dans les contrats établis avec chaque fournisseur intervenant dans le processus de dématérialisation et de conservation les conditions assurant le respect de la politique de sécurité et de la politique de dématérialisation et de conservation.

17 Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité

17.3 Continuité de l'activité et du SDC

Objectif : assurer la gestion correcte de la continuité du SDC et des processus de dématérialisation ou de conservation.

17.3.1 Organisation de la continuité

Les exigences pour la continuité des processus de dématérialisation ou de conservation en cas de situation défavorable, comme lors d'une crise ou d'un sinistre doivent être déterminées.

17.3.2 Mise en œuvre de la continuité

Les processus, procédures et mesures pour assurer le niveau requis de continuité pendant une situation défavorable doivent être établis, documentés, mis en œuvre et maintenus.

17.3.3 Vérifier, revoir et évaluer la continuité

La mise en œuvre des mesures liées à la continuité du SDC doit être vérifiée à intervalles réguliers pour s'assurer qu'elles sont toujours valides et en vigueur pendant une situation défavorable.

18 Conformité

18.2 Revue de la sécurité de l'information

18.2.4 Revue indépendante de la conformité du système et des processus de dématérialisation ou de conservation

Un audit interne de conformité du SDC doit être réalisé afin d'attester de la conformité de son fonctionnement et des activités effectuées par le personnel concerné par rapport à la description

détaillée du SDC, par rapport aux spécifications des mécanismes de sécurité, par rapport à la politique de dématérialisation et de conservation, par rapport aux procédures et aux règles définies dans ces procédures et par rapport aux lois et aux règlements en vigueur.

18.2.5 Revue indépendante de la sécurité du SDC

Un audit technique du SDC et des mécanismes de sécurité doit être réalisé afin d'attester de la sécurité adéquate du SDC et du fonctionnement correct de ses mécanismes de sécurité indiqué dans la description détaillée du SDC.

JOURNAL OFFICIEL

DU GRAND-DUCHÉ DE LUXEMBOURG

MÉMORIAL A

N° 562 du 14 juin 2017

Institut Luxembourgeois de Régulation - Règlement ILR/T17/4 du 9 juin 2017 portant sur la fixation du plafond tarifaire pour la prestation de terminaison d'appel vocal sur les réseaux mobiles individuels (maché 2/2014) - Secteur communications électroniques.

La Direction de l'Institut Luxembourgeois de Régulation,

Vu la loi du 27 février 2011 sur les réseaux et les services de communications électroniques (« Loi de 2011 »);

Vu la directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques (directive « cadre »);

Vu la directive 2002/19/CE du Parlement européen et du Conseil du 7 mars 2002 relative à l'accès aux réseaux de communications électroniques et aux ressources associées, ainsi qu'à leur interconnexion (directive « accès »);

Vu la directive 2002/22/CE du Parlement européen et du Conseil du 7 mars 2202 concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques (directive « service universel »);

Vu la directive 2009/140/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant les directives 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques, 2002/19/CE du Parlement européen et du Conseil du 7 mars 2002 relative à l'accès aux réseaux de communications électroniques et aux ressources associées, ainsi qu'à leur interconnexion et 2002/20/CE relative à l'autorisation des réseaux et services de communications électroniques;

Vu le règlement 13/168/ILR du 21 août 2013 relatif à la procédure de consultation instituée par l'article 78 de la loi du 27 février 2011 sur les réseaux et les services de communications électroniques;

Vu le règlement 15/190/ILR du 17 mars 2015 complétant la définition des marchés pertinents de la terminaison d'appel vocal sur réseaux mobiles individuels (Marché 7), l'identification des opérateurs puissants sur ces marchés et les obligations imposées à ce titre pour Join Experience S.A. et portant modification du règlement 14/172/ILR sur la définition des marchés pertinents de la terminaison d'appel vocal sur réseaux mobiles individuels (Marché 7), l'identification des opérateurs puissants sur ces marchés et les obligations imposées à ce titre;

Vu le règlement 15/191/ILR du 20 mars 2015 portant fixation du plafond tarifaire pour les prestations de la terminaison d'appel vocal sur les réseaux mobiles individuels (Marché 7/2007) et portant modification du règlement 14/172/ILR sur la définition des marchés pertinents de la terminaison d'appel vocal sur les réseaux mobiles individuels (Marché 7/2007), l'identification des opérateurs puissants sur ces marchés et les obligations imposées à ce titre;

Vu le règlement ILR/T17/3 du 9 juin 2017 portant sur la définition du marché pertinent de la fourniture en gros de terminaison d'appel vocal sur les réseaux mobiles individuels (Marché 2/2014), l'identification des opérateurs puissants sur ce marché et les obligations imposées à ce titre;

Vu la recommandation 2009/396/CE de la Commission du 7 mai 2009 sur le traitement réglementaire des tarifs de terminaison d'appels fixe et mobile dans l'UE;

Vu la recommandation C(2008) 5925 de la Commission du 15 octobre 2008 concernant les notifications, délais et consultations prévus par l'article 7 de la directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques;

Vu la demande d'avis de l'Institut du projet de l'extension de son modèle de coûts concernant la détermination des taux de terminaison d'appel mobile (MTRs) au Luxembourg du 22 janvier 2016 jusqu'au 29 février 2016, le résultat y relatif et la réponse de l'Institut;

Vu la consultation publique nationale relative au projet de règlement portant sur la fixation du plafond tarifaire pour la prestation de terminaison d'appel vocal sur réseaux mobiles individuels (Marché 2/2014) du 21 novembre 2016 au 21 décembre 2016;

Vu les réponses à la consultation publique susvisée;

Vu l'avis du Conseil de la concurrence n°2016-AV-12 du 21 décembre 2016 ;

Vu la consultation publique internationale relative au projet de règlement portant sur la fixation du plafond tarifaire pour la prestation de terminaison d'appel vocal sur réseaux mobiles individuels (Marché 2/2014) du 18 avril 2017 au 18 mai 2017;

Les commentaires des autorités règlementaires de l'Union européenne et de l'ORECE ayant été demandés;

Vu la décision C(2017) 3460 final de la Commission européenne du 16 mai 2017;

Considérant que la documentation concernant le modèle de coûts mobile "Development of a Bottom-Up Mobile Network and Cost Model for the Determination of the Cost of Terminating Calls in Mobile Networks Version 2.0" et le document "Explanatory Memorandum - Regulatory project regarding the determination of the price cap for the provisioning of wholesale voice call termination on individual mobile networks (market 2/2014)" servent notamment de motivation au présent règlement;

Arrête:

Art. 1er.

Les opérateurs identifiés comme puissants sur le marché de la fourniture en gros de terminaison d'appel vocal sur réseaux mobiles individuels (Marché 2/2014) portent à l'égard de l'Institut la charge de la preuve que, sur la base du trafic réel terminé par eux, l'application de leurs tarifs aboutit, en moyenne pondérée annuelle, à des prix au plus égaux au plafond tarifaire tel que déterminé par l'Institut. L'Institut peut à tout moment demander la preuve du respect du plafond tarifaire sur base des prestations fournies et facturées pendant une période déterminée.

Art. 2.

Le plafond tarifaire visé à l'article 1er, calculé en fonction des coûts pur LRIC d'un opérateur générique efficace au Luxembourg sur base du modèle de coûts de l'Institut, s'élève à 0,89 €cts/min pour la période allant jusqu'au 31 décembre 2019. Le plafond tarifaire visé à l'article 1er est applicable à partir de l'entrée en vigueur du présent règlement.

Art. 3.

Le règlement 15/190/ILR du 17 mars 2015 complétant la définition des marchés pertinents de la terminaison d'appel vocal sur réseaux mobiles individuels (Marché 7), l'identification des opérateurs puissants sur ces marchés et les obligations imposées à ce titre pour Join Experience S.A. et portant modification du règlement 14/172/ILR sur la définition des marchés pertinents de la terminaison d'appel vocal sur réseaux mobiles individuels (Marché 7), l'identification des opérateurs puissants sur ces marchés et les obligations imposées à ce titre est abrogé.

Art. 4.

Le règlement 15/191/ILR du 20 mars 2015 portant fixation du plafond tarifaire pour les prestations de la terminaison d'appel vocal sur les réseaux mobiles individuels (Marché 7/2007) et portant modification du règlement 14/172/ILR sur la définition des marchés pertinents de la terminaison d'appel vocal sur les réseaux mobiles individuels (Marché 7/2007), l'identification des opérateurs puissants sur ces marchés et les obligations imposées à ce titre est abrogé.

Art. 5.

Le présent règlement entre en vigueur le premier jour du mois qui suit sa publication au Journal Officiel du Grand-Duché de Luxembourg.

Art. 6.

Le présent règlement sera publié au Journal Officiel du Grand-Duché de Luxembourg et sur le site Internet de l'Institut.

Pour l'Institut Luxembourgeois de Régulation

La Direction

(s.) Michèle Bram	**(s.) Camille Hierzig**	**(s.) Luc Tapella**
Directrice adjointe	***Directeur adjoint***	***Directeur***

JOURNAL OFFICIEL

DU GRAND-DUCHÉ DE LUXEMBOURG

MÉMORIAL A

N° 561 du 14 juin 2017

Institut Luxembourgeois de Régulation - Règlement ILR/T17/3 du 9 juin 2017 portant sur la définition du marché pertinent de la fourniture en gros de terminaison d'appel vocal sur réseaux mobiles individuels (Marché 2/2014), l'identification des opérateurs puissants sur ce marché et les obligations imposées à ce titre - Secteur communications électroniques.

La Direction de l'Institut Luxembourgeois de Régulation,

Vu la loi du 27 février 2011 sur les réseaux et les services de communications électroniques (« Loi de 2011 »);

Vu la directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques (directive « cadre »);

Vu la directive 2002/19/CE du Parlement européen et du Conseil du 7 mars 2002 relative à l'accès aux réseaux de communications électroniques et aux ressources associées, ainsi qu'à leur interconnexion (directive « accès »);

Vu la directive 2002/22/CE du Parlement européen et du Conseil du 7 mars 2002 concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques (directive « service universel »);

Vu la directive 2009/140/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant les directives 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques, 2002/19/CE du Parlement européen et du Conseil du 7 mars 2002 relative à l'accès aux réseaux de communications électroniques et aux ressources associées, ainsi qu'à leur interconnexion et 2002/20/CE relative à l'autorisation des réseaux et services de communications électroniques;

Vu le règlement 13/168/ILR du 21 août 2013 relatif à la procédure de consultation instituée par l'article 78 de la loi du 27 février 2011 sur les réseaux et les services de communications électroniques;

Vu le règlement 14/172/ILR du 6 janvier 2014 portant sur la définition des marchés pertinents de la terminaison d'appel sur réseaux mobiles individuels (Marché 7), l'identification des opérateurs puissants sur ces marchés et les obligations imposées à ce titre;

Vu le règlement 15/190/ILR du 17 mars 2015 complétant la définition des marchés pertinents de la terminaison d'appel vocal sur réseaux mobiles individuels (Marché 7), l'identification des opérateurs puissants sur ces marchés et les obligations imposées à ce titre pour Join Experience S.A. et portant modification du règlement 14/172/ILR sur la définition des marchés pertinents de la terminaison d'appel vocal sur réseaux mobiles individuels (Marché 7), l'identification des opérateurs puissants sur ces marchés et les obligations imposées à ce titre;

Vu le règlement 15/191/ILR du 20 mars 2015 portant fixation du plafond tarifaire pour les prestations de la terminaison d'appel vocal sur les réseaux mobiles individuels (Marché 7/2007) et portant modification du règlement 14/172/ILR sur la définition des marchés pertinents de la terminaison d'appel vocal sur les réseaux mobiles individuels (Marché 7/2007), l'identification des opérateurs puissants sur ces marchés et les obligations imposées à ce titre;

Vu les lignes directrices 2002/C 165/03 de la Commission du 11 juillet 2002 sur l'analyse du marché et l'évaluation de la puissance sur le marché en application du cadre réglementaire communautaire pour les réseaux et les services de communications électroniques;

Vu la recommandation C(2008) 5925 de la Commission du 15 octobre 2008 concernant les notifications, délais et consultations prévus par l'article 7 de la directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques;

Vu la recommandation 2014/710/UE de la Commission du 9 octobre 2014 concernant les marchés pertinents de produits et de services dans le secteur des communications électroniques susceptibles d'être soumis à une réglementation ex ante conformément à la directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques;

Vu la recommandation 2009/396/CE de la Commission du 7 mai 2009 sur le traitement réglementaire des tarifs de terminaison d'appels fixe et mobile dans l'UE;

Vu la consultation publique nationale de l'Institut Luxembourgeois de Régulation (ci-après l'«Institut») relative à l'analyse du marché de la fourniture en gros de terminaison d'appel vocal sur réseaux mobiles individuels (Marché 2/2014) et au projet de règlement afférent du 28 février 2017 au 28 mars 2017;

Vu les réponses à la consultation publique susvisée;

Vu l'accord du Conseil de la concurrence du 27 mars 2017;

Vu la consultation publique internationale relative à l'analyse du marché de la fourniture en gros de terminaison d'appel vocal sur réseaux mobiles individuels (Marché 2/2014) et au projet de règlement afférent du 18 avril 2017 au 18 mai 2017;

Les commentaires des autorités règlementaires de l'Union européenne et de l'ORECE ayant été demandés;

Vu la décision C(2017) 3460 final de la Commission européenne du 16 mai 2017;

Considérant que l'analyse du marché de la fourniture en gros de terminaison d'appel vocal sur réseaux mobiles individuels (Marché 2/2014) telle que soumise à la consultation internationale du 18 avril 2017 au 18 mai 2017 sert notamment de motivation au présent règlement;

Arrête:

Titre I[er] - Définition du marché pertinent et désignation des opérateurs puissants

Art. 1[er].

La dimension géographique du marché de la terminaison d'appel vocal sur les réseaux publics mobiles est nationale.

Art. 2.

(1) Les marchés pertinents sont :

a) le marché de la terminaison d'appel vocal sur le réseau mobile d'e-Lux Mobile Telecommunication Services S.A.;
b) le marché de la terminaison d'appel vocal sur le réseau mobile d'Eltrona Interdiffusion S.A.;
c) le marché de la terminaison d'appel vocal sur le réseau mobile de l'Entreprise des postes et télécommunications;
d) le marché de la terminaison d'appel vocal sur le réseau mobile de Tango S.A.;
e) le marché de la terminaison d'appel vocal sur le réseau mobile d'Orange Communications Luxembourg S.A.;
f) le marché de la terminaison d'appel vocal sur le réseau mobile de Join Experience S.A..

(2) Si un nouvel entrant devenait opérateur de réseau mobile, le marché de la terminaison d'appel vocal sur son réseau mobile deviendrait également un marché pertinent.

