N° 8307

CHAMBRE DES DEPUTES

Session ordinaire 2022-2023

PROJET DE LOI

portant transposition de la directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, et abrogeant la directive 2008/114/CE du Conseil, et modifiant :

1° la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'Etat ;

2° la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale

* * *

Document de dépôt

Dépôt: le 1.9.2023

*

Le Premier Ministre,

Vu les articles 76 et 95, alinéa 1er, de la Constitution ;

Vu l'article 10 du Règlement interne du Gouvernement ;

Vu l'article 58, paragraphe 1er, du Règlement de la Chambre des Députés ;

Vu l'article 1er, paragraphe 1er, de la loi modifiée du 16 juin 2017 sur l'organisation du Conseil d'État ;

Considérant la décision du Gouvernement en conseil du du 28 juillet 2023 approuvant sur proposition du Premier Ministre, Ministre d'État le projet de loi ci-après ;

Arrête :

Art. 1er. Le Premier Ministre, Ministre d'État est autorisé à déposer au nom du Gouvernement à la Chambre des Députés le projet de loi portant transposition de la directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, et abrogeant la directive 2008/114/CE du Conseil, et modifiant 1° la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État ; 2° la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale et à demander l'avis y relatif au Conseil d'État.

Art. 2. Le Ministre aux Relations avec le Parlement est chargé, pour le compte du Premier Ministre, Ministre d'État, de l'exécution du présent arrêté.

Luxembourg, le 1er septembre 2023

Le Premier Ministre,
Ministre d'État,
Xavier BETTEL

TEXTE DU PROJET DE LOI

Chapitre 1er – Définition et champ d'application

Art. 1er. (1) La présente loi ne s'applique pas aux questions couvertes par la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148, sans préjudice de l'article 8.

(2) Lorsque des dispositions d'actes juridiques sectoriels de l'Union européenne exigent des entités critiques qu'elles adoptent des mesures pour renforcer leur résilience, et lorsque ces exigences ont un effet au moins équivalent aux obligations correspondantes prévues par la présente loi, les dispositions pertinentes de la présente loi, y compris les dispositions relatives à la supervision et à l'exécution prévues au chapitre 6, ne s'appliquent pas.

(3) La présente loi est sans préjudice du droit de l'Union européenne relatif à la protection des données à caractère personnel, en particulier le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE et la loi modifiée du 30 mai 2005 relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques et portant modification des articles 88-2 et 88-4 du Code d'instruction criminelle.

Art. 2. Pour l'application de la présente loi, on entend par :

1° « entité critique » : une entité publique ou privée qui a été désignée conformément à l'article 7 comme appartenant à l'une des catégories qui figurent dans la troisième colonne du tableau de l'annexe ;

2° « résilience » : la capacité d'une entité critique à prévenir tout incident, à s'en protéger, à y réagir, à y résister, à l'atténuer, à l'absorber, à s'y adapter et à s'en rétablir ;

3° « incident » : un événement qui perturbe ou est susceptible de perturber de manière importante la fourniture d'un service essentiel, y compris lorsqu'il affecte les systèmes nationaux qui préservent l'état de droit ;

4° « infrastructure critique » : un bien, une installation, un équipement, un réseau ou un système, ou une partie d'un bien, d'une installation, d'un équipement, d'un réseau ou d'un système, qui est nécessaire à la fourniture d'un service essentiel ;

5° « service essentiel » : un service qui est crucial pour le maintien de fonctions sociétales ou d'activités économiques vitales, de la santé publique et de la sûreté publique, ou de l'environnement ;

6° « maintien de fonctions sociétales vitales » : la disponibilité de services indispensables à la sauvegarde des intérêts vitaux ou des besoins essentiels de tout ou partie du pays ou de la population ;

7° « risque » : le potentiel de perte ou de perturbation causé par un incident, à exprimer comme la combinaison de l'ampleur de cette perte ou de cette perturbation et la probabilité que l'incident se produise ;

8° « évaluation des risques » : l'ensemble du processus permettant de déterminer la nature et l'étendue d'un risque en déterminant et en analysant les menaces, les vulnérabilités et les dangers potentiels pertinents qui pourraient conduire à un incident et en évaluant la perte ou la perturbation potentielle de la fourniture d'un service essentiel causée par cet incident ;

9° « entité de l'administration publique » : toute entité, à l'exclusion de l'organisation judiciaire, de la Chambre des députés et de la Banque centrale du Luxembourg, qui satisfait aux critères suivants :

a) elle a été créée pour satisfaire des besoins d'intérêt général et n'a pas de caractère industriel ou commercial ;

b) elle est dotée de la personnalité juridique ou est juridiquement habilitée à agir pour le compte d'une autre entité dotée de la personnalité juridique ;

c) elle est financée majoritairement par les autorités de l'État ou d'autres organismes de droit public de niveau central, ou sa gestion est soumise à un contrôle de la part de ces autorités ou organismes, ou son organe d'administration, de direction ou de surveillance est composé, pour plus de la moitié, de membres désignés par les autorités de l'État ou d'autres organismes de droit public de niveau central ;

d) elle a le pouvoir d'adresser à des personnes physiques ou morales des décisions administratives ou réglementaires affectant leurs droits en matière de mouvements transfrontières des personnes, des biens, des services ou des capitaux.

Chapitre 2 – Autorités compétentes et point de contact national unique

Art. 3. La Commission de surveillance du secteur financer est l'autorité compétente chargée de veiller à l'application correcte de la présente loi pour le secteur bancaire et le secteur des infrastructures des marchés financiers, figurant aux points 3 et 4 du tableau de l'annexe, ainsi que le secteur des infrastructures numériques, figurant au point 8 du tableau de l'annexe, pour les activités qui tombent sous la surveillance de la Commission de surveillance du secteur financer.

Le Haut-Commissariat à la Protection nationale est l'autorité compétente chargée de veiller à l'application correcte de la présente loi pour les autres secteurs visés à l'annexe, ainsi que le secteur des infrastructures numériques, figurant au point 8 du tableau de l'annexe, pour les activités qui ne tombent pas sous la surveillance de la Commission de surveillance du secteur financier.

L'obligation au secret professionnel prévue par l'article 16 de la loi modifiée du 23 décembre 1998 portant création d'une Commission de surveillance du secteur financier ne fait pas obstacle à l'échange d'informations confidentielles entre les autorités compétentes dans le cadre et aux seules fins de la présente loi et des mesures prises pour son exécution.