(3) Si un « full » MVNO vendait un service de terminaison d'appel vers ses abonnés, le marché de la terminaison d'appel vocal vers ses abonnés deviendrait également un marché pertinent.

(4) Si un « medium » MVNO vendait un service de terminaison d'appel vers ses abonnés, le marché de la terminaison d'appel vocal vers ses abonnés deviendrait également un marché pertinent.

Art. 3.

(1) Les entreprises notifiées suivantes occupent une position équivalente à une position dominante individuelle et sont dès lors désignées comme opérateurs puissants sur le marché de la terminaison d'appel vocal sur leur réseau mobile (ci-après : « opérateur identifié comme puissant ») :

a) e-Lux Mobile Telecommunication Services S.A.;
b) Eltrona Interdiffusion S.A.;
c) Entreprise des Postes et Télécommunications;
d) Join Experience S.A.;
e) Orange Communications Luxembourg S.A.;
f) Tango S.A..

(2) Si un nouvel entrant devenait opérateur de réseau mobile, il occuperait également une position équivalente à une position dominante individuelle et serait dès lors désigné comme opérateur puissant sur le marché de la terminaison d'appel vocal sur son réseau mobile.

(3) Si un « full » MVNO vendait un service de terminaison d'appel vocal vers ses abonnés, il occuperait également une position équivalente à une position dominante individuelle et serait dès lors désigné opérateur identifié comme puissant.

(4) Si un « medium » MVNO vendait un service de terminaison d'appel vocal vers ses abonnés, il occuperait également une position équivalente à une position dominante individuelle et serait dès lors désigné opérateur identifié comme puissant.

Titre II - Fixation des obligations de gros

Chapitre I^{er} : Obligation d'accès

Art. 4.

(1) En vertu des articles 28(1) d) et 32 de la Loi de 2011, les opérateurs identifiés comme puissant sont, à l'égard des demandeurs d'accès et/ou d'interconnexion, soumis à l'obligation de satisfaire les demandes raisonnables de services de terminaison d'appel sur leur réseau mobile et à des ressources associées, ainsi que d'en autoriser l'utilisation. Pour tenir compte du développement technologique, l'obligation de satisfaire les demandes raisonnables d'accès et d'interconnexion ne s'applique pas seulement aux services d'accès et d'interconnexion prévus dans une offre de référence, mais également à ceux qui n'y sont pas prévus.

Chaque opérateur identifié comme puissant exécute son obligation de satisfaire les demandes raisonnables d'accès et/ou d'interconnexion dans le meilleur respect du principe de la neutralité technologique, tel que consacré à l'article 8(1) de la directive « cadre » modifiée.

L'obligation de chaque opérateur identifié comme puissant de satisfaire les demandes raisonnables d'accès et/ou d'interconnexion s'applique à tout le territoire couvert par le réseau de l'opérateur identifié comme puissant concerné, indépendamment de l'origine de l'appel (y compris de l'étranger) et quels que soient notamment :

- l'usage privé ou professionnel de l'utilisateur auquel le service est destiné ;
- la technologie utilisée pour acheminer l'appel.

Des contraintes techniques dûment justifiées ou la nécessité de préserver l'intégrité du réseau peuvent justifier le caractère déraisonnable de la demande d'accès et/ou d'interconnexion et motiver un refus d'accès et/ou d'interconnexion par l'opérateur identifié comme puissant. Toute décision de refus d'accès et/ou d'interconnexion est notifiée à l'Institut parallèlement à l'information y relative du demandeur d'accès et/ou d'interconnexion.

(2) En vertu de l'article 32a) de la Loi de 2011, les opérateurs identifiés comme puissants sont soumis à l'obligation de satisfaire les demandes raisonnables d'accès et/ou d'interconnexion à leur réseau ou à leurs ressources de réseau. Cette obligation comprend les services d'acheminement de l'appel vers les numéros mobiles ainsi que vers des numéros portés, indépendamment de la technologie utilisée et de l'origine de l'appel (y compris les appels en provenance de l'étranger).

(3) En vertu de l'article 32b) de la Loi de 2011, les opérateurs identifiés comme puissants négocient de bonne foi avec les demandeurs d'accès et/ou d'interconnexion.

En ce qui concerne les demandes d'accès et/ou d'interconnexion qui s'inscrivent dans l'offre de référence d'un opérateur identifié comme puissant, ce dernier déploie ses meilleurs efforts pour aboutir à la conclusion d'un accord dans un délai de quinze (15) jours à compter du moment où le demandeur d'accès et/ou d'interconnexion lui a fourni toutes les informations requises pour le traitement de la demande, sauf prorogation décidée d'un commun accord des parties. Suite à la réception de la demande d'accès et/ou d'interconnexion, l'opérateur identifié comme puissant concerné communique sans tarder au demandeur d'accès et/ou d'interconnexion une liste complète et détaillée des informations requises pour le traitement de la demande d'accès et/ou d'interconnexion.

En ce qui concerne les demandes d'accès et/ou d'interconnexion qui ne s'inscrivent pas dans l'offre de référence de l'opérateur identifié comme puissant concerné, ce dernier déploie ses meilleurs efforts pour aboutir à la conclusion d'un accord dans un délai de trois (3) mois à compter de la réception de la demande d'accès et/ou d'interconnexion, sauf prorogation décidée d'un commun accord des parties.

(4) En vertu de l'article 32i) de la Loi de 2011, chaque opérateur identifié comme puissant accorde l'interconnexion en mode IP à son réseau en cas de demande raisonnable d'un opérateur national ou étranger.

L'Institut arrête, après consultation, par règlement les conditions techniques et opérationnelles relatives à l'interconnexion en mode IP. À cette fin, l'Institut peut mettre en place des groupes de travail visant l'élaboration des conditions à utiliser et la concertation entre les opérateurs au sujet de la mise en place pratique de l'interconnexion IP pour la voix.

(5) En vertu de l'article 32e) de la Loi de 2011, les opérateurs identifiés comme puissants accordent un accès ouvert aux interfaces techniques, protocoles ou autres technologies clés qui revêtent une importance essentielle pour l'interopérabilité des services, en ligne avec les évolutions technologiques.

En cas de demande raisonnable d'un demandeur d'accès et/ou d'interconnexion pour le déploiement d'une nouvelle technologie, l'opérateur identifié comme puissant concerné développe, dans un délai raisonnable et de concert avec les bénéficiaires d'accès et/ou d'interconnexion concernés, les paramètres techniques y relatifs et les inclut dans son offre de référence.

En cas de désaccord persistant entre l'opérateur identifié comme puissant concerné et le demandeur d'accès et/ou d'interconnexion sur les paramètres techniques, l'Institut peut, après consultation, imposer les conditions techniques et opérationnelles relatives aux interfaces techniques, protocoles ou autres technologies clés à utiliser.

(6) Conformément à l'article 32c) de la Loi de 2011, les opérateurs identifiés comme puissants sont soumis à l'obligation de ne pas retirer l'accès et/ou l'interconnexion lorsqu'il a déjà été accordé, sous réserve des dispositions qui suivent :

a) Sans préjudice quant aux règles contractuelles de droit commun, un opérateur identifié comme puissant ne peut, en cas de violation alléguée de ses obligations contractuelles par le bénéficiaire d'accès, procéder à un retrait d'accès et/ou d'interconnexion, y inclus une suspension provisoire, seulement après envoi d'une lettre recommandée au bénéficiaire d'accès aux termes de laquelle:
   - ce dernier est mis en demeure de mettre un terme à ladite violation, et
   - le retrait de l'accès et/ou de l'interconnexion accordé est annoncé après l'expiration d'un délai de trente (30) jours suivant la réception de la mise en demeure restée infructueuse.

b) L'opérateur identifié comme puissant informe l'Institut, parallèlement au bénéficiaire d'accès et/ou d'interconnexion, du lancement de la procédure de retrait d'accès et/ou d'interconnexion et des suites qui y seront réservées.
   En cas d'une modification de son réseau, l'opérateur identifié comme puissant concerné met à disposition des solutions d'accès et/ou d'interconnexion de remplacement aux bénéficiaires d'accès et/ou d'interconnexion concernés. Ces solutions de remplacement sont fournies préalablement et présentent des caractéristiques techniques et financières au moins équivalentes aux accès et/ou interconnexions à supprimer ou à modifier.

c) Un litige en cette matière entre un opérateur identifié comme puissant et une ou plusieurs partie(s) concernée(s) peut être soumis à l'Institut conformément à l'article 81 de la Loi 2011 à l'issue duquel l'Institut peut, en tenant dûment compte des circonstances du cas concret lui soumis, fixer un délai plus court.

Chapitre II : Obligation de non-discrimination

Art. 5.

(1) En vertu des articles 28(1)b) et 30 de la Loi de 2011, chaque opérateur identifié comme puissant sur le marché est soumis à des obligations de non-discrimination.

Au titre de ces obligations de non-discrimination, chaque opérateur identifié comme puissant sur le marché applique dans des circonstances équivalentes des conditions équivalentes à toute entreprise notifiée fournissant des services équivalents. Chaque opérateur identifié comme puissant sur le marché fournit à cette entreprise des services et des informations dans les mêmes conditions et avec la même qualité que ceux qu'il assure à ses propres services, filiales et partenaires commerciaux.

Sur demande, chaque opérateur identifié comme puissant sur le marché rapporte la preuve vis-à-vis de l'Institut qu'il n'opère pas de discriminations tarifaires ou non-tarifaires entre les entreprises notifiées et ses propres services de détail, filiales et partenaires commerciaux.

(2) Les conditions tarifaires que chaque opérateur identifié comme puissant sur le marché offre pour ses prestations de gros d'accès et/ou d'interconnexion sont non-discriminatoires, d'une part, par rapport à ses services de détail, filiales et partenaires commerciaux et les demandeurs d'accès et/ou d'interconnexion et, d'autre part, entre les différents demandeurs d'accès et/ou d'interconnexion proprement dits. Ainsi, chaque opérateur identifié comme puissant sur le marché applique des prix de gros pour la fourniture des services identiques aux prix pratiqués pour ses transferts internes ou offerts à ses filiales et partenaires commerciaux. Par rapport aux prix de transferts internes, les prestations de gros offertes aux entreprises notifiées ne donnent pas lieu à une majoration tarifaire due aux frais de leur mise à disposition aux entreprises précitées sur le marché de gros.

(3) Chaque opérateur identifié comme puissant sur le marché offre aux demandeurs d'accès et/ou d'interconnexion les mêmes prestations de gros qu'il fournit à ses propres services de détail, ses filiales et partenaires commerciaux.

(4) Chaque opérateur identifié comme puissant sur le marché met à disposition des demandeurs d'accès et/ou d'interconnexion les informations actuelles et pertinentes au regard des prestations de terminaison d'appel, concernant notamment l'état du développement et de l'évolution technologique, dans les mêmes délais et avec la même qualité qu'elles sont mises à disposition à ses propres services de détail, filiales et partenaires commerciaux.

Chapitre III : Obligation de transparence

Art. 6.

(1) En vertu des articles 28(1)a) et 29 de la Loi de 2011, chaque opérateur identifié comme puissant sur le marché est soumis à des obligations de transparence concernant la fourniture en gros de la terminaison d'appel mobile.

(2) En vertu de l'article 29(1) de la Loi, chaque opérateur identifié comme puissant sur le marché est soumis à l'obligation de publier une offre de référence unique pour la fourniture en gros de la terminaison d'appel mobile.

Cette offre de référence doit être suffisamment détaillée pour garantir que les demandeurs d'accès et/ou d'interconnexion ne sont pas tenus de payer pour des ressources qui ne sont pas nécessaires pour le service demandé. Elle devra ainsi contenir une description des différents services offerts et être répartie en plusieurs éléments en fonction des besoins du marché tout en indiquant les modalités et conditions correspondantes, y compris les tarifs applicables.

Dans le cas d'un « Medium » MVNO, cette offre de référence doit être suffisamment détaillée pour garantir que les demandeurs d'accès et/ou d'interconnexion puissent identifier le/s prestataire/s de service sélectionné/s pour la fourniture de la terminaison d'appel respectivement de l'interconnexion.

L'Institut fixe les modalités de publication de l'offre de référence dans un règlement.

(3) L'offre de référence unique pour la fourniture en gros de la terminaison d'appel à publier par chaque opérateur identifié comme puissant sur le marché contient au moins les éléments suivants:

a) Les conditions techniques et utilisations associées aux services de terminaison d'appel, notamment les interfaces techniques, protocoles ou autres technologies clés qui revêtent une importance essentielle pour l'interopérabilité des services;
b) Pour le « Medium » MVNO, identification sans ambiguïté du/des prestataire/s de service sélectionné/s pour la fourniture de la terminaison d'appel respectivement de l'interconnexion ;
c) Les conditions tarifaires associées aux services de terminaison d'appel;
d) Les conditions d'assistance opérationnelle ou les systèmes logiciels similaires;
e) Les conditions de fourniture, notamment les délais de réponse et les indemnités prévues en cas de non-respect de ces délais;
f) L'information que sans préjudice quant aux règles contractuelles de droit commun, l'opérateur identifié comme puissant sur le marché de la terminaison d'appel vocal sur son réseau mobile ne peut, en cas de violation alléguée des obligations contractuelles par le bénéficiaire d'accès et/ou d'interconnexion, procéder à un retrait d'accès et/ou d'interconnexion, y inclus une suspension provisoire, seulement après l'envoi d'une lettre recommandée au bénéficiaire d'accès et/ou d'interconnexion aux termes de laquelle :
   - ce dernier est mis en demeure de mettre un terme à ladite violation, et
   - le retrait de l'accès et/ou de l'interconnexion accordé est annoncé après l'expiration d'un délai de trente (30) jours suivant la réception de la mise en demeure restée infructueuse.
g) Un glossaire des termes nécessaires aux prestations de gros, ainsi que d'autres éléments concernés.

Chapitre IV : Obligation de récupération des coûts et contrôle des prix

Art. 7.

(1) Conformément à l'article 28(1)e) de la Loi de 2011, chaque opérateur identifié comme puissant sur le marché est soumis à des obligations liées à la récupération des coûts et au contrôle des prix.

(2) Conformément à l'article 33(1) et (2) de la Loi de 2011, chaque opérateur identifié comme puissant sur le marché oriente ses tarifs de gros récurrents et non récurrents de ses prestations de terminaison d'appel mobile en fonction des coûts engendrés par un opérateur efficace hypothétique au Luxembourg.

La méthode de comptabilisation des coûts que l'Institut décide d'appliquer pour le calcul des coûts engendrés par un opérateur efficace hypothétique au Luxembourg pour les prestations d'accès et/ou d'interconnexion susvisées est la méthode de calcul des coûts différentiels à long terme calculés avec un modèle ascendant (Bottom Up pur LRIC) de l'Institut. La description des principes et méthodes de calcul est publiée par l'Institut sur son site internet.