Art. 4. Le Haut-Commissariat à la Protection nationale constitue le point de contact national unique chargé d'exercer une fonction de liaison afin d'assurer la coopération transfrontière avec les points de contact uniques des autres États membres et avec le groupe sur la résilience des entités critiques visé à l'article 19 de la directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, et abrogeant la directive 2008/114/CE du Conseil. En outre, le point de contact national unique exerce une fonction de liaison avec la Commission européenne et assure la coopération avec les pays tiers.

Chapitre 3 – Cadre national pour la résilience des entités critiques

Art. 5. Le Haut-Commissariat à la Protection nationale élabore, après consultation de la Commission de surveillance du secteur financier, une stratégie visant à renforcer la résilience des entités critiques qui définit des objectifs stratégiques et des mesures politiques, en s'appuyant sur des stratégies nationales et sectorielles, des plans ou des documents similaires pertinents existants, en vue d'atteindre et de maintenir un niveau élevé de résilience des entités critiques et de couvrir au moins les secteurs figurant à l'annexe.

La stratégie contient les éléments suivants :

1° les objectifs stratégiques et les priorités aux fins de renforcer la résilience globale des entités critiques, compte tenu des dépendances et des interdépendances transfrontières et transsectorielles ;

2° un cadre de gouvernance permettant d'atteindre les objectifs stratégiques et les priorités, y compris une description des rôles et des responsabilités des différentes autorités, entités critiques et autres parties participant à la mise en oeuvre de la stratégie ;

3° une description des mesures nécessaires pour renforcer la résilience globale des entités critiques, y compris une description de l'évaluation des risques visée à l'article 6 ;

4° une description du processus par lequel les entités critiques sont recensées ;

5° une description du processus de soutien aux entités critiques conformément au présent chapitre, y compris les mesures visant à renforcer la coopération entre le secteur public, d'une part, et le secteur privé et les entités publiques et privées, d'autre part ;

6° une liste des principales autorités et parties prenantes concernées, autres que les entités critiques, participant à la mise en oeuvre de la stratégie ;

7° un cadre d'action pour la coordination entre les autorités compétentes au sens de la présente loi et les autorités compétentes en vertu de la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 aux fins du partage d'informations sur les risques, menaces et incidents en matière de cybersécurité ainsi que sur les risques, menaces et. incidents non liés à la cybersécurité, et de l'exercice des tâches de supervision ;

8° une description des mesures déjà en place visant à faciliter la mise en oeuvre des obligations prévues au chapitre 4 par les petites et moyennes entreprises au sens de l'annexe de la recommandation 2003/361/CE de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises recensées en tant qu'entités critiques.

À la suite d'une consultation qui est, dans la mesure du possible en pratique, ouverte aux parties prenantes concernées, le Haut-Commissariat à la Protection nationale met à jour la stratégie au moins tous les quatre ans.

Art. 6. (1) Le Haut-Commissariat à la Protection nationale effectue une évaluation des risques sur base des services essentiels identifiés par la Commission européenne. Cette évaluation des risques est utilisée pour recenser les entités critiques conformément à l'article 7 et pour aider les entités critiques à adopter des mesures en vertu de l'article 12.

(2) Afin de procéder à l'évaluation des risques, le Haut-Commissariat à la Protection nationale tient compte des éléments suivants :

1° l'analyse des risques qui tient compte des risques naturels et d'origine humaine pertinents, y compris ceux qui revêtent un caractère transsectoriel ou transfrontière, des accidents, des catastrophes naturelles, des urgences de santé publique et des menaces hybrides ou autres menaces antagonistes, lesquelles comprennent les infractions terroristes prévues par le Code pénal ;

2° l'évaluation des risques générale effectuée en vertu de l'article 6, paragraphe 1er, de la décision n° 1313/2013/UE du Parlement européen et du Conseil du 17 décembre 2013 relative au mécanisme de protection civile de l'Union européenne ;

3° d'autres évaluations des risques pertinentes effectuées conformément aux exigences des actes juridiques sectoriels pertinents de l'Union européenne, y compris le règlement (UE) 2017/1938 du Parlement européen et du Conseil du 25 octobre 2017 concernant des mesures visant à garantir la sécurité de l'approvisionnement en gaz naturel et abrogeant le règlement (UE) n° 994/2010 et le règlement (UE) 2019/941 du Parlement européen et du Conseil du 5 juin 2019 sur la préparation aux risques dans le secteur de l'électricité et abrogeant la directive 2005/89/CE, ainsi que la loi modifiée du 19 décembre 2008 relative à l'eau et la loi du 28 avril 2017 concernant la maîtrise des dangers liés aux accidents majeurs impliquant des substances dangereuses ;

4° les risques pertinents découlant de la mesure dans laquelle les secteurs figurant à l'annexe dépendent les uns des autres, y compris de la mesure dans laquelle ils dépendent d'entités situées dans d'autres États membres et des pays tiers, et l'incidence qu'une perturbation importante dans un secteur peut avoir sur d'autres secteurs, y compris tout risque important pour les citoyens et le marché intérieur ;

5° toute information sur les incidents notifiés conformément à l'article 16.

Aux fins du premier alinéa, point 4, le Haut-Commissariat à la Protection nationale coopère avec les autorités compétentes d'autres États membres en vertu de la directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, et abrogeant la directive 2008/114/CE du Conseil et les autorités compétentes de pays tiers, s'il y a lieu.

(3) Le Haut-Commissariat à la Protection nationale met à la disposition des entités critiques recensées conformément à l'article 7, les éléments pertinents des évaluations des risques.

Art. 7. (1) Les autorités compétentes recensent les entités critiques pour les secteurs et sous-secteurs figurant à l'annexe.

La désignation d'une entité critique fait l'objet d'un arrêté grand-ducal.

(2) Lorsqu'une autorité compétente recense les entités critiques en vertu du paragraphe 1er, elle tient compte des résultats de l'évaluation des risques effectuée en vertu de l'article 6 et de la stratégie visée à l'article 5 et applique tous les critères suivants :

1° l'entité fournit un ou plusieurs services essentiels ;

2° l'entité exerce ses activités sur le territoire luxembourgeois et son infrastructure critique est située sur ledit territoire; et

3° un incident aurait des effets perturbateurs importants, déterminés conformément au paragraphe 3 du présent article, sur la fourniture par l'entité d'un ou de plusieurs services essentiels ou sur la fourniture d'autres services essentiels dans les secteurs figurant à l'annexe qui dépendent dudit ou desdits services essentiels.

L'entité critique est tenue de mettre à la disposition de l'autorité compétente toutes les données sollicitées aux fins du recensement, de la désignation et de la protection des entités critiques.

(3) L'importance d'un effet perturbateur visé au paragraphe 2, point 3, est déterminée sur base des critères suivants :

1° le nombre d'utilisateurs tributaires du service essentiel fourni par l'entité concernée ;

2° la mesure dans laquelle les autres secteurs et sous-secteurs figurant à l'annexe dépendent du service essentiel en question ;

3° l'impact que des incidents pourraient avoir, du point de vue de l'ampleur et de la durée, sur les activités économiques et sociétales, l'environnement, la sûreté et la sécurité publiques, ou la santé de la population ;

4° la part de marché de l'entité sur le marché du ou des services essentiels concernés ;

5° la zone géographique susceptible d'être affectée par un incident, y compris toute incidence transfrontière, compte tenu de la vulnérabilité associée au degré d'isolement de certains types de zones géographiques ;

6° l'importance que revêt l'entité pour le maintien d'un niveau suffisant de service essentiel, compte tenu de la disponibilité de solutions de rechange pour la fourniture de ce service essentiel.

(4) Les autorités compétentes dressent une liste des entités critiques recensées et désignées en vertu du paragraphe 2 et veillent à ce que ces entités critiques reçoivent notification de ce qu'elles ont été désignées en tant qu'entités critiques dans un délai d'un mois à compter de cette désignation. Les autorités compétentes informent ces entités critiques des obligations qui leur incombent en vertu des chapitres 4 et 5 et de la date à partir de laquelle ces obligations leur sont applicables, sans préjudice de l'article 8. Les autorités compétentes informent les entités critiques des secteurs figurant aux points 3 et 4 du tableau de l'annexe qu'elles ne sont soumises à aucune des obligations prévues aux chapitres 4 et 5. De même, les autorités compétentes informent les entités critiques du secteur figurant au point 8 du tableau de l'annexe qu'elles ne sont soumises à aucune des obligations prévues aux chapitres 4 et 5, pour les activités qui tombent sous la surveillance de la Commission de surveillance du secteur financier.

Le chapitre 4 s'applique aux entités critiques concernées à l'expiration d'un délai de dix mois à compter de la date de la notification visée au premier alinéa du présent paragraphe.

(5) L'entité critique, à la suite de la notification visée au paragraphe 4, informe son autorité compétente lorsqu'elle fournit des services essentiels à ou dans six États membres ou plus. En pareil cas, l'entité critique informe son autorité compétente au sujet des services essentiels qu'elle fournit à ou dans ces États membres et au sujet des États membres auxquels ou dans lesquels elle fournit ces services essentiels. Les dispositions du chapitre 5 s'appliquent.

(6) Les autorités compétentes notifient aux autorités compétentes en vertu de la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 l'identité des entités critiques qu'ils ont recensées et désignées dans un délai d'un mois à compter de la désignation. Cette notification précise, le cas échéant, que les entités critiques concernées sont des entités des secteurs figurant aux points 3 et 4 du tableau de l'annexe et qu'elles ne sont soumises à

aucune des obligations prévues aux chapitres 4 et 5. De même, cette notification précise. le cas échéant, que les entités critiques concernées sont des entités des secteurs figurant au point 8 du tableau de l'annexe et qu'elles ne sont soumises à aucune des obligations prévues aux chapitres 4 et 5, pour les activités qui tombent sous la surveillance de la Commission de surveillance du secteur financier.

(7) Si nécessaire et en tout état de cause au moins tous les quatre ans, les autorités compétentes réexaminent et, s'il y a lieu, mettent à jour la liste des entités critiques recensées et désignées visées au paragraphe 4. Lorsque ces mises à jour entraînent le recensement et la désignation d'entités critiques supplémentaires, les paragraphes 4 à 6 s'appliquent à ces entités critiques supplémentaires. En outre, les autorités compétentes notifient en temps utile les entités qui ne sont plus recensées en tant qu'entités critiques, à la suite d'une telle mise à jour, de ce fait et du fait qu'elles ne sont plus soumises aux obligations prévues au chapitre 4 à compter de la date de réception de cette notification.

Art. 8. L'article 10 et les chapitres 4, 5 et 6 ne s'appliquent ni aux entités critiques recensées dans les secteurs figurant aux points 3 et 4 du tableau de l'annexe, ni aux entités critiques recensées dans le secteur figurant au point 8 du tableau de l'annexe, pour les activités qui tombent sous la surveillance de la Commission de surveillance du secteur financier.

Art. 9. (1) Les autorités compétentes aident les entités critiques à renforcer leur résilience.

(2) Les autorités compétentes coopèrent et échangent des informations et des bonnes pratiques avec les entités critiques des secteurs figurant à l'annexe.

Art. 10. Chaque fois que cela est approprié, les autorités compétentes se consultent avec les autorités compétentes des autres États membres au sujet des entités critiques aux fins d'assurer l'application cohérente de la présente loi. Ces consultations ont lieu en particulier au sujet des entités critiques qui :

1° utilisent des infrastructures critiques qui sont physiquement connectées entre deux États membres ou plus ;

2° font partie de structures d'entreprise qui sont connectées ou liées à des entités critiques dans d'autres États membres ;

3° ont été recensées en tant qu'entités critiques dans un État membre et fournissent des services essentiels à ou dans d'autres États membres.

Chapitre 4 – Résilience des entités critiques

Art. 11. (1) Sans préjudice de l'article 7, paragraphe 4, deuxième alinéa, les entités critiques procèdent à une évaluation des risques dans un délai de neuf mois suivant la réception de la notification visée à l'article 7, paragraphe 4, selon les besoins par la suite et au moins tous les quatre ans, sur la base de l'évaluation des risques visée à l'article 6 et d'autres sources d'informations pertinentes, afin d'évaluer tous les risques pertinents qui pourraient perturber la fourniture de leurs services essentiels (ci-après dénommée « évaluation des risques d'entité critique »).

(2) Les évaluations des risques d'entités critiques rendent compte de tous les risques naturels et d'origine humaine pertinents, susceptibles d'entraîner un incident, y compris ceux qui revêtent un caractère transsectoriel ou transfrontière, des accidents, des catastrophes naturelles, des urgences de santé publique et des menaces hybrides et autres menaces antagonistes, lesquelles comprennent les infractions terroristes prévues par le Code pénal. Une évaluation des risques d'entité critique tient compte de la mesure dans laquelle d'autres secteurs figurant à l'annexe dépendent du service essentiel fourni par l'entité critique et de la mesure dans laquelle cette entité critique dépend des services essentiels fournis par d'autres entités de ces autres secteurs, y compris s'il y a lieu, dans les États membres voisins et les pays tiers.