Au moyen de la prédite méthode de calcul des coûts BU pur LRIC, l'Institut calcule pour les prestations d'accès et/ou d'interconnexion susvisées le(s) plafond(s) tarifaire(s) qui sont basés sur l'orientation en fonction des coûts d'un opérateur efficace hypothétique au Luxembourg.

Sur base du principe de l'orientation des prix en fonction des coûts engendrés par un opérateur efficace hypothétique, les tarifs offerts par chaque opérateur identifié comme puissant sur le marché ne dépassent pas les plafonds tarifaires fixés par l'Institut.

Chaque opérateur identifié comme puissant sur le marché porte à l'égard de l'Institut la charge de la preuve que les tarifs de ses prestations d'accès et/ou d'interconnexion susvisées ne dépassent pas les plafonds tarifaires fixés par l'Institut. L'Institut peut à tout moment demander la preuve du respect des plafonds tarifaires sur base des prestations fournies et facturées pendant une période déterminée.

Les tarifs proposés par l'opérateur identifié comme puissant pour les prestations d'accès et/ou d'interconnexion susvisées figurant dans son projet d'offre de référence sont à justifier de manière détaillée à l'égard de l'Institut avec fourniture des pièces afférentes à l'appui.

L'Institut peut exiger la modification des tarifs des prestations d'accès et/ou d'interconnexion susvisées par l'opérateur identifié comme puissant, s'il constate que ceux-ci ne respectent pas les plafonds tarifaires fixés et ne correspondent partant pas à des tarifs orientés en fonction des coûts engendrés par un opérateur efficace hypothétique au Luxembourg.

(3) Par dérogation aux dispositions du paragraphe qui précède, chaque opérateur identifié comme puissant sur le marché est libre de fixer les tarifs de gros récurrents et non récurrents de ses prestations de terminaison d'appel mobile pour les appels en provenance des pays ne faisant pas partie de l'espace économique européen (« EEE »).

Pour éviter des pratiques de contournement, cette dérogation est d'application pour tous les flux de terminaison d'appel, qu'ils soient acheminés par une interconnexion directe ou par le biais d'un opérateur de transit ayant une présence en Europe.

Tous les six mois, l'opérateur puissant sur le marché fournit à l'Institut des informations concernant le trafic émis et reçus vers des opérateurs situés en dehors de l'EEE. En distinguant par pays concerné, chaque opérateur PSM indique ainsi le volume échangé et les tarifs par minute appliqués. Ces informations sont à fournir pour la première fois six mois après l'entrée en vigueur du présent règlement.

Titre III - Dispositions finales et abrogatoires

Art. 8.

(1) Le règlement 14/172/ILR du 6 janvier 2014 portant sur la définition des marchés pertinents de la terminaison d'appel sur réseaux mobiles individuels (Marché 7), l'identification des opérateurs puissants sur ces marchés et les obligations imposées à ce titre, est abrogé.

(2) Le règlement 15/190/ILR du 17 mars 2015 complétant la définition des marchés pertinents de la terminaison d'appel vocal sur réseaux mobiles individuels (Marché 7), l'identification des opérateurs puissants sur ces marchés et les obligations imposées à ce titre pour Join Experience S.A. et portant modification du règlement 14/172/ILR sur la définition des marchés pertinents de la terminaison d'appel vocal sur réseaux mobiles individuels (Marché 7), l'identification des opérateurs puissants sur ces marchés et les obligations imposées à ce titre, est abrogé.

Art. 9.

Le présent règlement entre en vigueur le premier jour du mois qui suit sa publication au Journal Officiel du Grand-Duché de Luxembourg.

Art. 10.

Le présent règlement sera publié au Journal Officiel du Grand-Duché de Luxembourg et sur le site Internet de l'Institut.

Pour l'Institut Luxembourgeois de Régulation
La Direction

Directrice adjointe	*Directeur adjoint*	*Directeur*
(s.) Michèle Bram	**(s.) Camille Hierzig**	**(s.) Luc Tapella**

JOURNAL OFFICIEL

DU GRAND-DUCHÉ DE LUXEMBOURG

MÉMORIAL A

N° 560 du 14 juin 2017

Loi du 13 juin 2017 transposant la directive 2014/40/UE du Parlement européen et du Conseil du 3 avril 2014 relative au rapprochement des dispositions législatives, réglementaires et administratives des États membres en matière de fabrication, de présentation et de vente des produits du tabac et des produits connexes; abrogeant la directive 2001/37/CE; modifiant la loi modifiée du 11 août 2006 relative à la lutte antitabac.

Nous Henri, Grand-Duc de Luxembourg, Duc de Nassau,

Notre Conseil d'Etat entendu;

De l'assentiment de la Chambre des Députés;

Vu la décision de la Chambre des Députés du 1er juin 2017 et celle du Conseil d'Etat du 13 juin 2017 portant qu'il n'y a pas lieu à second vote;

Avons ordonné et ordonnons :

Art. 1er.

L'article 2 de la loi modifiée du 11 août 2006 relative à la lutte antitabac est modifié comme suit :

« 1° le point a) est complété à la fin par la partie de phrase suivante :
« qu'il soit ou non génétiquement modifié, ainsi que les produits destinés à être fumés même s'ils ne contiennent pas de tabac, à la seule exclusion des cigarettes et produits à fumer qui sont destinés à un usage médicamenteux et qui sont présentés comme supprimant l'envie de fumer ou réduisant l'accoutumance au tabac. »

2° à la suite du point f), sont insérés les points g) à v) libellés comme suit :

« g) « produit du tabac sans combustion », un produit du tabac ne faisant appel à aucun processus de combustion, notamment le tabac à mâcher, à priser et à usage oral ;

h) « nouveau produit du tabac », un produit du tabac qui ne relève d'aucune des catégories suivantes : cigarette, tabac à rouler, tabac à pipe, tabac à pipe à eau, cigare, cigarillo, tabac à mâcher, tabac à priser ou tabac à usage oral ;

i) « produit à fumer à base de plantes », un produit à base de végétaux, de plantes aromatiques ou de fruits, ne contenant pas de tabac et pouvant être consommé au moyen d'un processus de combustion ;

j) « produits du tabac à fumer », des produits du tabac qui ne sont pas des produits du tabac sans combustion ;

k) « cigarette électronique », un produit ou tout composant de ce produit ou dispositif, y compris une cartouche, un réservoir et le dispositif dépourvu de cartouche ou de réservoir, qui peut être utilisé, au moyen d'un embout buccal, pour la consommation de vapeur ou l'inhalation de toute substance contenant ou non de la nicotine ; la cigarette électronique pouvant être jetable ou rechargeable au moyen d'un flacon de recharge et un réservoir ou au moyen d'une cartouche à usage unique ;

l) « flacon de recharge », un récipient renfermant un liquide contenant ou non de la nicotine, qui est utilisé pour recharger une cigarette électronique ;

m) « ingrédient », le tabac, un additif, ainsi que toute autre substance ou tout autre élément présent dans un produit fini du tabac ou dans des produits connexes, y compris le papier, le filtre, l'encre, les capsules et les colles ;

n) « émissions », les substances dégagées lorsqu'un produit du tabac ou un produit connexe est utilisé aux fins prévues, telles que les substances contenues dans la fumée ou celles qui sont libérées lors de l'utilisation d'un produit du tabac sans combustion ;

o) « niveau maximal » ou « niveau d'émission maximal », la teneur ou l'émission maximale, y compris égale à zéro, d'une substance présente dans un produit du tabac, mesurée en milligrammes ;
p) « additif », une substance autre que du tabac, qui est ajoutée à un produit du tabac, à son conditionnement unitaire ou à tout emballage extérieur ;
q) « emballage extérieur », tout emballage dans lequel les produits du tabac ou les produits connexes sont mis sur le marché, comprenant une unité de conditionnement ou un ensemble d'unités de conditionnement ; les suremballages transparents ne sont pas considérés comme des emballages extérieurs ;
r) « unité de conditionnement », le plus petit conditionnement individuel d'un produit du tabac ou d'un produit connexe mis sur le marché ;
s) « tabac à pipe à eau », un produit du tabac pouvant être consommé au moyen d'une pipe à eau. Aux fins de la présente loi et des règlements pris en son exécution, le tabac à pipe à eau est réputé être du tabac à fumer. Si un produit peut être utilisé à la fois dans une pipe à eau et comme tabac à rouler, il est réputé être du tabac à rouler ;
t) « arôme caractérisant », une odeur ou un goût clairement identifiable autre que celle ou celui du tabac, provenant d'un additif ou d'une combinaison d'additifs, notamment à base de fruits, d'épices, de plantes aromatiques, d'alcool, de confiseries, de menthol ou de vanille, et qui est identifiable avant ou pendant la consommation du produit du tabac ;
u) « aire de jeux », tout espace spécialement aménagé et équipé pour être utilisé, de façon collective, par des enfants à des fins de jeux ;
v) « fumer », le fait d'aspirer la fumée dégagée par la combustion d'un produit du tabac ou la vapeur d'une cigarette électronique ou de tout autre dispositif de cette nature. »

»

Art. 2.

L'article 3 de la même loi est modifié comme suit :

« 1° Le paragraphe 1er est modifié comme suit :

a) L'alinéa 1er est remplacé par la disposition suivante :

« La publicité en faveur du tabac, de ses produits, de ses ingrédients, des cigarettes électroniques et des flacons de recharge, ainsi que toute distribution gratuite d'un produit du tabac ou d'une cigarette électronique ou d'un flacon de recharge sont interdites. »

b) L'alinéa 2 est remplacé par la disposition suivante :

« Cette interdiction englobe l'utilisation de l'emblème de la marque ou du nom de la marque du tabac ou de produits du tabac ou de la cigarette électronique ou du flacon de recharge ainsi que l'utilisation de toute autre représentation ou mention susceptible de s'y référer sur des objets usuels autres que ceux qui sont directement liés à l'usage du tabac ou de la cigarette électronique. »
2° Au paragraphe 2, le deuxième tiret est remplacé comme suit :
« - la simple indication, sur un véhicule servant ordinairement au commerce du tabac, ou de ses produits ou des cigarettes électroniques et des flacons de recharge, de la dénomination du produit, de sa composition, du nom et de l'adresse du fabricant et, le cas échéant, du distributeur, ainsi que la représentation graphique ou photographique du produit, de son emballage et de l'emblème de la marque.»
3° Au paragraphe 3, le premier tiret est remplacé comme suit :
« - aux publications et services de communication en ligne édités par les organisations professionnelles de producteurs, fabricants et distributeurs des produits du tabac, des cigarettes électroniques et des flacons de recharge réservés à leurs adhérents, ni aux publications professionnelles spécialisées, ni aux services de communication en ligne édités a titre professionnel qui ne sont accessibles qu'aux professionnels de la production, de la fabrication et de la distribution des produits du tabac et des cigarettes électroniques et des flacons de recharge. »
4° Au paragraphe 4, l'alinéa 1er est remplacé par la disposition suivante :
« Les dispositions du paragraphe 1er ne s'appliquent pas à la publicité faite à l'intérieur des débits de tabac. Dans les commerces offrant en vente également des produits ne relevant pas de la présente loi, la présente dérogation ne vaut que dans les surfaces réservées à la vente des produits du tabac ainsi

que des cigarettes électroniques et des flacons de recharge et, dans les commerces ne comportant aucune subdivision en surfaces de vente, à proximité immédiate des étalages exposant des produits du tabac, des cigarettes électroniques ou des flacons de recharge. »

5° Le paragraphe 5 est remplacé comme suit :

« (5) Toute opération de parrainage en faveur du tabac ou de produits du tabac ou de cigarettes électroniques ou de flacons de recharge est interdite. »

»

Art. 3.

Entre les articles 3 et 4 de la même loi sont insérés les articles nouveaux 3*bis* et 3*ter* libellés comme suit :

« **Art. 3*bis*.**

(1) Les fabricants et les importateurs de produits du tabac sont tenus de transmettre, par marque et par type, à la Direction de la santé ; ci-après « la direction » une liste de tous les ingrédients et de leurs quantités utilisés dans la fabrication des produits du tabac, par ordre décroissant du poids de chaque ingrédient inclus dans le produit du tabac, ainsi que les niveaux d'émissions de goudron, de nicotine et de monoxyde de carbone.

Les fabricants ou les importateurs informent également la direction si la composition d'un produit est modifiée de telle sorte que cela a une répercussion sur l'information communiquée au titre du présent article.

Pour un produit du tabac nouveau ou modifié, les informations requises en vertu du présent article sont communiquées avant la mise sur le marché de ce produit.

(2) La liste mentionnée au paragraphe 1er est accompagnée d'une déclaration qui comporte des informations portant notamment sur le statut des ingrédients au regard du règlement (CE) n° 1907/2006 du 18 décembre 2006 et du règlement (CE) n° 1272/2008 du 16 décembre 2008, les données toxicologiques, les effets sur la santé du consommateur, l'effet de dépendance des ingrédients, la raison de l'utilisation des ingrédients, ainsi qu'une description générale des additifs utilisés et leurs propriétés.

(3) Les fabricants et les importateurs de produits du tabac communiquent à la direction les études internes et externes concernant le marché et les préférences des groupes de consommateurs, y compris les jeunes et les fumeurs actuels, en matière d'ingrédients et d'émissions, ainsi que des synthèses d'études en vue du lancement de nouveaux produits. Ils déclarent annuellement, avant la fin du premier trimestre, à la direction le volume de leurs ventes pour l'année écoulée, par marque et par type, exprimé en nombre de cigarettes/cigares/cigarillos ou en kilogrammes.

(4) Au plus tard dix-huit mois après l'inscription d'un additif sur la liste prioritaire établie suivant décision d'exécution prévue à l'article 6 de la directive 2014/40/UE du 3 avril 2014, les fabricants et les importateurs soumettent à la direction les études approfondies qu'ils ont réalisées concernant cet additif.

(5) Les fabricants et importateurs sont tenus de mentionner parmi les informations qu'ils communiquent conformément au paragraphe 1er, celles qu'ils estiment relever du secret commercial.

(6) Pour les substances autres que le goudron, la nicotine, le monoxyde de carbone émises par les cigarettes et pour les substances émises par les produits du tabac autres que les cigarettes, les fabricants et les importateurs indiquent les méthodes de mesure des émissions employées.

Art. 3*ter*.