Lorsqu'une entité critique a réalisé d'autres évaluations des risques ou établi des documents en vertu d'obligations prévues dans d'autres actes juridiques qui sont pertinents pour son évaluation des risques d'entité critique, elle peut utiliser ces évaluations et documents pour satisfaire aux exigences énoncées dans le présent article. Dans l'exercice de ses fonctions de supervision, l'autorité compétente peut déclarer qu'une évaluation des risques existante réalisée par une entité critique qui porte sur les risques

et le degré de dépendance visés au premier alinéa du présent paragraphe respecte, en tout ou en partie, les obligations prévues par le présent article.

Art. 12. (1) Les entités critiques prennent des mesures techniques, des mesures de sécurité et des mesures organisationnelles appropriées et proportionnées pour garantir leur résilience, sur la base des informations pertinentes fournies par les autorités compétentes concernant l'évaluation des risques visée à l'article 6 et les résultats de l'évaluation des risques d'entité critique, y compris des mesures nécessaires pour :

1° prévenir la survenance d'incidents, en tenant dûment compte de mesures de réduction des risques de catastrophe et d'adaptation au changement climatique ;

2° assurer une protection physique adéquate de leurs locaux et infrastructures critiques ;

3° réagir et résister aux conséquences des incidents et les atténuer, en prenant dament en considération la mise en oeuvre de procédures et protocoles de gestion des risques et des crises et de procédures d'alerte ;

4° se rétablir d'incidents, en prenant dament en considération des mesures assurant la continuité des activités et la détermination d'autres chaînes d'approvisionnement, afin de reprendre la fourniture du service essentiel ;

5° assurer une gestion adéquate de la sécurité liée au personnel, en prenant dament en considération des mesures telles que la définition des catégories de personnel qui exercent des fonctions critiques, l'établissement de droits d'accès aux locaux, aux infrastructures critiques et aux informations sensibles, la mise en place de procédures de vérification des antécédents conformément aux articles 13 à 15, la désignation des catégories de personnes tenues de faire l'objet de telles vérifications des antécédents et la définition d'exigences et de qualifications appropriées en matière de formation ;

6° sensibiliser le personnel concerné aux mesures visées aux points 1 à 5, en tenant dament compte des séances de formation, du matériel d'information et des exercices.

Aux fins du premier alinéa, point 5, les entités critiques tiennent compte du personnel des prestataires de services extérieurs lorsqu'ils définissent les catégories de personnel qui exercent des fonctions critiques.

(2) Les entités critiques mettent en place et appliquent un plan de résilience ou un ou plusieurs documents équivalents, qui décrivent les mesures prises en application du paragraphe 1er. Dans l'exercice de ses fonctions de supervision, l'autorité compétente peut déclarer que des mesures existantes de renforcement de la résilience prises par une entité critique qui portent, de manière appropriée et proportionnée, sur les mesures techniques, les mesures de sécurité et les mesures organisationnelles visées au paragraphe 1er respectent, en tout ou en partie, les obligations prévues par le présent article.

(3) Chaque entité critique désigne un agent de liaison ou une personne ayant une fonction équivalente en tant que point de contact avec les autorités compétentes.

Art. 13. (1) La Police grand-ducale est chargée de procéder à des vérifications des antécédents et en est le responsable du traitement tel que défini par le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/4610E. Elle procède, sur demande des entités critiques et dans le seul but d'évaluer un risque potentiel pour la sécurité de l'entité concernée, à des vérifications des antécédents des personnes :

1° qui occupent des fonctions sensibles au sein de l'entité critique ou au bénéfice de celle-ci, notamment en ce qui concerne la résilience de l'entité critique ;

2° qui occupent la fonction de responsable du système informatique ou du système de contrôle de l'entité critique ;

3° dont le recrutement est envisagé à des postes répondant aux critères énoncés aux points 1 à 2.

Préalablement à l'introduction de la demande visée au paragraphe 1er, les catégories de personnes tenues de faire l'objet d'une vérification des antécédents désignées dans le cadre des mesures prévues à l'article 12, feront l'objet d'un avis favorable par l'autorité compétente. Une copie de cet avis sera transmise à la Police grand-ducale.

(2) Cette demande contient les éléments suivants :

1° l'identité de la personne visée au paragraphe 1er : noms et prénoms, date et lieu de naissance, résidence, nationalité, numéro d'identification national et numéro de la pièce d'identité ainsi qu'une photographie récente ;

2° la nature du contrat de travail ou de la relation juridique liant la personne visée au paragraphe 1er à l'entité critique ;

3° la déclaration écrite ou électronique de la personne visée au paragraphe 1er, contenant l'autorisation de procéder à une vérification des antécédents et de demander toute information relative à la demande disponible et directement accessible aux autorités compétentes nationales, ou tout document équivalent auprès des autorités des pays de résidence des cinq dernières années ou dont il a la nationalité ;

4° une liste des lieux de résidence des cinq dernières années et un certificat de résidence datant de moins de trois mois ;

5° un extrait du casier judiciaire des pays énoncés au point 3, à l'exception du Luxembourg, datant de moins de trois mois ;

6° l'accord de la personne visée au paragraphe 1er, que le bulletin N° 2 du casier judiciaire puisse être délivré directement à la Police grand-ducale ;

7° la signature de la personne visée au paragraphe 1er ;

8° le cachet et la signature de l'entité dont relève la personne visée au paragraphe 1er, précédés d'une attestation de ladite entité certifiant le bien-fondé et les motifs de la demande ;

9° une documentation concernant les emplois, les études et les interruptions au cours des cinq dernières années ;

10° une photocopie de la carte d'identité ou du passeport en cours de validité ;

11° un questionnaire biographique dûment rempli.

La Police grand-ducale procède à la vérification des antécédents sur une période de cinq ans précédant la demande. Lorsque la personne visée au paragraphe 1er est âgée de moins de vingt-trois ans au moment de l'introduction de la demande, la Police est autorisée à consulter le registre spécial prévu par l'article 15 de la loi modifiée du 10 août 1992 relative à la protection de la jeunesse.

Toute demande incomplète est retournée à l'entité critique requérante et non traitée.

(3) Au terme de la vérification, la Police grand-ducale émet, en application de l'article 14, paragraphe 3, un avis qu'elle transmet à l'entité critique requérante. La Police grand-ducale ne communique pas à l'entité requérante les informations personnelles qu'elle a recueillies dans le cadre de la vérification des antécédents.

(4) Les vérifications des antécédents ont une durée de validité de 5 ans. Une demande de renouvellement pour une vérification des antécédents est â introduire au plus tôt six mois et au plus tard quatre mois avant la fin de validité de la vérification des antécédents actuelle.