(1) L'étiquetage des unités de conditionnement, tout emballage extérieur ainsi que le produit du tabac ne peuvent comprendre aucun élément ou dispositif qui :

a) contribue à la promotion d'un produit du tabac ou incite à sa consommation en donnant une impression erronée quant aux caractéristiques, effets sur la santé, risques ou émissions de ce produit ; les étiquettes ne comprennent aucune information sur la teneur en nicotine, en goudron ou en monoxyde de carbone du produit du tabac ;
b) suggère qu'un produit du tabac donné est moins nocif que d'autres ou vise à réduire l'effet de certains composants nocifs de la fumée ou présente des propriétés vitalisantes, énergisantes, curatives, rajeunissantes, naturelles, biologiques ou a des effets bénéfiques sur la santé ou le mode de vie ;

c) évoque un goût, une odeur, tout arôme ou tout autre additif, ou l'absence de ceux-ci ;
d) ressemble à un produit alimentaire ou cosmétique ;
e) suggère qu'un produit du tabac donné est plus facilement biodégradable ou présente d'autres avantages pour l'environnement.

(2) Les unités de conditionnement et tout emballage extérieur ne suggèrent aucun avantage économique au moyen de bons imprimés, d'offres de réduction, de distribution gratuite, de promotion ou d'autres offres similaires.

»

Art. 4.

L'article 4 de la même loi est remplacé comme suit :

«

(1) Chaque unité de conditionnement ainsi que tout emballage extérieur de cigarettes, de tabac à rouler et de tabac à pipe à eau porte un avertissement général, un message d'information et des avertissements sanitaires combinés. Chaque unité de conditionnement ainsi que tout emballage extérieur d'un produit du tabac à fumer autre que les cigarettes, le tabac à rouler et le tabac à pipe à eau porte un avertissement général et un message d'avertissement spécifique.

Le contenu de l'avertissement général, des messages d'information, du message d'avertissement spécifique et des avertissements sanitaires combinés, les langues employées, les modalités d'impression et de présentation, ainsi que la surface des différentes unités de conditionnement et emballages extérieurs visés à l'alinéa 1er couverte par les avertissements et messages sont déterminés par règlement grand-ducal.

(2) Les niveaux d'émissions maximaux de goudron, de nicotine et de monoxyde de carbone sont fixés par règlement grand-ducal qui fixe en outre les méthodes de mesure de ces émissions.

Les mesures des émissions visées à l'alinéa 1er sont vérifiées par le Laboratoire national de santé ou par tout laboratoire agréé par le ministre ayant la Santé dans ses attributions. Ces laboratoires, qui n'appartiennent pas à l'industrie du tabac et ne sont pas contrôlés, ni directement ni indirectement par celle-ci, sont contrôlés par la direction. Un règlement grand-ducal précise les conditions d'agrément et de contrôle de ces laboratoires.

»

Art. 5.

Entre les articles 4 et 5 sont insérés les articles nouveaux 4*bis* à 4*decies* libellés comme suit :

« ***Art. 4bis.***

(1) Les unités de conditionnement de produits du tabac sont revêtus d'un identifiant unique, imprimé ou apposé de façon inamovible et indélébile. Cet identifiant n'est ni dissimulé, ni interrompu et permet d'accéder à des données relatives à la fabrication et aux mouvements de ces produits du tabac.

(2) Les personnes concernées par le commerce des produits du tabac, du fabricant au dernier opérateur avant le premier détaillant, enregistrent l'entrée de toutes les unités de conditionnement en leur possession, ainsi que tous les mouvements intermédiaires et la sortie définitive des unités de conditionnement.

Les personnes qui interviennent dans la chaîne d'approvisionnement des produits du tabac conservent un relevé complet et précis de toutes les opérations concernées.

(3) Les fabricants de produits du tabac fournissent à toutes les personnes concernées par le commerce de ces produits, du fabricant au dernier opérateur avant le premier détaillant, y compris les importateurs, entrepôts et sociétés de transport, l'équipement nécessaire pour enregistrer les produits du tabac achetés, vendus, stockés, transportés ou soumis à toute autre manipulation. Cet équipement permet de lire les données enregistrées et de les transmettre sous forme électronique à une installation de stockage de données.

(4) Les informations qui font partie intégrante de l'identifiant unique prévu au paragraphe 1er, et qui doivent être accessibles électroniquement au moyen d'un lien vers l'identifiant unique, sont précisées

par règlement grand-ducal, de même que les modalités d'impression ou d'apposition du dispositif de sécurité.

Art. 4*ter.*

(1) Les fabricants et les importateurs de produits du tabac concluent un contrat de stockage des données accessibles grâce à l'identifiant unique avec un tiers indépendant, dans le but d'héberger l'installation de stockage des données mentionnée à l'article 4*bis*, paragraphe 3.

(2) Ce tiers indépendant est approuvé par la Commission européenne, qui prend en considération notamment son indépendance et ses capacités techniques. Il en va de même pour le contrat de stockage de données.

(3) L'installation de stockage de données est physiquement située sur le territoire de l'Union européenne. La Commission européenne a pleinement accès à cette installation. Les agents habilités des ministères ayant respectivement la Santé et les Finances dans leurs attributions ont pleinement accès aux installations de stockage situées sur le territoire du Grand-Duché de Luxembourg.

(4) Les activités du tiers indépendant sont contrôlées par un auditeur externe, proposé et rémunéré par le fabricant ou l'importateur, et approuvé par la Commission européenne. L'auditeur externe soumet aux ministres ayant respectivement la Santé et les Finances dans leurs attributions et à la Commission européenne un rapport annuel dans lequel sont en particulier évaluées les irrégularités éventuelles liées à l'accès aux données stockées par le tiers indépendant.

(5) Les informations mentionnées au paragraphe 1er ne peuvent pas être modifiées ou effacées par un opérateur économique concerné par le commerce des produits du tabac. Ces informations sont enregistrées dans des traitements automatisés de données à caractère personnel dans les conditions de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

Art. 4*quater.*

Sur avis de la Commission nationale pour la protection des données, un règlement peut préciser les normes techniques pour la mise en place et le fonctionnement du système d'identification et de traçabilité prévu aux articles 4*bis* et 4*ter*, y compris le marquage à l'aide d'un identifiant unique, l'enregistrement, la transmission, le traitement et le stockage des données et l'accès aux données stockées.

Art. 4*quinquies*.

Outre l'identifiant unique mentionné à l'article 4*bis*, les unités de conditionnements des produits du tabac, mises sur le marché, comportent un dispositif de sécurité infalsifiable, composé d'éléments visibles et invisibles. Le dispositif de sécurité est imprimé ou apposé de façon inamovible et indélébile. Il n'est ni dissimulé, ni interrompu.

Art. 4*sexies*.

Chaque unité de conditionnement des produits du tabac sans combustion ainsi que tout emballage extérieur doit porter un avertissement sanitaire, dont les modalités de présentation, ainsi que les dimensions et le contenu sont précisés par règlement grand-ducal.

Art. 4*septies.*

(1) a) Chaque unité de conditionnement de produits à fumer à base de plantes ainsi que tout emballage extérieur doit porter un avertissement sanitaire, dont le message et les modalités de présentation sont précisés par règlement grand-ducal.

b) Les unités de conditionnement et tout emballage extérieur de produits à fumer à base de plantes ne peuvent comporter aucun des éléments ou dispositifs énoncés à l'article 3*ter*, paragraphe 1er, points a), b) et d), et ne peuvent indiquer que le produit est exempt d'additifs ou d'arômes.

(2) Les fabricants et les importateurs de produits à fumer à base de plantes soumettent à la direction une liste de tous les ingrédients, y compris leurs quantités, qui sont utilisés dans la fabrication desdits produits, par marque et par type. Lorsque la composition d'un produit est modifiée de telle sorte que cette modification a une incidence sur les informations communiquées au titre du présent article, les fabricants et les importateurs sont tenus d'en informer la direction. Les informations requises en vertu du présent article sont communiquées avant la mise sur le marché d'un produit à fumer à base de plantes nouveau ou modifié.

Art. 4*octies.*

(1) Les fabricants et les importateurs de cigarettes électroniques et de flacons de recharge sont tenus de soumettre une notification à la direction concernant tout produit de ce type qu'ils ont l'intention de mettre sur le marché.

(2) La notification visée au paragraphe 1er est soumise sous forme électronique six mois avant la date prévue de mise sur le marché. Une nouvelle notification doit être soumise pour toute modification substantielle du produit.

(3) La notification visée au paragraphe 1er doit contenir, selon qu'elle concerne une cigarette électronique ou un flacon de recharge, les informations suivantes:

a) le nom et les coordonnées du fabricant, d'une personne physique ou morale responsable au sein de l'Union européenne et, le cas échéant, de l'importateur dans l'Union européenne ;
b) une liste de tous les ingrédients contenus dans le produit et des émissions résultant de l'utilisation de ce produit, par marque et par type, avec leurs quantités;
c) les données toxicologiques relatives aux ingrédients et aux émissions du produit, y compris lorsqu'ils sont chauffés, en ce qui concerne en particulier leurs effets sur la santé des consommateurs lorsqu'ils sont inhalés et compte tenu, entre autres, de tout effet de dépendance engendré ;
d) les informations sur le dosage et l'inhalation de nicotine dans des conditions de consommation normales ou raisonnablement prévisibles ;
e) une description des composants du produit, y compris, le cas échéant, du mécanisme d'ouverture et de recharge de la cigarette électronique ou du flacon de recharge ;
f) une description du processus de production, en indiquant notamment s'il implique une production en série, et une déclaration selon laquelle le processus de production garantit la conformité aux exigences du présent article ;
g) une déclaration selon laquelle le fabricant et l'importateur assument l'entière responsabilité de la qualité et de la sécurité du produit lors de sa mise sur le marché et dans des conditions d'utilisation normales ou raisonnablement prévisibles ;
h) la preuve du paiement de la taxe prévue au paragraphe 4.

(4) Une taxe de 5.000 euros est due pour toute notification visée au paragraphe 1er.

La taxe est à acquitter moyennant un versement ou un virement sur un compte bancaire de l'Administration de l'Enregistrement et des Domaines, comprenant indication de l'identité du requérant ainsi que l'objet du virement ou versement.

(5) Lorsque la direction considère que les informations présentées sont incomplètes, elle est habilitée à demander qu'elles soient complétées.

(6) Les fabricants et les importateurs de cigarettes électroniques et de flacons de recharge soumettent chaque année à la direction:

a) des données exhaustives sur les volumes de vente, par marque et par type de produit ;
b) des informations sur les préférences des différents groupes de consommateurs, y compris les jeunes, les non-fumeurs et les principaux types d'utilisateurs actuels;
c) le mode de vente des produits;
d) des synthèses de toute étude de marché réalisée à l'égard de ce qui précède, y compris leur traduction en anglais.

(7) Les fabricants et les importateurs de cigarettes électroniques et de flacons de recharge mettent en place et tiennent à jour un système de collecte d'informations sur tous les effets indésirables présumés de ces produits sur la santé humaine.

Si l'un de ces opérateurs économiques considère ou a des raisons de croire que les cigarettes électroniques ou les flacons de recharge qui sont en sa possession et qui sont destinés à être mis sur le marché ou sont mis sur le marché ne sont pas sûrs, ne sont pas de bonne qualité ou ne sont pas conformes à la présente loi, cet opérateur économique prend immédiatement les mesures correctives nécessaires pour mettre le produit concerné en conformité, le retirer ou le rappeler, le cas échéant.

Dans ces cas, l'opérateur économique est tenu d'informer immédiatement la direction en précisant en particulier les risques pour la santé humaine et la sécurité, toute mesure corrective prise, ainsi que les résultats de ces mesures correctives.

Des informations supplémentaires peuvent être demandées aux opérateurs économiques par la direction sur tout aspect touchant à la sécurité et à la qualité ou à tout effet indésirable éventuel des cigarettes électroniques ou des flacons de recharge.

Art. 4*nonies.*

(1) Le liquide contenant de la nicotine ne peut être mis sur le marché que dans des flacons de recharge spécifiques d'un volume maximal de 10 millilitres, dans des cigarettes électroniques jetables ou dans des cartouches à usage unique. Les cartouches ou les réservoirs ne doivent pas excéder 2 millilitres.

(2) Le liquide contenant de la nicotine ne doit pas contenir de nicotine au-delà de 20 milligrammes par millilitre.

(3) Le liquide contenant de la nicotine ne contient pas d'additifs énumérés à l'article 7, paragraphe 3, points c) à g).

(4) Ne peuvent être utilisés que des ingrédients de haute pureté pour la fabrication du liquide contenant de la nicotine. Les substances autres que les ingrédients visés à l'article 4*octies*, paragraphe 3, point b sont uniquement présentes dans le liquide contenant de la nicotine sous forme de traces, et uniquement lorsque ces traces sont techniquement inévitables au cours de la fabrication.

(5) Seuls peuvent être utilisés dans le liquide contenant de la nicotine, à l'exception de la nicotine, des ingrédients qui, chauffés ou non, ne présentent pas de risques pour la santé humaine.

(6) Les cigarettes électroniques diffusent les doses de nicotine de manière constante dans des conditions d'utilisation normale.

(7) Les cigarettes électroniques et les flacons de recharge qui leur sont associés doivent être munis d'un dispositif de sécurité pour enfants et être inviolables. Ils sont protégés contre le bris et les fuites et sont munis d'un dispositif garantissant l'absence de fuite au remplissage.

(8) Un règlement grand-ducal peut définir les normes techniques relatives au mécanisme de remplissage prévu au paragraphe 7.

Art. 4*decies.*

(1) Les unités de conditionnement des cigarettes électroniques et des flacons de recharge comprennent un dépliant présentant :

a) les consignes d'utilisation et de stockage du produit, et notamment une note indiquant que l'utilisation du produit n'est pas recommandée aux jeunes et aux non-fumeurs;
b) les contre-indications;
c) les avertissements pour les groupes à risque spécifiques;
d) les effets indésirables possibles;
e) l'effet de dépendance et la toxicité;
f) les coordonnées du fabricant ou de l'importateur et d'une personne physique ou morale au sein de l'Union européenne.

(2) Les unités de conditionnement ainsi que tout emballage extérieur des cigarettes électroniques et des flacons de recharge incluent:

a) une liste de tous les ingrédients contenus dans le produit par ordre décroissant de leur poids ;
b) une indication de la teneur en nicotine du produit et la quantité diffusée par dose ;
c) l'indication du numéro de lot ; et

d) une recommandation selon laquelle le produit doit être tenu hors de portée des enfants.

(3) Sans préjudice du paragraphe 2, les unités de conditionnement ainsi que tout emballage extérieur des cigarettes électroniques et des flacons de recharge ne contiennent pas d'éléments ou de dispositifs visés à l'article 3*ter*, à l'exception du paragraphe 1er, points a) et c) de l'article 3*ter*, concernant les informations sur la teneur en nicotine et sur les arômes.

(4) Les unités de conditionnement ainsi que tout emballage extérieur des cigarettes électroniques et des flacons de recharge comportent un avertissement sanitaire dont le message et les modalités de présentation sont précisés par règlement grand-ducal.