La décision de renouvellement de la vérification des antécédents prend effet à la fin de validité de la décision antérieure.

Art. 14. (1) Dans le cadre de l'établissement de l'identité de la personne visée à l'article 13, paragraphe 1er, la Police grand-ducale consulte les autorités policières étrangères. Si la personne visée à l'article 13, paragraphe 1er, possède la nationalité d'un pays étranger ou réside dans un pays étranger et sous condition de disposer de l'accord écrit ou électronique de cette personne, la Police grand-ducale peut adresser une demande motivée au procureur général d'État en vue de l'obtention d'un extrait du casier judiciaire de l'autorité compétente de l'État membre dont la personne a la nationalité ou de l'autorité compétente de l'État membre dans lequel la personne a résidé au cours des cinq dernières années.

(2) La Police grand-ducale peut également consulter tout employeur ou tout établissement d'éducation antérieur ou actuel afin de vérifier l'authenticité des informations fournies.

(3) La Police grand-ducale peut demander à la personne visée à l'article 13, paragraphe 1er, toute précision qu'elle juge utile par rapport aux éléments fournis dans sa demande.

(4) La Police grand-ducale indique dans son avis si la personne visée à l'article 13, paragraphe 1er a:

1° commis ou tenté de commettre une des infractions contre la sûreté de l'État visées aux articles 101 à 135-17 du Code pénal ;

2° commis ou tenté de commettre une des infractions de corruption visées aux articles 246 à 250 du Code pénal ;

3° fait des fausses déclarations en relation avec la demande de vérification des antécédents.

Art. 15. (1) La Police grand-ducale met en place un système informatique centralisé permettant de faciliter la gestion administrative des demandes de vérification des antécédents.

(2) Les données à caractère personnel en relation avec les vérifications des antécédents sont conservées pendant une année à partir de la notification de l'avis à l'entité critique.

Art. 16. (1) Les entités critiques notifient sans retard injustifié à l'autorité compétente les incidents qui perturbent ou sont susceptibles de perturber de manière importante la fourniture de services essentiels. Sauf à être dans l'incapacité de le faire pour des raisons opérationnelles, les entités critiques présentent une première notification au plus tard vingt-quatre heures après avoir pris connaissance d'un incident, suivie, s'il y a lieu, d'un rapport détaillé au plus tard un mois après. Afin de déterminer l'importance de la perturbation, les paramètres suivants sont, en particulier, pris en compte :

1° le nombre et la proportion d'utilisateurs affectés par la perturbation ;

2° la durée de la perturbation ;

3° la zone géographique concernée par la perturbation, en tenant compte de son éventuel isolement géographique.

Les paramètres permettant de déterminer l'importance de la perturbation sont précisés par règlement grand-ducal.

(2) Les notifications visées au paragraphe 1er comprennent toutes les informations disponibles nécessaires pour permettre à l'autorité compétente de comprendre la nature, la cause et les conséquences possibles de l'incident, y compris toute information disponible nécessaire pour déterminer tout impact transfrontière de l'incident. Ces notifications n'ont pas pour effet de soumettre les entités critiques à une responsabilité accrue.

(3) Sur la base des informations fournies par une entité critique dans une notification visée au paragraphe 1er, l'autorité compétente concernée, par l'intermédiaire du point de contact unique, informe le point de contact unique des autres États membres affectés lorsque l'incident a ou pourrait avoir un impact important sur les entités critiques et sur la continuité de la fourniture de services essentiels à ou dans un ou plusieurs autres États membres.

Le point de contact unique qui envoie et reçoit des informations en vertu du premier alinéa traite ces informations de manière à en respecter la confidentialité et à préserver la sécurité et les intérêts commerciaux de l'entité critique concernée.

(4) Dès que possible après la réception d'une notification visée au paragraphe 1er, l'autorité compétente concernée fournit à l'entité critique concernée des informations de suivi pertinentes, y compris des informations qui pourraient aider ladite entité critique à réagir efficacement à l'incident en question. Les autorités compétentes informent le public lorsqu'ils estiment qu'il serait dans l'intérêt général de le faire.

Chapitre 5 – Entités critiques d'importance européenne particulière

Art. 17. (1) Une entité est considérée comme une entité critique d'importance européenne particulière lorsqu'elle:

1° a été désignée en tant qu'entité critique conformément à l'article 7, paragraphe 1er ;

2° fournit les mêmes services essentiels ou des services essentiels similaires à ou dans six États membres ou plus ; et

3° a fait l'objet d'une notification de la part de la Commission européenne, par l'intermédiaire de son autorité compétente, qu'elle est considérée comme une entité critique d'importance européenne particulière.

(2) Les entités critiques d'importance européenne particulière accordent aux missions de conseil organisées par la Commission européenne afin d'évaluer les mesures mises en place par ladite entité pour satisfaire aux obligations qui lui incombent en vertu du chapitre 4, l'accès aux informations, systèmes et installations relatifs à la fourniture de leurs services essentiels nécessaires à l'exécution de la mission de conseil concernée.

Chapitre 6 – Supervision et exécution

Art. 18. (1) Afin d'évaluer le respect des obligations découlant de la présente loi, les autorités compétentes sont autorisées à :

1° procéder à des inspections sur place de l'infrastructure critique et des locaux utilisés par l'entité critique pour fournir ses services essentiels afin de s'assurer de la mise en œuvre des mesures prises par les entités critiques conformément à l'article 12 ;

2° procéder à la supervision à distance des mesures prises par les entités critiques conformément à l'article 12 ;

3° ordonner un audit visant à contrôler la mise en oeuvre effective des mesures prises par les entités critiques conformément à l'article 12.

Les inspections sur place prévues au point 1 se font entre huit heures et dix-sept heures, moyennant préavis d'au moins deux semaines, par un agent du groupe de traitement ou du groupe d'indemnité A1 ou A2 de l'autorité compétente. Ces inspections pourront se dérouler en dehors de cette plage horaire, en cas d'accord de l'entité critique.

Les agents visés à l'alinéa 2 signalent leur présence à l'agent de liaison de l'entité critique ou, le cas échéant, à son remplaçant. Ce dernier peut les accompagner et leur prêter concours, le cas échéant, pour mener à bien les inspections.

L'agent visé à l'alinéa 2 est tenu de dresser un rapport relatif à l'inspection opérée. Une copie de ce rapport est transmise à l'agent de liaison de l'entité critique.

(2) Les entités en vertu de la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 désignées en tant qu'entités critiques en vertu de la présente loi sont tenues de fournir aux autorités compétentes, dans un délai raisonnable fixé par celles-ci :

1° les informations nécessaires pour évaluer si les mesures prises par ces entités pour garantir leur résilience satisfont aux exigences énoncées à l'article 12 ;

2° la preuve de la mise en couvre effective de ces mesures, y compris les résultats d'un audit effectué par un auditeur indépendant et qualifié sélectionné par ladite entité et effectué à ses frais.

Ces données comprennent toutes les informations qui sont nécessaires dans le contexte de la prévention ou de la gestion d'une crise en vertu de la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale.

Lorsqu'elles requièrent ces informations, les autorités compétentes mentionnent la finalité de la demande et précisent les informations exigées.

(3) Sans préjudice de la possibilité d'imposer des sanctions conformément à l'article 19, les autorités compétentes peuvent, à la suite des mesures de supervision visées au paragraphe 1er ou de l'évaluation des informations visées au paragraphe 2, enjoindre aux entités critiques concernées de prendre les mesures nécessaires et proportionnées pour remédier à toute violation constatée de la présente loi, dans un délai raisonnable fixé par lesdites autorités, et de leur fournir des informations sur les mesures prises. Ces injonctions tiennent compte, notamment, de la gravité de la violation.

(4) Lorsqu'une autorité compétente évalue le respect par une entité critique de ses obligations en vertu du présent article, ladite autorité compétente en informe les autorités compétentes nationales en

vertu de la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148. A cette fin, les autorités compétentes demandent aux autorités compétentes nationales en vertu de la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 d'exercer leurs pouvoirs de supervision et d'exécution à l'égard d'une entité relevant de ladite directive qui a été désignée en tant qu'entité critique en vertu de la présente loi. À cette fin, les autorités compétentes coopèrent et échangent des informations avec les autorités nationales compétentes en vertu de la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148.

Art. 19. (1) Lorsque l'autorité compétente concernée constate une violation des obligations prévues par les articles 11, 12, 16 et 18 elle peut frapper l'entité critique concernée d'une ou de plusieurs des sanctions suivantes :

1° un avertissement ;

2° un blâme ;

3° une amende administrative, dont le montant est proportionné à la gravité du manquement, à la situation de l'intéressé, à l'ampleur du dommage et aux avantages qui en sont tirés sans pouvoir excéder 250 000 euros.

(2) En cas de constatation d'un fait susceptible de constituer un manquement visé au paragraphe 1er, l'autorité compétente concernée engage une procédure contradictoire dans laquelle l'entité critique concernée a la possibilité de consulter le dossier et de présenter ses observations écrites ou verbales. L'entité critique concernée peut se faire assister ou représenter par une personne de son choix. À l'issue de la procédure contradictoire, l'autorité compétente concernée peut prononcer à l'encontre de l'entité critique concernée une ou plusieurs des sanctions visées au paragraphe 1er.

(3) Les décisions prises par l'autorité compétente concernée à l'issue de la procédure contradictoire sont motivées et notifiées à l'entité critique concernée.

(4) Contre les décisions visées au paragraphe 3 un recours en réformation est ouvert devant le tribunal administratif.

(5) L'Administration de l'enregistrement, des domaines et de la TVA est chargée du recouvrement des amendes administratives qui lui sont communiquées par l'autorité compétente moyennant la transmission d'une copie des décisions de fixation. Le recouvrement est poursuivi comme en matière d'enregistrement.

Chapitre 7 – Dispositions modificatives

Art. 20. Dans l'article 22, paragraphe 10, de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État, les mots « pour assurer l'opérationnalité permanente du Centre national de crise » sont insérés après les mots « soumis à une obligation de permanence ou de présence ».

Art. 21. La loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale est modifiée comme suit :

1° A l'article 1er, alinéa 1er, les termes « infrastructures critiques » sont remplacés par ceux de « entités critiques » ;

2° L'article 2, point 4, est remplacé par le texte suivant :

« 4. « entité critique » : une entité au sens de la loi du XXX sur la résilience des entités critiques ; » ;

3° L'article 3 est modifié comme suit :

a) Le paragraphe 1er, lettre b), point 3, est remplacé par le texte suivant :

« 3. de veiller à l'exécution des mesures relatives à la résilience des entités critiques en application de la loi du XXX sur la résilience des entités critiques ; »

b) Aux paragraphes 1*ter*, lettre g, 1*quater*, lettres a et b, et 3, les termes « infrastructures critiques » sont remplacés par ceux de « entités critiques » ;

4° L'intitulé du chapitre 4 est remplacé par l'intitulé suivant :

« Chapitre 4 – La protection des entités critiques » ;

5° Les articles 4 à 8 sont abrogés ;

6° A l'article 9, alinéa 1er, les termes « infrastructure critique » sont remplacés par ceux de « entité critique » et le terme « infrastructure » est remplacé par celui de « entité ».

Chapitre 8 – Intitulé de citation

Art. 22. La référence à la présente loi se fait sous la forme suivante : « loi du XXX sur la résilience des entités critiques ».

*

ANNEXE

Secteurs, sous-secteurs et catégories d'entités

Secteurs	*Sous-secteurs*	*Catégories d'entités*
1. Énergie	a) Électricité	– Entreprises d'électricité au sens de l'article 1er, point 14, de la loi modifiée du 1er août 2007 relative à l'organisation du marché de l'électricité, qui assurent la fonction de « fourniture » au sens de l'article 1er, point 21, de la même loi
		– Gestionnaires de réseau de distribution au sens de l'article 1er, point 24, de la loi modifiée du 1er août 2007 relative à l'organisation du marché de l'électricité
		– Gestionnaires de réseau de transport au sens de l'article 1er, point 25, de la loi modifiée du 1er août 2007 relative à l'organisation du marché de l'électricité
		– Producteurs au sens de l'article 1er, point 39, de la loi modifiée du 1er août 2007 relative à l'organisation du marché de l'électricité
		– Opérateurs désignés du marché de l'électricité au sens de l'article 2, point 8, du règlement (UE) 2019/943 du Parlement européen et du Conseil du 5 juin 2019 sur le marché intérieur de l'électricité
		– Acteurs du marché au sens de l'article 2, point 25, du règlement (UE) 2019/943 du Parlement européen et du Conseil du 5 juin 2019 sur le marché intérieur de l'électricité, qui fournissent des services d'agrégation, de participation active de la demande ou de stockage d'énergie au sens de l'article 1er, points 1*quindecies*, 31*quater* et 49*ter*, de la loi de 1er août 2007 relative à l'organisation du marché de l'électricité
	b) Réseaux de chaleur et de froid	– Opérateurs de réseaux de chaleur ou de réseau de froid au sens de l'article 2, point 19, de la directive (UE) 2018/2001 du Parlement européen et du Conseil du 11 décembre 2018 relative à la promotion de l'utilisation de l'énergie produite à partir de sources renouvelables