»

Art. 6.

A l'article 6, paragraphe 1er, de la même loi, les modifications suivantes sont apportées:

« 1° Au point 11, les termes « dans les autobus des services de transports publics de personnes » sont remplacés par les termes « dans tout moyen collectif de transport de personnes ».
2° Le point 12 est remplacé par la disposition suivante :
« dans les aires de jeux, ainsi que dans toutes les enceintes sportives accueillant des mineurs de moins de 16 ans accomplis, y exerçant une activité sportive ».
3° A la suite du point 18 est inséré le point 19 libellé comme suit :
« dans tout véhicule en présence d'un enfant de moins de douze ans accomplis. »

»

Art. 7.

Les articles 7, 8 et 9 sont remplacés par les dispositions suivantes :

« **Art. 7.**

(1) La mise sur le marché, la vente, la distribution ou l'offre à titre gratuit, la détention en vue de la vente, ainsi que l'importation à des fins commerciales des tabacs à usage oral sont interdites.

(2) La mise sur le marché, la vente, la distribution ou l'offre à titre gratuit de paquets de moins de vingt cigarettes, ainsi que des contenants de moins de trente grammes de tabac à rouler, quel que soit leur conditionnement, sont interdites.

(3) Sont interdites la mise sur le marché, la vente, la distribution ou l'offre à titre gratuit de produits du tabac :

a) contenant un arôme caractérisant particulier ;
b) contenant tout dispositif technique permettant de modifier l'odeur ou le goût des produits du tabac ou leur intensité de combustion ;
c) contenant des vitamines ou d'autres additifs laissant entendre qu'un produit du tabac a des effets bénéfiques sur la santé ou que les risques qu'il présente pour la santé ont été réduits ;
d) contenant de la caféine, de la taurine ou d'autres additifs et stimulants associés à l'énergie et à la vitalité ;
e) contenant des additifs qui confèrent des propriétés colorantes aux émissions de fumée ;
f) contenant des additifs qui facilitent l'inhalation ou l'absorption de nicotine ;
g) contenant des additifs qui, sans combustion, ont des propriétés cancérogènes, mutagènes ou toxiques pour la reproduction humaine ;
h) contenant des arômes dans l'un de leurs composants tels que les filtres, le papier, le conditionnement et les capsules, ou tout dispositif technique permettant de modifier l'odeur ou le goût des produits du tabac concernés ou leur intensité de combustion. Les filtres, le papier et les capsules ne doivent pas contenir de tabac ni de nicotine.

Les produits du tabac autres que les cigarettes et le tabac à rouler sont exemptés des interdictions visées aux points a) et h).

Art. 8.

(1) Les fabricants et les importateurs de nouveaux produits du tabac soumettent une notification à la direction six mois avant la date prévue de mise sur le marché de tels produits. Cette notification est soumise sous forme électronique. Elle est assortie d'une description détaillée du nouveau produit du tabac concerné ainsi que des instructions de son utilisation.

(2) La notification visée au paragraphe 1er doit contenir les informations suivantes :

a) la liste de tous les ingrédients, avec leurs quantités, utilisés dans la fabrication du nouveau produit du tabac et ses émissions et leurs niveaux, conformément à l'article 4;
b) les études scientifiques disponibles sur la toxicité, l'effet de dépendance et l'attractivité du nouveau produit du tabac, en particulier du point de vue de ses ingrédients et de ses émissions ;
c) les études disponibles, leur synthèse et les analyses de marché au sujet des préférences des différents groupes de consommateurs, y compris les jeunes et les fumeurs actuels ;
d) d'autres informations utiles disponibles, notamment une analyse risques/bénéfices du produit, ses effets attendus sur l'arrêt de la consommation de tabac, ses effets attendus sur l'initiation à la consommation de tabac ainsi que des prévisions concernant la perception des consommateurs ;
e) la preuve du paiement de la taxe prévue au paragraphe 4.

(3) Les fabricants et les importateurs de nouveaux produits du tabac soumettent à la direction toute information nouvelle ou actualisée sur les études, recherches et autres informations visées au paragraphe 2, points b) à d). La direction peut exiger des fabricants ou des importateurs de nouveaux produits du tabac qu'ils procèdent à des essais supplémentaires ou qu'ils présentent des informations complémentaires.

(4) Une taxe de 5.000 euros est due pour toute notification visée au paragraphe 1er. La taxe est à acquitter moyennant un versement ou un virement sur un compte bancaire de l'Administration de l'Enregistrement et des Domaines, comprenant indication de l'identité du requérant ainsi que l'objet du virement ou versement.

(5) La mise sur le marché de nouveaux produits du tabac est soumise à autorisation préalable à délivrer par le ministre sur avis de la direction.

Art. 9.

(1) La mise sur le marché, la vente, la détention en vue de la vente et l'importation à des fins commerciales de confiseries et de jouets destinés aux enfants et fabriqués avec la nette intention de donner au produit ou à son emballage l'apparence d'un type de produit du tabac ou d'une cigarette électronique ou d'une recharge sont interdites.

(2) Il est interdit de vendre ou d'offrir gratuitement du tabac et des produits du tabac, ainsi que des cigarettes électroniques et des flacons de recharge à des mineurs âgés de moins de dix-huit ans accomplis.

(3) Tout exploitant d'appareils automatiques de distribution délivrant du tabac et des produits du tabac, ainsi que des cigarettes électroniques et des flacons de recharge, est tenu de prendre des mesures empêchant les mineurs âgés de moins de dix-huit ans accomplis d'avoir accès auxdits appareils.

(4) Tout exploitant d'un débit de tabac ou d'un commerce offrant en vente des produits du tabac, ainsi que des cigarettes électroniques et des flacons de recharge, doit veiller à conserver ces produits de façon à ce que la clientèle ne puisse y avoir accès sans l'aide d'un préposé.

(5) Est interdite la vente à distance de produits du tabac, ainsi que de cigarettes électroniques et de flacons de recharge, y compris lorsque l'acquéreur est situé à l'étranger.

»

Art. 8.

L'article 10 de la même loi est modifié comme suit :

« 1° Le premier alinéa est remplacé comme suit :

« Les infractions aux dispositions des articles 3, 3*bis* paragraphe 1er, 3*ter*, 4*bis* paragraphe 1er, 4*ter* paragraphe 5, 4*quinquies*, 4*sexies*, 4*septies*, 4*octies* paragraphes 1er, 6 et 7, de l'article 4*nonies* et des articles 7, 8 paragraphe 1er et de l'article 9 de la présente loi, ainsi que les infractions aux dispositions du règlement grand-ducal à prendre en vertu de ses articles 4 et 4*sexies*, sont punies d'une amende de 251 à 50.000 euros. »

2° L'alinéa 4 est supprimé.

3° Aux alinéas 5 et 6, la référence aux « alinéas 1 et 4 » est remplacée par celle relative au « premier alinéa ».

»

Art. 9.

A l'article 13 de la loi, premier alinéa, le point 1 est remplacé par la disposition suivante :

« Les producteurs, fabricants et commerçants de tabac, de produits du tabac, de cigarettes électroniques ou de flacons de recharge, ainsi que les exploitants des lieux, à la demande desquels est effectuée la publicité irrégulière.

»

Art. 10.

L'article 14 de la loi est remplacé par la disposition suivante:

« **Art. 14.**

(1) En cas d'infraction aux dispositions des articles 4, 4*sexies* et 4*septies* de la présente loi, sont poursuivis comme auteurs principaux ceux qui fabriquent, mettent sur le marché, importent à des fins commerciales, vendent en gros ou détiennent en vue de la vente en gros des produits du tabac qui :

a) sont dépourvus d'un avertissement sanitaire conforme,
b) sont dépourvus d'un identifiant unique et d'un dispositif de sécurité infalsifiable.

(2) En cas d'infraction aux dispositions de l'article 4*decies* de la même loi, sont poursuivis comme auteurs principaux ceux qui fabriquent, mettent sur le marché, importent à des fins commerciales, vendent en gros ou détiennent en vue de la vente en gros des cigarettes électroniques et des flacons de recharge des produits du tabac qui sont dépourvus d'un avertissement sanitaire conforme.

(3) La vente au détail d'un des produits visés aux paragraphes 1er et 2, non conforme aux prédites dispositions, ainsi que d'un produit du tabac non conforme à l'article 7, paragraphe 3, ne sont pas constitutives d'infraction.

»

Art. 11.

(1) Par dérogation à l'article 4, paragraphe 1er de la loi modifiée du 11 août 2006 relative à la lutte antitabac, les produits du tabac fabriqués ou mis en libre circulation et étiquetés conformément au règlement grand-ducal pris en exécution de l'article 4, paragraphe 1er de la même loi, peuvent être mis sur le marché jusqu'au 20 mai 2017.

(2) Par dérogation aux articles 4*octies* et 4*nonies* de la même loi, les cigarettes électroniques et les flacons de recharge fabriqués ou mis en libre circulation avant le 20 novembre 2016 peuvent être mis sur le marché jusqu'au 28 février 2017.

(3) Toute première déclaration annuelle mentionnée à l'article 3*bis*, paragraphe 3 de la même loi, porte sur les années à partir du 1er janvier 2015.

Art. 12.

La présente loi entre en vigueur le premier jour du deuxième mois qui suit sa publication au Journal officiel du Grand-Duché de Luxembourg, à l'exception :

1. des articles 4*bis*, 4*ter*, 4*quinquies* et 14, paragraphe 1er, point b) de la loi du 11 août 2006 relative à la lutte antitabac, telle que modifiée, qui prennent effet :

a) le 20 mai 2019 pour les cigarettes et le tabac à rouler ;
b) le 20 mai 2024 pour les produits du tabac autres que les cigarettes et le tabac à rouler ; et

2. de l'article 7, paragraphe 3 de la loi du 11 août 2006 relative à la lutte antitabac, telle que modifiée, qui prend effet le 20 mai 2020 pour les produits du tabac contenant un arôme caractérisant particulier, dont le volume des ventes à l'échelle de l'Union européenne représente trois pourcent ou plus dans une catégorie de produits déterminée.

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.

La Ministre de la Santé,
Lydia Mutsch

Le Ministre de la Justice,
Félix Braz

Palais de Luxembourg, le 13 juin 2017.
Henri

Doc. parl. 7030; sess. ord. 2015-2016 et 2016-2017; Dir. 2014/40/UE et 2014/109/UE.

JOURNAL OFFICIEL

DU GRAND-DUCHÉ DE LUXEMBOURG

MÉMORIAL A

N° 559 du 14 juin 2017

Loi du 13 juin 2017 relative aux comptes de paiement et portant :

1. **transposition de la directive 2014/92/UE du Parlement européen et du Conseil du 23 juillet 2014 sur la comparabilité des frais liés aux comptes de paiement, le changement de compte de paiement et l'accès à un compte de paiement assorti de prestations de base; et**
2. **modification de la loi modifiée du 15 décembre 2000 sur les services financiers postaux.**

Nous Henri, Grand-Duc de Luxembourg, Duc de Nassau,

Notre Conseil d'Etat entendu;

De l'assentiment de la Chambre des Députés;

Vu la décision de la Chambre des Députés du 1er juin 2017 et celle du Conseil d'Etat du 13 juin 2017 portant qu'il n'y a pas lieu à second vote;

Avons ordonné et ordonnons :

Chapitre 1er - Définitions, champ d'application et autorité compétente

Art. 1er.

Aux fins de la présente loi, on entend par :

1. « autorité compétente » : une autorité désignée comme autorité compétente par un État membre conformément à l'article 21 de la directive 2014/92/UE du Parlement européen et du Conseil du 23 juillet 2014 sur la comparabilité des frais liés aux comptes de paiement, le changement de compte de paiement et l'accès à un compte de paiement assorti de prestations de base, dénommée ci-après « directive 2014/92/UE ». Est visée au Luxembourg, la Commission de surveillance du secteur financier créée par la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier, dénommée ci-après « CSSF » ;
2. « bénéficiaire » : une personne physique ou morale qui est le destinataire prévu de fonds ayant fait l'objet d'une opération de paiement ;
3. « changement de compte » ou « service de changement de compte » : à la demande du consommateur, soit la communication, d'un prestataire de services de paiement à un autre, d'informations concernant tout ou partie des ordres permanents de virements, des domiciliations de créances récurrentes ou des virements entrants récurrents exécutés sur un compte de paiement, soit le transfert de tout solde positif de ce compte de paiement sur un autre compte, ou les deux, qu'il y ait ou non clôture du premier compte de paiement ;
4. « consommateur » : toute personne physique qui agit à des fins qui n'entrent pas dans le cadre de son activité commerciale, industrielle, artisanale ou libérale ;
5. « consommateur résidant légalement dans l'Union européenne »: toute personne physique qui agit à des fins qui n'entrent pas dans le cadre de son activité commerciale, industrielle, artisanale ou libérale et qui a le droit de résider dans un État membre en vertu du droit de l'Union européenne ou du droit national, y compris les consommateurs qui ne possèdent pas d'adresse fixe et les demandeurs d'asile au titre de la convention de Genève du 28 juillet 1951 relative au statut des réfugiés, de son protocole du 31 janvier 1967 et des autres traités internationaux pertinents ;
6. « contrat-cadre » : un contrat de services de paiement qui régit l'exécution future d'opérations de paiement individuelles et successives et qui peut énoncer les obligations et les conditions liées à l'ouverture d'un compte de paiement ;

7. « compte de paiement » : un compte détenu au nom d'un ou de plusieurs consommateurs et servant à exécuter au moins les opérations de paiement suivantes :
   a) verser des fonds sur un autre compte de paiement ;
   b) retirer des espèces ; et
   c) exécuter des opérations de paiements, y compris des virements, en faveur d'un tiers et être bénéficiaire de telles opérations effectuées par un tiers ;
8. « compte de paiement de base » : un compte de paiement assorti de prestations de base tel que visé à l'article 27, paragraphe 1er ;
9. « dépassement » : un découvert tacitement accepté en vertu duquel un prestataire de services de paiement autorise le consommateur à disposer de fonds qui dépassent le solde courant du compte de paiement du consommateur ou la facilité de découvert convenue ;
10. « domiciliation de créances » ou « domiciliation » : un service de paiement national ou transfrontalier visant à débiter le compte de paiement d'un payeur, lorsque l'opération de paiement est initiée par le bénéficiaire sur la base de l'accord du payeur ;
11. « établissement de crédit » : un établissement de crédit au sens de l'article 4, paragraphe 1er, point 1 du règlement (UE) n°575/2013 du Parlement européen et du Conseil du 26 juin 2013 concernant les exigences prudentielles applicables aux établissements de crédit et aux entreprises d'investissement et modifiant le règlement (UE) n° 648/2012 ;
12. « État membre » : un Etat membre de l'Union européenne. Sont assimilés aux Etats membres de l'Union européenne les Etats parties à l'Accord sur l'Espace économique européen autres que les Etats membres de l'Union européenne, dans les limites définies par cet accord et les actes y afférents ;
13. « facilité de découvert » **:** un contrat de crédit explicite en vertu duquel un prestataire de services de paiement permet au consommateur de disposer de fonds qui dépassent le solde courant du compte de paiement du consommateur ;
14. « fonds » : les billets de banque et les pièces, la monnaie scripturale et la monnaie électronique au sens de l'article 1er, point 23 de la loi modifiée du 10 novembre 2009 relative aux services de paiement ;
15. « frais » : tous les frais et pénalités éventuels dus par le consommateur au prestataire de services de paiement pour, ou en rapport avec, des services liés à un compte de paiement ;
16. « instrument de paiement » : un instrument de paiement au sens de l'article 1er, point 26 de la modifiée du 10 novembre 2009 relative aux services de paiement ;
17. « jour ouvrable » : un jour au cours duquel le prestataire de services de paiement concerné exerce les activités nécessaires à l'exécution d'une opération de paiement ;
18. « opération de paiement » **:** une action, initiée par le payeur ou par le bénéficiaire, consistant à verser, transférer ou retirer des fonds, indépendamment de toute obligation sous-jacente entre le payeur et le bénéficiaire ;
19. « ordre de paiement » : toute instruction donnée par un payeur ou un bénéficiaire à son prestataire de services de paiement demandant l'exécution d'une opération de paiement ;
20. « ordre permanent » : une instruction donnée par le payeur au prestataire de services de paiement qui détient son compte de paiement pour exécuter des virements à intervalles réguliers ou à des dates fixées à l'avance ;
21. « payeur » : une personne physique ou morale qui est titulaire d'un compte de paiement et qui autorise un ordre de paiement à partir de ce compte ou, en l'absence de compte de paiement du payeur, une personne physique ou morale qui donne un ordre de paiement vers le compte de paiement d'un bénéficiaire ;
22. « prestataire de services de paiement » : un prestataire de services de paiement au sens de l'article 4, point 9 de la directive 2007/64/CE du Parlement européen et du Conseil du 13 novembre 2007 concernant les services de paiement dans le marché intérieur, modifiant les directives 97/7/CE, 2002/65/CE, 2005/60/CE, ainsi que 2006/48/CE et abrogeant la directive 97/5/CE ;
23. « prestataire de services de paiement destinataire » : le prestataire de services de paiement auquel les informations nécessaires pour effectuer le changement de compte sont transmises ;
24. « prestataire de services de paiement transmetteur » : le prestataire de services de paiement à partir duquel les informations nécessaires pour effectuer le changement de compte sont transmises ;
25. « service de paiement » : un service de paiement au sens de l'article 1er, point 38 de la loi modifiée du 10 novembre 2009 relative aux services de paiement ;

26. « services liés au compte de paiement »: tous les services liés à l'ouverture, à la gestion et à la clôture d'un compte de paiement, y compris les services de paiement et les opérations de paiement visées à l'article 3, lettre g), de la loi modifiée du 10 novembre 2009 relative aux services de paiement, ainsi que les facilités de découvert et les dépassements ;
27. « support durable » : tout instrument permettant au consommateur de stocker des informations qui lui sont adressées personnellement d'une manière permettant de s'y reporter ultérieurement pendant un laps de temps adapté aux fins auxquelles les informations sont destinées et qui permet la reproduction à l'identique des informations stockées ;
28. « taux d'intérêt créditeur » : le taux de l'intérêt qui est versé au consommateur pour les fonds détenus sur un compte de paiement ;
29. « virement » : un service de paiement national ou transfrontalier, fourni par le prestataire de services de paiement qui détient le compte de paiement du payeur, et consistant à créditer, sur la base d'une instruction du payeur, le compte de paiement d'un bénéficiaire par une opération ou une série d'opérations de paiement réalisées à partir du compte de paiement du payeur.

Art. 2.

La présente loi s'applique aux comptes de paiement.

Art. 3.

(1) La CSSF est l'autorité compétente pour assurer l'application et l'exécution de la présente loi et est à ce titre l'autorité compétente unique servant de point de contact aux fins de la directive 2014/92/UE.

(2) Toutes les personnes exerçant ou ayant exercé une activité pour la CSSF, ainsi que les réviseurs d'entreprises agréés ou experts mandatés par la CSSF, sont tenus au secret professionnel visé à l'article 16 de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier. Ce secret implique que les informations confidentielles qu'ils reçoivent dans l'exercice de leur fonction ne peuvent être divulguées à quelque personne ou autorité que ce soit, excepté sous une forme sommaire ou abrégée, sans préjudice des cas relevant du droit pénal ou de la présente loi.

L'alinéa 1er ne fait pas obstacle à ce que la CSSF échange ou transmette aux autorités compétentes des autres États membres des informations confidentielles dans les limites, sous les conditions et suivant les modalités définies par la présente loi.

(3) La CSSF est compétente pour régler sur une base extrajudiciaire les litiges portant sur les droits et obligations institués par la présente loi conformément aux dispositions du livre 4 du Code de la consommation.

Chapitre 2 - Frais liés aux comptes de paiement

Art. 4.

Le présent chapitre s'applique aux prestataires de services de paiement offrant des comptes de paiement au Luxembourg.

Art. 5.

(1) En temps utile avant de conclure un contrat relatif à un compte de paiement avec un consommateur, les prestataires de services de paiement fournissent au consommateur, sur un support papier ou sur un autre support durable, un document d'information tarifaire qui informe le consommateur sur les frais liés aux services les plus représentatifs rattachés à un compte de paiement.

Un règlement grand-ducal détermine la liste des services les plus représentatifs rattachés à un compte de paiement à figurer dans le document d'information tarifaire, désignée ci-après « liste normalisée ». La liste normalisée intègre, le cas échéant, la terminologie normalisée visée à l'article 3, paragraphe 4 de la directive 2014/92/UE.

La liste normalisée visée à l'alinéa 2 regroupe des services liés à la gestion et tenue du compte de paiement, des services de paiement nationaux et internationaux, des services liés aux découverts ou aux dépassements et des services liés aux instruments de paiement.

(2) Le document d'information tarifaire indique, lorsque ces services sont proposés par le prestataire de services de paiement, les frais correspondants pour chaque service figurant sur la liste normalisée des services.

(3) Le document d'information tarifaire :

1. est un document succinct et distinct ;
2. est présenté et mis en page d'une manière claire et facile à lire, avec des caractères d'une taille lisible ;
3. n'est pas moins compréhensible lorsque, l'original ayant été imprimé en couleurs, il est imprimé ou photocopié en noir et blanc ;
4. est rédigé en luxembourgeois, français ou allemand ou, si le consommateur et le prestataire de services de paiement le décident d'un commun accord, dans une autre langue ;
5. est exact, non trompeur et établi dans la monnaie du compte de paiement ou, si le consommateur et le prestataire de services de paiement le décident d'un commun accord, dans une autre monnaie de l'Union européenne ;
6. comporte, en haut de la première page, l'intitulé « document d'information tarifaire », à côté du symbole commun servant à distinguer ce document de toute autre documentation ;
7. comporte une déclaration précisant qu'il indique les frais afférents aux services les plus représentatifs rattachés au compte de paiement et que des informations précontractuelles et contractuelles complètes sur l'ensemble des services sont données dans d'autres documents.

(4) Lorsqu'un ou plusieurs services sont proposés dans le cadre d'une offre groupée de services liés à un compte de paiement, le document d'information tarifaire indique :

1. les frais facturés pour l'ensemble de l'offre groupée ;
2. les services inclus dans l'offre groupée et leur nombre ;
3. les frais supplémentaires pour tout service excédant le nombre de services inclus dans l'offre groupée et compris dans les frais applicables à cette offre groupée.

(5) Les prestataires de services de paiement mettent à la disposition du consommateur un glossaire comprenant au moins la liste normalisée et les définitions correspondantes. Le glossaire ainsi que d'autres définitions, le cas échéant, sont rédigés dans un langage clair, dénué d'ambiguïté, non technique et non trompeur.

(6) Les prestataires de services de paiement veillent à ce que le document d'information tarifaire et le glossaire soient disponibles à tout moment pour les consommateurs. Ces documents sont mis à disposition sous une forme aisément accessible, y compris pour les personnes qui ne sont pas clientes, dans les locaux du prestataire de services de paiement qui sont accessibles aux consommateurs. Les prestataires de services de paiement disposant d'un site internet mettent ces documents également à disposition desdites personnes sous forme électronique sur leur site internet. Le document d'information tarifaire et le glossaire sont fournis, à titre gratuit, sur un support papier ou sur un autre support durable, à tout consommateur qui en fait la demande.

(7) Le présent article s'applique sans préjudice de l'article 71, point 3 de la loi modifiée du 10 novembre 2009 relative aux services de paiement et du livre 2, titre 2, chapitre 4, section 2 du Code de la consommation.

Art. 6.

(1) Les prestataires de services de paiement fournissent aux consommateurs qui sont leurs clients, au moins une fois par an et à titre gratuit, un relevé de tous les frais encourus ainsi que, le cas échéant, des informations concernant les taux d'intérêt mentionnés au paragraphe 2, points 3 et 4, pour les services liés à leurs comptes de paiement. Les prestataires de services de paiement utilisent, le cas échéant, les termes de la liste normalisée.

(2) Le relevé de frais comporte au moins les informations suivantes :

1. le prix unitaire facturé pour chaque service et le nombre de fois que le service a été utilisé pendant la période considérée et, lorsque les services sont combinés dans une offre groupée, les frais facturés pour l'ensemble de l'offre groupée et le nombre de fois que les frais afférents à l'offre groupée ont été facturés durant la période considérée, ainsi que les frais supplémentaires pour toute prestation excédant le nombre de prestations compris dans les frais applicables à l'offre groupée ;

2. le montant total des frais encourus au cours de la période considérée pour chaque service, chaque offre groupée de services et les prestations excédant le nombre de prestations compris dans les frais applicables à l'offre groupée ;
3. le taux d'intérêt débiteur appliqué au compte de paiement et le montant total des intérêts facturés en lien avec le découvert au cours de la période considérée, le cas échéant ;
4. le taux d'intérêt créditeur appliqué au compte de paiement et le montant total des intérêts versés au cours de la période considérée, le cas échéant ;
5. le montant total des frais facturés pour l'ensemble des services fournis au cours de la période considérée.

(3) Le relevé de frais :

1. est présenté et mis en page d'une manière claire et facile à lire, avec des caractères d'une taille lisible ;
2. est exact, non trompeur et établi dans la monnaie du compte de paiement ou, si le consommateur et le prestataire de services de paiement le décident d'un commun accord, dans une autre monnaie ;
3. comporte, en haut de la première page du relevé, l'intitulé «relevé de frais», à côté du symbole commun servant à distinguer ce document de toute autre documentation ;
4. est rédigé en luxembourgeois, français ou allemand ou, si le consommateur et le prestataire de services de paiement le décident d'un commun accord, dans une autre langue.

(4) Le mode de transmission du relevé de frais est fixé d'un commun accord entre le consommateur et le prestataire de services de paiement. Le relevé de frais est fourni sur un support papier, à tout le moins lorsque le consommateur en fait la demande.

(5) Le présent article s'applique sans préjudice des articles 76 et 77 de la loi modifiée du 10 novembre 2009 relative aux services de paiement et de l'article L. 224-13 du Code de la consommation.

Art. 7.

(1) Les prestataires de services de paiement emploient dans leurs informations contractuelles, commerciales et de marketing destinées aux consommateurs les termes figurant sur la liste normalisée.

Les prestataires de services de paiement peuvent employer dans leurs informations contractuelles, commerciales et de marketing destinées aux consommateurs des noms commerciaux pour désigner leurs services, à condition d'indiquer clairement, le cas échéant, les termes correspondants figurant sur la liste normalisée.

(2) Les prestataires de services de paiement peuvent employer dans le document d'information tarifaire visé à l'article 5, paragraphe 1er et le relevé de frais visé à l'article 6, des noms commerciaux, à condition que de tels noms soient employés en sus de la terminologie figurant sur la liste normalisée et en tant que désignation secondaire de ces services.

Art. 8.

Lorsqu'un compte de paiement est proposé dans le cadre d'une offre groupée comprenant un autre produit ou service qui n'est pas lié à un compte de paiement, les prestataires de services de paiement informent le consommateur de la possibilité d'ouvrir ce compte de paiement séparément et, si tel est le cas, leur fournissent des informations distinctes sur les coûts et frais afférents à chacun des autres produits et services compris dans ladite offre groupée qui peut être acheté séparément.

Art. 9.

La CSSF met en place et gère un site internet comparateur permettant de comparer au moins les frais facturés pour les services figurant sur la liste normalisée.

Le site internet comparateur répond aux conditions suivantes :

1. il recense au moins les frais qui sont facturés aux consommateurs par les prestataires de services de paiement remplissant les critères prévus à l'article 23, paragraphe 1er pour les services figurant sur la liste normalisée. Les prestataires de services de paiement qui ne remplissent pas les critères prévus à l'article 23, paragraphe 1er peuvent demander à la CSSF de recenser également les frais qu'ils facturent aux consommateurs pour les services en question. Avant l'affichage des résultats, une mention claire indique la part de marché couverte par ces résultats ;

2. il est gratuitement mis à disposition des consommateurs et emploie un langage clair et dénué d'ambiguïté et, le cas échéant, les termes figurant sur la liste normalisée ;
3. il est indépendant sur le plan opérationnel en réservant le même traitement aux prestataires de services de paiement concernés dans les résultats de recherches ;
4. il énonce les critères clairs et objectifs selon lesquels la comparaison est effectuée ;
5. il indique clairement que la mise en ligne et la gestion est assurée par la CSSF ;
6. il fournit des informations exactes et mises à jour conformément aux alinéas 3 et 4 et indique la date et l'heure de la dernière mise à jour ;
7. il prévoit une procédure efficace pour signaler les informations inexactes quant aux frais publiés.

Les prestataires de services de paiement visés à l'alinéa 2, point 1 notifient à la CSSF les données requises pour l'application du présent article. Ils notifient à la CSSF spontanément et sans tarder toute modification ayant trait à ces données aux fins de la mise à jour du site internet comparateur.

La CSSF met à jour le site internet comparateur à intervalles réguliers et au moins trimestriellement.

La CSSF ne peut pas être tenue responsable pour le non-affichage d'un changement des frais qui sont facturés aux consommateurs par un prestataire de services de paiement visé à l'alinéa 2, point 1 qui est intervenu après la dernière mise à jour du site internet comparateur.

La CSSF informe les consommateurs sur son site internet de l'existence du site internet comparateur.

Chapitre 3 - Changement de compte de paiement

Art. 10.