Secteurs	*Sous-secteurs*	*Catégories d'entités*
	c) Pétrole	– Exploitants d'oléoducs
		– Exploitants d'installations de production, de raffinage, de traitement, de stockage et de transport de pétrole
		– Entités centrales de stockage au sens de l'article 1er, lettre g), de la loi modifiée du 10 février 2015 relative à l'organisation du marché de produits pétroliers
	d) Gaz	– Entreprises de fourniture au sens de l'article 1er, point 14, de la loi modifiée du 1er août 2007 relative à l'organisation du marché de gaz naturel
		– Gestionnaires de réseau de distribution au sens de l'article 1er, point 22, de la loi modifiée du 1er août 2007 relative à l'organisation du marché de gaz naturel
		– Gestionnaires de réseau de transport au sens de l'article 1er, point 24, de la loi modifiée du 1er août 2007 relative à l'organisation du marché de gaz naturel
		– Gestionnaires d'installation de stockage au sens de l'article 1er, point 25, de la loi modifiée du 1er août 2007 relative à l'organisation du marché du gaz naturel
		– Gestionnaires d'installation de GNL au sens de l'article 1er, point 23, de la loi modifiée du 1er août 2007 relative à l'organisation du marché du gaz naturel
		– Entreprises de gaz naturel au sens de l'article 1er, point 15, de la loi modifiée du 1er août 2007 relative à l'organisation du marché de gaz naturel
		– Exploitants d'installations de raffinage et de traitement de gaz naturel
	e) Hydrogène	– Exploitants de systèmes de production, de stockage et de transport d'hydrogène
2. Transports	a) Transports aériens	– Transporteurs aériens au sens de l'article 3, point 4, du règlement (CE) n° 300/2008 du Parlement européen et du Conseil du 11 mars 2008 relatif à l'instauration de règles communes dans le domaine de la sûreté de l'aviation civile et abrogeant le règlement (CE) n° 2320/2002 utilisés à des fins commerciales
		– Entités gestionnaires d'aéroports au sens de l'article 2, point 1, de loi du 23 mai 2012 portant transposition de la directive 2009/12/CE du Parlement européen et du Conseil du 11 mars 2009 sur les redevances aéroportuaires et portant modification : 1) de la loi modifiée du 31 janvier 1948 relative à la réglementation de la navigation aérienne ; 2) de la loi modifiée du 19 mai 1999 ayant pour objet a) de réglementer l'accès au marché de l'assistance en escale à l'aéroport de Luxembourg, b) de créer un cadre réglementaire dans le domaine de la sûreté de l'aviation civile, et c) d'instituer une Direction de l'Aviation Civile, aéroports au sens de l'article 2, point 1, de la directive 2009/12/CE du Parlement européen et du Conseil du 11 mars 2009 sur les redevances aéroportuaires, y compris les aéroports du réseaux central énumérés à l'annexe II, section 2, du règlement (UE) n° 1315/2013 du Parlement européen et du Conseil du 11 décembre 2013 sur les orientations de l'Union pour le développement du réseau transeuropéen de transport et abrogeant la décision n° 661/2010/UE, et entités exploitant les installations annexes se trouvant dans les aéroports

Secteurs	*Sous-secteurs*	*Catégories d'entités*
		– Services du contrôle de la circulation aérienne assurant les services du contrôle de la circulation aérienne au sens de l'article 2, point 1, du règlement (CE) n° 549/2004 du Parlement européen et du Conseil du 10 mars 2004 fixant le cadre pour la réalisation du ciel unique européen
	b) Transports ferroviaires	– Gestionnaires de l'infrastructure au sens de l'article 2, point 31, de la loi du 5 février 2021 relative à l'interopérabilité ferroviaire, à la sécurité ferroviaire et à la certification des conducteurs de train
		– Entreprises ferroviaires au sens de l'article 2, point 15, de la loi modifiée du 6 juin 2019 portant transposition de la directive (UE) 2016/2370 du Parlement européen et du Conseil du 14 décembre 2016 modifiant la directive 2012/34/UE en ce qui concerne l'ouverture du marché des services nationaux de transport de voyageurs par chemin de fer et la gouvernance de l'infrastructure ferroviaire et exploitants d'installations de services au sens de l'article 2, point 18, de la même loi
	c) Transports par eau	– Sociétés de transport par voie d'eau intérieure, maritime et côtier de passagers et de fret telles qu'elles sont définies pour le domaine du transport maritime visé à l'annexe I du règlement (CE) n° 725/2004 du Parlement européen et du Conseil du 31 mars 2004 relatif à l'amélioration de la sûreté des navires et des installations portuaires, à l'exclusion des navires exploités à titre individuel par ces sociétés
		– Entités gestionnaires des ports au sens de l'article 3, point 1, de la directive 2005/65/CE du Parlement européen et du Conseil du 26 octobre 2005 relative à l'amélioration de la sûreté des ports, y compris les installations portuaires au sens de l'article 2, point 11, du règlement (CE) n° 725/2004 du Parlement européen et du Conseil du 31 mars 2004 relatif à l'amélioration de la sûreté des navires et des installations portuaires, ainsi que les entités exploitant des ateliers et des équipements à l'intérieur des ports
		– Exploitants de services de trafic maritime (STM) au sens de l'article 2, lettre o), du règlement grand-ducal modifié du 27 février 2011 relatif à la mise en place d'un système communautaire de suivi du trafic des navires et d'information
	d) Transports routiers	– Autorités routières au sens de l'article 2, point 12, du règlement délégué (UE) 2015/962 de la Commission du 18 décembre 2014 complétant la directive 2010/40/UE du Parlement européen et du Conseil en ce qui concerne la mise à disposition, dans l'ensemble de l'Union, de services d'informations en temps réel sur la circulation, chargées du contrôle de la gestion de la circulation, à l'exclusion des entités publiques pour lesquelles la gestion de la circulation ou l'exploitation des systèmes de transport intelligents constituent une partie non essentielle de leur activité générale
		– Exploitants de systèmes de transport intelligents au sens de la lettre circulaire du 22 février 2012 concernant la directive 2010/40/UE du Parlement européen et du Conseil du 7 juillet 2010 concernant le cadre pour le déploiement de systèmes de transport intelligents dans le domaine du transport routier et d'interfaces avec d'autres modes de transport