Le présent chapitre s'applique aux prestataires de services de paiement offrant des comptes de paiement au Luxembourg.

Art. 11.

Les prestataires de services de paiement proposent un service de changement de compte entre des comptes de paiement tenus dans la même monnaie à tout consommateur qui ouvre ou détient un compte de paiement auprès d'un autre prestataire de services de paiement également situé au Luxembourg, conformément aux dispositions du présent chapitre.

Art. 12.

Le prestataire de services de paiement destinataire initie le service de changement de compte à la demande du consommateur.

Le prestataire de services de paiement destinataire exécute le service de changement de compte après réception de l'autorisation du consommateur. Lorsqu'un compte de paiement a plusieurs titulaires, l'autorisation est obtenue auprès de chacun d'entre eux.

L'autorisation permet au consommateur :

1. d'identifier les virements entrants, les ordres permanents de virement et les mandats de domiciliation qui doivent être transférés ;
2. de donner son accord au prestataire de services de paiement transmetteur pour l'accomplissement de chacune des tâches visées à l'article 13 et au prestataire de services de paiement destinataire pour l'accomplissement de chacune des tâches visées à l'article 15 ;
3. de préciser la date à partir de laquelle les ordres permanents de virement et les mandats de domiciliation doivent être exécutés à partir du compte de paiement ouvert ou détenu auprès du prestataire de services de paiement destinataire. Cette date est fixée à au moins six jours ouvrables à compter de la réception, par le prestataire de services de paiement destinataire, des documents communiqués par le prestataire de services de paiement transmetteur en vertu de l'article 14.

L'autorisation est établie en luxembourgeois, français ou allemand ou, si le consommateur et le prestataire de services de paiement le décident d'un commun accord, dans une autre langue. Le consommateur donne l'autorisation visée au présent article par écrit et une copie lui est remise.

Art. 13.

Dans un délai de deux jours ouvrables à compter de la réception de l'autorisation visée à l'article 12, le prestataire de services de paiement destinataire demande au prestataire de services de paiement transmetteur d'accomplir, pour autant qu'elles soient prévues dans l'autorisation donnée par le consommateur, les tâches suivantes :

1. transmettre au prestataire de services de paiement destinataire et à la demande expresse du consommateur, à ce dernier, la liste des ordres permanents de virement existants et les informations disponibles sur les mandats de domiciliation faisant l'objet du changement ;
2. transmettre au prestataire de services de paiement destinataire et, si cela a été spécifiquement demandé par le consommateur, à ce dernier, les informations disponibles sur les virements entrants récurrents et les domiciliations initiées par le créancier qui ont été effectués sur le compte de paiement du consommateur au cours des treize derniers mois ;
3. cesser d'accepter les domiciliations et les virements entrants avec effet à la date indiquée dans l'autorisation lorsque le prestataire de services de paiement transmetteur ne propose pas de système de réacheminement automatique des virements entrants et des domiciliations vers le compte de paiement détenu par le consommateur auprès du prestataire de services de paiement destinataire ;
4. annuler les ordres permanents avec effet à la date indiquée dans l'autorisation ;
5. transférer sur le compte de paiement ouvert ou détenu auprès du prestataire de services de paiement destinataire tout solde positif éventuel à la date indiquée par le consommateur ;
6. clore le compte de paiement détenu auprès du prestataire de services de paiement transmetteur à la date indiquée par le consommateur.

Art. 14.

Dès la réception de la demande du prestataire de services de paiement destinataire visée à l'article 13, le prestataire de services de paiement transmetteur accomplit, pour autant qu'elles soient prévues dans l'autorisation donnée par le consommateur, les tâches suivantes :

1. transmettre au prestataire de services de paiement destinataire les informations visées à l'article 13, points 1 et 2, dans un délai de cinq jours ouvrables ;
2. cesser d'accepter les domiciliations et les virements entrants sur le compte de paiement avec effet à la date indiquée dans l'autorisation lorsque le prestataire de services de paiement transmetteur ne propose pas de système de réacheminement automatique des virements entrants et des domiciliations vers le compte de paiement ouvert ou détenu par le consommateur auprès du prestataire de services de paiement destinataire. Le prestataire de services de paiement transmetteur informe le payeur ou le bénéficiaire des raisons du refus d'exécuter l'opération de paiement ;
3. annuler les ordres permanents avec effet à la date indiquée dans l'autorisation ;
4. transférer sur le compte ouvert ou détenu auprès du prestataire de services de paiement destinataire tout solde positif éventuel du compte de paiement à la date indiquée dans l'autorisation ;
5. sans préjudice de l'article 74, paragraphe 1er de la loi modifiée du 10 novembre 2009 relative aux services de paiement, clore le compte de paiement à la date indiquée dans l'autorisation si le consommateur n'a pas d'obligations de paiement en suspens liées à ce compte de paiement et pour autant que les tâches énumérées aux points 1 à 3 aient été exécutées. Le prestataire de services de paiement informe immédiatement le consommateur si des obligations en suspens empêchent la clôture de son compte de paiement.

Art. 15.

(1) Dans un délai de cinq jours ouvrables à compter de la réception des informations demandées au prestataire de services de paiement transmetteur visées à l'article 13, le prestataire de services de paiement destinataire, pour autant que l'autorisation le prévoie et selon les modalités prévues dans celle-ci, et dans la mesure où les informations communiquées par le prestataire de services de paiement transmetteur ou le consommateur lui permettent de le faire, accomplit les tâches suivantes :

1. mettre en place les ordres permanents de virement demandés par le consommateur et les exécuter avec effet à la date indiquée dans l'autorisation ;

2. prendre les dispositions nécessaires pour accepter les domiciliations et pour les accepter avec effet à la date indiquée dans l'autorisation ;
3. le cas échéant, informer les consommateurs de leurs droits en vertu de l'article 5, paragraphe 3, lettre d), du règlement (UE) n° 260/2012 du Parlement européen et du Conseil du 14 mars 2012 établissant des exigences techniques et commerciales pour les virements et les prélèvements en euros et modifiant le règlement (CE) n° 924/2009 ;
4. communiquer aux payeurs mentionnés dans l'autorisation et effectuant des virements entrants récurrents sur le compte de paiement d'un consommateur les coordonnées de son compte de paiement auprès du prestataire de services de paiement destinataire et transmettre aux payeurs une copie de l'autorisation donnée par le consommateur. Si le prestataire de services de paiement destinataire ne dispose pas de toutes les informations dont il a besoin pour informer les payeurs, il demande au consommateur ou au prestataire de services de paiement transmetteur de lui fournir les informations manquantes ;
5. communiquer aux bénéficiaires mentionnés dans l'autorisation et utilisant la domiciliation pour percevoir des fonds provenant du compte de paiement du consommateur les coordonnées de son compte de paiement auprès du prestataire de services de paiement destinataire et la date à partir de laquelle les domiciliations doivent être effectuées à partir de ce compte de paiement, et transmettre aux bénéficiaires une copie de l'autorisation donnée par le consommateur. Si le prestataire de services de paiement destinataire ne dispose pas de toutes les informations dont il a besoin pour informer les bénéficiaires, il demande au consommateur ou au prestataire de services de paiement transmetteur de lui fournir les informations manquantes.

(2) Lorsque le consommateur choisit de fournir lui-même les informations visées au paragraphe 1er, points 4 et 5 aux payeurs ou aux bénéficiaires plutôt que de donner son accord spécifique en vertu de l'article 12 au prestataire de services de paiement destinataire pour que celui-ci s'en charge, le prestataire de services de paiement destinataire lui fournit des lettres types indiquant les coordonnées du compte de paiement et la date de début précisée dans l'autorisation, dans le délai prévu au paragraphe 1er.

Art. 16.

Sans préjudice de l'article 82, paragraphe 2 de la loi modifiée du 10 novembre 2009 relative aux services de paiement, le prestataire de services de paiement transmetteur ne bloque pas les instruments de paiement avant la date indiquée dans l'autorisation donnée par le consommateur, afin que la fourniture de services de paiement au consommateur ne soit pas interrompue pendant la procédure de changement de compte.

Art. 17.

(1) Les prestataires de services de paiement transmetteur et destinataire donnent aux consommateurs gratuitement accès aux informations personnelles qu'ils détiennent concernant leurs ordres permanents et leurs domiciliations existantes.

(2) Le prestataire de services de paiement transmetteur fournit les informations demandées par le prestataire de services de paiement destinataire en vertu de l'article 14, point 1, sans facturer de frais ni au prestataire de services de paiement destinataire, ni au consommateur.

(3) Les frais éventuellement facturés par le prestataire de services de paiement transmetteur au consommateur pour la clôture de son compte de paiement sont fixés conformément à l'article 74, paragraphes 2 et 4 de la loi modifiée du 10 novembre 2009 relative aux services de paiement.

(4) Les frais éventuellement facturés au consommateur par le prestataire de services de paiement transmetteur ou destinataire pour tout service fourni au titre des articles 12 à 16, autre que les services visés aux paragraphes 1er à 3 du présent article, sont raisonnables et correspondent aux coûts réels supportés par le prestataire de services de paiement concerné.

Art. 18.

Toute perte financière, y compris les frais et intérêts, subie par le consommateur et résultant directement du non-respect par le prestataire de services de paiement transmetteur ou destinataire des obligations lui incombant au titre des articles 12 à 16, est remboursée sans tarder par le prestataire de services de paiement en question.

Le remboursement prévu à l'alinéa 1er n'est dû ni en cas de force majeure, ni lorsque le prestataire de services de paiement a agi en conformité avec la loi.

Art. 19.

Les prestataires de services de paiement mettent à la disposition des consommateurs les informations suivantes concernant le service de changement de compte :

1. le rôle du prestataire de services de paiement transmetteur et celui du prestataire de services de paiement destinataire lors de chacune des étapes de la procédure de changement de compte, telle qu'elle est prévue aux articles 12 à 16 ;
2. les délais d'accomplissement des différentes étapes ;
3. les frais éventuels facturés pour le changement de compte ;
4. les informations que le consommateur devra éventuellement produire ;
5. la procédure de règlement extrajudiciaire des litiges visée à l'article 3, paragraphe 3 ;
6. des informations sur les différents éléments de l'autorisation visée à l'article 12.

Ces informations sont mises à disposition gratuitement sur un support papier ou sur un autre support durable dans tous les locaux du prestataire de services de paiement accessibles aux consommateurs. Les prestataires de services de paiement rendent attentifs les consommateurs manifestant un intérêt de procéder à un changement de compte à la faculté d'utiliser le service de changement de compte proposé par les prestataires de services de paiement conformément aux dispositions du présent chapitre ainsi qu'à la disponibilité des informations visées à l'alinéa 1er.

Les informations visées à l'alinéa 1er sont fournies aux consommateurs sur demande. Les prestataires de services de paiement disposant d'un site internet mettent ces informations à disposition à tout moment sous forme électronique sur leur site internet.

Art. 20.

(1) Lorsqu'un consommateur indique à son prestataire de services de paiement qu'il souhaite ouvrir un compte de paiement auprès d'un prestataire de services de paiement situé dans un État membre autre que le Luxembourg, le prestataire de services de paiement auprès duquel le consommateur détient un compte de paiement fournit au consommateur, dès réception d'une telle demande, l'assistance suivante :

1. la fourniture gratuite au consommateur d'une liste de tous les ordres permanents de virement et de tous les mandats de domiciliation initiés par le débiteur actuellement actifs, lorsque ceux-ci sont disponibles, et les informations disponibles concernant les virements entrants récurrents et les domiciliations initiées par le créancier récurrentes qui ont été effectués sur le compte de paiement du consommateur au cours des treize derniers mois ;
2. le transfert de tout solde positif éventuel du compte de paiement détenu par le consommateur sur le compte de paiement ouvert ou détenu par le consommateur auprès du nouveau prestataire de services de paiement, pour autant que la demande comporte tous les renseignements permettant d'identifier le nouveau prestataire de services de paiement et le compte de paiement du consommateur ;
3. la clôture du compte de paiement détenu par le consommateur.

(2) Sans préjudice de l'article 74, paragraphe 1er de la loi modifiée du 10 novembre 2009 relative aux services de paiement, et si le consommateur n'a pas d'obligations de paiement en suspens liées à son compte de paiement, le prestataire de services de paiement auprès duquel le consommateur détient ledit compte de paiement accomplit les étapes décrites au paragraphe 1er à la date indiquée par le consommateur, qui correspond à au moins six jours ouvrables après la réception par ce prestataire de services de paiement de la demande du consommateur qu'il souhaite ouvrir un compte de paiement auprès d'un prestataire de services de paiement situé dans un État membre autre que le Luxembourg, sauf accord contraire entre les parties. Le prestataire de services de paiement informe immédiatement le consommateur si des obligations en cours empêchent la clôture de son compte de paiement.

Chapitre 4 - Accès au compte de paiement et droit au compte de paiement de base

Art. 21.

Le présent chapitre s'applique aux établissements de crédit et aux prestataires de services de paiement visés à l'article 1er, point 37, lettre iii) de la loi modifiée du 10 novembre 2009 relative aux services de paiement, qui offrent des services au Luxembourg, désignés ci-après « établissements concernés ».

Art. 22.

Les établissements concernés n'opèrent aucune discrimination à l'encontre des consommateurs résidant légalement dans l'Union européenne du fait de leur nationalité ou de leur lieu de résidence, ou pour tout autre motif visé à l'article 21 de la charte des droits fondamentaux de l'Union européenne, lorsque ces consommateurs font une demande d'ouverture d'un compte de paiement ou accèdent à un tel compte. Les conditions applicables à la détention d'un compte de paiement de base ne sont en aucun cas discriminatoires.

Art. 23.

(1) Les établissements concernés qui remplissent au Luxembourg chacune des conditions suivantes doivent offrir aux consommateurs des comptes de paiement de base :

1. l'établissement concerné dispose d'au moins 25 agences au Luxembourg ;
2. l'établissement concerné détient au moins 2,5 pour cent des dépôts garantis tels que définis à l'article 1er, point 36 de la loi modifiée du 18 décembre 2015 relative à la défaillance des établissements de crédit et de certaines entreprises d'investissement, détenus par l'ensemble des établissements concernés établis au Luxembourg.

La CSSF dresse et publie sur son site internet la liste qui reprend les établissements concernés visés à l'alinéa 1er. Cette liste est revue annuellement.

(2) Les consommateurs résidant légalement dans l'Union européenne, y compris les consommateurs qui n'ont pas de permis de séjour mais dont l'expulsion est impossible pour des raisons légales ou pratiques, ont le droit d'ouvrir auprès des établissements concernés visés au paragraphe 1er un compte de paiement de base et ont le droit de l'utiliser, indépendamment de leur lieu de résidence.

(3) L'accès à un compte de paiement de base n'est pas subordonné à l'achat de services supplémentaires ou d'actions des établissements concernés visés au paragraphe 1er, sauf si cette dernière obligation s'applique à tous les clients de ces établissements concernés.

(4) Les établissements concernés peuvent rejeter la demande d'ouverture d'un compte de paiement de base lorsque le consommateur détient déjà auprès d'un établissement concerné situé au Luxembourg un compte de paiement qui lui permet d'utiliser les services énumérés à l'article 27, paragraphe 1er, sauf lorsque le consommateur déclare avoir été averti que ce compte de paiement allait être clos.

Afin de vérifier si le consommateur détient déjà ou non un compte de paiement auprès d'un établissement concerné situé au Luxembourg qui lui permet d'utiliser les services énumérés à l'article 27, paragraphe 1er, l'établissement concerné peut, avant d'ouvrir un compte de paiement de base, se fonder sur une déclaration sur l'honneur signée à cette fin par le consommateur.

(5) Les établissements concernés rejettent une demande d'ouverture de compte de paiement de base :

1. s'il s'avère que les informations données par le consommateur en vue de l'ouverture du compte sont inexactes ou trompeuses ;
2. s'ils suspectent, sur base d'indices probants ou concordants, que le compte serait utilisé à des fins illégales.

Les établissements concernés peuvent rejeter une demande d'ouverture de compte de paiement de base lorsque le consommateur a commis une infraction pénale à l'encontre de l'établissement concerné, d'un employé ou préposé de l'établissement.

Art. 24.

Les établissements concernés rejettent une demande d'ouverture de compte de paiement de base lorsque l'ouverture ou le fonctionnement d'un tel compte entraînerait une violation de la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme.

Art. 25.

Les établissements concernés qui proposent des comptes de paiement de base ouvrent le compte de paiement de base ou rejettent une demande d'ouverture d'un tel compte présentée par un consommateur, dans les deux cas sans délai indu et au plus tard dans les dix jours ouvrables à compter de la réception d'une demande complète.

Art. 26.

En cas de rejet d'une demande d'ouverture d'un compte de paiement de base en vertu de l'article 23, paragraphe 4 ou de l'article 24, les établissements concernés, dès qu'ils ont pris leur décision, informent immédiatement le consommateur du refus et du motif précis de celui-ci, par écrit et gratuitement, à moins que cette communication d'informations ne soit contraire aux objectifs de sécurité nationale et de maintien de l'ordre public ou à la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme.

Les établissements concernés informent le consommateur de la procédure à suivre pour contester le refus et de son droit de saisir la CSSF et lui communiquent les coordonnées utiles.

Art. 27.

(1) Les comptes de paiement de base visés au présent chapitre comportent les services suivants :

1. des services permettant d'effectuer toutes les opérations requises pour l'ouverture, la gestion et la clôture d'un compte de paiement ;
2. des services permettant de verser des fonds sur un compte de paiement ;
3. des services permettant de retirer des espèces dans l'Union européenne à partir d'un compte de paiement, au guichet ou aux distributeurs automatiques pendant les heures d'ouverture des établissements concernés ou en dehors de celles-ci ;
4. des services permettant d'effectuer dans l'Union européenne les opérations de paiement suivantes :
   a) les domiciliations ;
   b) les opérations de paiement au moyen d'une carte de paiement, y compris les paiements en ligne ;
   c) les virements, y compris les ordres permanents, effectués, lorsqu'ils sont disponibles, aux terminaux, aux guichets et par l'intermédiaire des services en ligne des établissements concernés.

Les services énumérés à alinéa 1er sont proposés par les établissements concernés dans la mesure où ceux-ci les proposent déjà aux consommateurs titulaires d'un compte de paiement autre qu'un compte de paiement de base.

Les établissements concernés peuvent accorder une facilité de découvert liée à un compte de paiement de base.

(2) Le compte de paiement de base est proposé au moins en euros.

(3) Le compte de paiement de base permet au consommateur d'effectuer un nombre illimité d'opérations en rapport avec les services visés au paragraphe 1er.

(4) Pour les services visés au paragraphe 1er, points 1 à 3 et point 4, lettre b), à l'exclusion des opérations de paiement effectuées au moyen d'une carte de crédit, les établissements concernés ne facturent pas de frais au-delà des frais raisonnables éventuels visés à l'article 28, indépendamment du nombre d'opérations effectuées sur le compte de paiement de base.

(5) Les établissements concernés veillent à ce que le consommateur puisse gérer et initier des opérations de paiement à partir de son compte de paiement de base dans les locaux de l'établissement concerné et, le cas échéant, par l'intermédiaire de services en ligne.

Art. 28.

Les établissements concernés proposent aux consommateurs les services visés à l'article 27 à titre gratuit ou moyennant des frais raisonnables.

Ces frais raisonnables sont fixés en tenant au moins compte des niveaux des revenus nationaux et des frais moyens facturés par les établissements concernés au Luxembourg pour les services proposés en liaison avec un compte de paiement.

Art. 29.

(1) Sans préjudice des paragraphes 2 et 3, les contrats-cadres donnant accès à un compte de paiement de base sont soumis à la loi modifiée du 10 novembre 2009 relative aux services de paiement.

(2) Les établissements concernés ne peuvent résilier unilatéralement un contrat-cadre que si au moins une des conditions suivantes est remplie :

1. le consommateur a délibérément utilisé son compte de paiement à des fins illégales ;
2. il n'y a eu aucune opération sur le compte de paiement pendant plus de vingt-quatre mois consécutifs ;
3. le consommateur a fourni des informations inexactes pour obtenir un compte de paiement de base, alors que des informations exactes auraient conduit à l'absence d'un tel droit ;
4. le consommateur n'est plus un consommateur résidant légalement dans l'Union européenne ;
5. le consommateur a ultérieurement ouvert un deuxième compte de paiement qui lui permet d'utiliser les services énumérés à l'article 27 au Luxembourg.

(3) Lorsqu'un établissement concerné résilie le contrat relatif à un compte de paiement de base pour un ou plusieurs des motifs figurant au paragraphe 2, points 2, 4 et 5, il informe le consommateur, par écrit et gratuitement, des motifs et de la justification de cette résiliation au moins deux mois avant que celle-ci n'entre en vigueur, à moins que cela ne soit contraire aux objectifs de sécurité nationale ou de maintien de l'ordre public.

Lorsque l'établissement concerné résilie le contrat conformément au paragraphe 2, point 1 ou 3, la résiliation prend effet immédiatement.

(4) Le consommateur est informé dans la notification de résiliation de la procédure à suivre pour contester la résiliation, le cas échéant, ainsi que de son droit de saisir la CSSF. Les coordonnées de la CSSF lui sont communiquées à cette fin.

(5) Les frais facturés au consommateur en cas de non-respect des engagements qu'il a pris dans le contrat-cadre sont raisonnables.

Ces frais raisonnables sont fixés en tenant au moins compte des niveaux des revenus nationaux et des frais moyens facturés par les établissements concernés au Luxembourg pour les services proposés en liaison avec un compte de paiement.

Art. 30.

(1) La CSSF prend des mesures adéquates pour faire connaître au public l'existence des comptes de paiement de base, leurs conditions tarifaires générales, les procédures à suivre pour exercer le droit d'accès à un compte de paiement de base et les voies d'accès à la procédure de règlement extrajudiciaire des litiges. Elle veille à ce que les mesures de communication soient suffisantes et bien ciblées, et touchent en particulier les consommateurs non bancarisés, vulnérables et mobiles.

(2) Les établissements concernés qui proposent des comptes de paiement de base mettent gratuitement à la disposition des consommateurs des informations accessibles et une aide sur les caractéristiques spécifiques des comptes de paiement base qui leur sont proposés, sur les frais associés à ces comptes et sur les

conditions d'utilisation. Les informations indiquent clairement que l'achat de services supplémentaires n'est pas obligatoire pour avoir accès à un compte de paiement de base.

Chapitre 5 - Sanctions et pouvoirs de l'autorité compétente

Art. 31.

Aux fins de l'application de la présente loi, la CSSF est investie de tous les pouvoirs de surveillance, d'inspection et d'enquête nécessaires à l'exercice de ses fonctions.

Les pouvoirs de la CSSF incluent le droit :

1. de demander aux prestataires de services de paiement toute information utile à l'accomplissement de ses fonctions et missions dévolues par la présente loi ;
2. de prendre inspection des livres, comptes, registres ou autres actes et documents des prestataires de services de paiement ;
3. de procéder à des inspections sur place auprès les prestataires de services de paiement ;
4. d'enjoindre de cesser toute pratique contraire aux dispositions de la présente loi ;
5. de transmettre des informations au Procureur d'Etat en vue de poursuites pénales.

Art. 32.

(1) La CSSF peut sanctionner :

1. les prestataires de services de paiement au cas où ils ne respectent pas :
   a) les dispositions des articles 4 à 8 du chapitre 2 relatif aux frais liés aux comptes de paiement ;
   b) les dispositions des articles 10 à 20 du chapitre 3 relatif au changement de compte de paiement ;
2. les prestataires de services de paiement au cas où ils refusent de fournir les documents ou autres renseignements demandés, nécessaires à la CSSF pour les besoins de l'application de la présente loi ;
3. les prestataires de services de paiement au cas où ils ont fourni des documents ou autres renseignements qui se révèlent être incomplets, inexacts ou faux ;
4. les prestataires de services de paiement au cas où ils font obstacle à l'exercice des pouvoirs de surveillance, d'inspection et d'enquête de la CSSF ;
5. les établissements concernés visés à l'article 21, au cas où ils ne respectent pas les dispositions des articles 21 à 29 et 30, paragraphe 2 du chapitre 4 relatif à l'accès au compte de paiement et au droit au compte de paiement de base ;
6. les prestataires de services de paiement qui ne donnent pas suite aux injonctions de la CSSF prononcées en vertu de l'article 31, alinéa 2, point 4.

(2) Peuvent être prononcés par la CSSF, classés par ordre de gravité :

1. un avertissement ;
2. un blâme ;
3. une amende administrative dont le montant ne peut être ni inférieur à 251 euros, ni supérieur à 250.000 euros ;
4. l'interdiction limitée dans le temps ou définitive de proposer des comptes de paiement aux consommateurs.

Dans le prononcé de la sanction, la CSSF tient compte de la nature, de la durée et de la gravité de l'infraction, de la conduite et des antécédents du prestataire de services de paiement, du préjudice causé aux tierces personnes et des avantages ou gains potentiels ou effectivement tirés de l'infraction.

(3) La CSSF peut publier sur son site internet les sanctions prononcées en vertu du présent article, à moins que cette publication ne risque de perturber gravement les marchés financiers ou de causer un préjudice disproportionné aux parties en cause.

Toute information publiée en vertu de l'alinéa 1er demeure sur le site internet de la CSSF pendant cinq ans à partir de la publication.

Art. 33.

Toute décision prise par la CSSF en vertu de la présente loi peut être déférée dans le délai d'un mois à compter de la notification de la décision, sous peine de forclusion, au tribunal administratif qui statue comme juge du fond.

Chapitre 6 - Coopération avec les autorités compétentes des autres Etats membres

Art. 34.

(1) La CSSF coopère avec les autorités compétentes des autres Etats membres chaque fois que cela est nécessaire à l'accomplissement des missions qui lui incombent en vertu de la présente loi et qui incombent aux autorités compétentes des autres Etats membres en vertu de la directive 2014/92/UE, en faisant usage des pouvoirs qui lui sont conférés par la présente loi et ladite directive.

La CSSF prête son concours aux autorités compétentes des autres Etats membres notamment en échangeant des informations aux fins de la directive 2014/92/UE avec ces autorités et en coopérant dans le cadre d'enquêtes ou d'activités de surveillance aux fins de ladite directive.

(2) La CSSF communique, sans délai, aux autorités compétentes des autres Etats membres désignées comme point de contact unique en vertu de l'article 22, paragraphe 1er, de la directive 2014/92/UE les informations requises aux fins de l'exécution de leurs missions au titre de ladite directive.

Lorsque la CSSF échange des informations avec les autorités compétentes des autres Etats membres, elle peut indiquer, au moment de la communication, que les informations communiquées ne peuvent être divulguées sans son accord exprès, auquel cas ces informations peuvent être échangées uniquement aux fins pour lesquelles la CSSF a donné son accord.

La CSSF peut transmettre les informations reçues aux autres autorités compétentes, mais elle ne les transmet pas à d'autres organismes ou personnes physiques ou morales sans le consentement exprès des autorités compétentes qui les ont divulguées et uniquement aux fins pour lesquelles les autorités compétentes ont donné leur consentement, sauf si la divulgation d'informations est exigée par ou en vertu d'une loi, auquel cas elle informe immédiatement son point de contact qui a envoyé les informations.

(3) La CSSF ne peut refuser de donner suite à une demande de coopérer à une enquête, à une activité de surveillance ou à un échange d'informations que lorsque :

1. l'enquête, la vérification sur place ou l'activité de surveillance est susceptible de porter atteinte à la souveraineté, à la sécurité ou à l'ordre public de l'Etat luxembourgeois ;
2. une procédure judiciaire a déjà été engagée pour les mêmes faits et à l'encontre des mêmes personnes devant les tribunaux luxembourgeois ;
3. un jugement définitif a été rendu pour les mêmes faits à l'encontre des mêmes personnes au Luxembourg.

En cas de refus, la CSSF informe l'autorité compétente requérante de façon aussi circonstanciée que possible.

(4) La CSSF peut saisir l'Autorité bancaire européenne et solliciter son assistance au titre de l'article 19 du règlement (UE) n° 1093/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité bancaire européenne), modifiant la décision n° 716/2009/CE et abrogeant la décision 2009/78/CE de la Commission européenne lorsqu'une demande de coopération de la CSSF en vertu de l'article 22 de la directive 2014/92/UE, notamment en vue de l'échange d'informations, a été rejetée ou n'a pas été suivie d'effet dans un délai raisonnable.

Chapitre 7 - Disposition modificative et dispositions finales

Art. 35.

L'article 3 de la loi modifiée du 15 décembre 2000 sur les services financiers postaux est abrogé.

Art. 36.
La référence à la présente loi se fait sous la forme suivante : « loi du 13 juin 2017 relative aux comptes de paiement ».

Art. 37.
L'article 5, paragraphe 1er, alinéa 1er et paragraphes 2 à 7, et les articles 6, 7 et 9 entrent en vigueur neuf mois après l'entrée en vigueur de l'acte délégué visé à l'article 3, paragraphe 4 de la directive 2014/92/UE.

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.

Pour le Ministre des Finances,
Le secrétaire d'État à la Culture,
Guy Arendt

Palais de Luxembourg, le 13 juin 2017.
Henri

Doc. parl. 7103; sess. ord. 2016-2017; Dir. 2014/92/UE.