Secteurs	*Sous-secteurs*	*Catégories d'entités*
	e) Transports publics	– Opérateurs de services publics au sens de l'article 2, lettre d), du règlement (CE) n° 1370/2007 du Parlement européen et du Conseil du 23 octobre 2007 relatif aux services publics de transport de voyageurs par chemin de fer et par route, et abrogeant les règlements (CEE) n° 1191/69 et (CEE) n° 1107/70 du Conseil
3. Secteur bancaire		– Établissements de crédit au sens de l'article 4, 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
4. Infrastructures des marchés financiers		– Exploitants de plates-formes de négociation au sens de l'article 1er, point 43, de la loi du 30 mai 2018 relative aux marchés d'instruments financiers
		– Contreparties centrales au sens de l'article 2, point 1, du règlement (UE) n° 648/2012 du Parlement européen et du Conseil du 4 juillet 2012 sur les produits dérivés de gré à gré, les contreparties centrales et les référentiels centraux
5. Santé		– Prestataires de soins de santé au sens de l'article 2, lettre e), de la loi modifiée du 24 juillet 2014 relative aux droits et obligations du patient
		– Laboratoires de référence de l'UE visés à l'article 15 du règlement (UE) 2022/2371 du Parlement européen et du Conseil du 23 novembre 2022 concernant les menaces transfrontières graves pour la santé et abrogeant la décision n° 1082/2013/UE
		– Entités exerçant des activités de recherche et de développement dans le domaine des médicaments au sens de l'article 1er, point 2, de la directive 2001/83/CE du Parlement européen et du Conseil du 6 novembre 2001 instituant un code communautaire relatif aux médicaments à usage humain
		– Entités fabriquant des produits pharmaceutiques de base et des préparations pharmaceutiques au sens de la NACE Rév. 2 Nomenclature statistique des activités économiques dans la Communauté européenne, section C, division 21
		– Entités fabriquant des dispositifs médicaux considérés comme critiques en cas d'urgence de santé publique (liste des dispositifs médicaux critiques en cas d'urgence de santé publique) au sens de l'article 22 du règlement (UE) 2022/123 du Parlement européen et du Conseil du 25 janvier 2022 relatif à un rôle renforcé de l'Agence européenne des médicaments dans la préparation aux crises et la gestion de celles-ci en ce qui concerne les médicaments et les dispositifs médicaux
		– Entités titulaires d'une autorisation de distribution au sens de l'article 4 de la loi modifiée du 6 janvier 1995 relative à la distribution en gros des médicaments
6. Eau potable		– Fournisseurs et distributeurs d'eaux destinées à la consommation humaine au sens de l'article 2, point 1, lettre a), de la loi du 23 décembre 2022 relative à la qualité des eaux destinées à la consommation humaine, à l'exclusion des distributeurs pour lesquels la distribution d'eaux destinées à la consommation humaine constitue une partie non essentielle de leur activité générale de distribution d'autres produits et biens

Secteurs	*Sous-secteurs*	*Catégories d'entités*
7. Eaux résiduaires		– Entreprises collectant, évacuant ou traitant les eaux urbaines résiduaires, des eaux ménagères usées ou des eaux industrielles usées au sens de l'article 2, points 1, 2 et 3, du règlement grand-ducal modifié du 13 mai 1994 relatif au traitement des eaux urbaines résiduaires, à l'exclusion des entreprises pour lesquelles la collecte, l'évacuation ou le traitement des eaux urbaines résiduaires, des eaux ménagères usées ou des eaux industrielles usées constituent une partie non essentielle de leur activité générale
8. Infrastructures numériques		– Fournisseurs de points d'échange internet au sens de l'article 6, point 18, de la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148
		– Fournisseurs de services DNS au sens de l'article 6, point 20, de la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148, à l'exclusion des opérateurs de serveurs racines de noms de domaines
		– Registres de noms de domaines de premier niveau au sens de l'article 6, point 21, de la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148
		– Fournisseurs de services d'informatique en nuage au sens de l'article 6, point 30, de la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148
		– Fournisseurs de services de centre de données au sens de l'article 6, point 31, de la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148
		– Fournisseurs de réseaux de diffusion de contenu au sens de l'article 6, point 32, de la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148
		– Prestataires de services de confiance au sens de l'article 3, point 19, du règlement (UE) n° 910/2014 du Parlement européen et 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

Secteurs	*Sous-secteurs*	*Catégories d'entités*
		– Fournisseurs de réseaux de communications électroniques publics au sens de l'article 2, point 8, de la loi du 17 décembre 2021 sur les réseaux et les services de communications électroniques
		– Fournisseurs de services de communications électroniques au sens de l'article 2, point 4, de la loi du 17 décembre 2021 sur les réseaux et les services de communications dans la mesure où leurs services sont accessibles au public
9. Administration publique		– Entité de l'administration publique telle que définie à l'article 2, point 9
10. Espace		– Exploitants d'infrastructures au sol, détenues, gérées et exploitées par des États membres ou par des parties privées, qui soutiennent la fourniture de services spatiaux, à l'exclusion des fournisseurs de réseaux de communications électroniques publics au sens de l'article 2, point 8, de la loi du 17 décembre 2021 sur les réseaux et les services de communications
11. Production, transformation et distribution de denrées alimentaires		– Entreprises du secteur alimentaire au sens de l'article 3, point 2, du règlement (CE) n° 178/2002 du Parlement européen et du Conseil du 28 janvier 2002 établissant les principes généraux et les prescriptions générales de la législation alimentaire, instituant l'Autorité européenne de sécurité des aliments et fixant des procédures relatives à la sécurité des denrées alimentaires, qui exercent exclusivement des activités de logistique et de distribution en gros ainsi que de production et de transformation industrielles à grande échelle
12. Gestion des déchets		– Entreprises impliquée dans la gestion des déchets au sens de l'article 4, point 22, de la loi modifiée du 21 mars 2012 relative aux déchets

*

EXPOSE DES MOTIFS

Le projet de loi se propose de transposer la directive (UE) 2022/2557 du Parlement européen et du Conseil du I4 décembre 2022 sur la résilience des entités critiques, et abrogeant la directive 2008/114/CE du Conseil (*Critical Entities Resilience Directive*, ci-après « directive CER »).

Le but primaire de la directive et du projet de loi y afférent est la protection des entités critiques, c'est-à-dire des entités qui assurent un service qui est indispensable pour assurer des fonctions sociétales ou des activités économiques vitales, dénommé « service essentiel ». Ces entités sont critiques dans un double sens. D'une part, ces entités et les services essentiels qu'elles fournissent sont en eux-mêmes cruciaux pour nos sociétés, et, d'autre part, vu les interdépendances entre différents entités et secteurs, la défaillance d'une entité risque de mettre en péril d'autres entités dites critiques.

1. Le contexte dans lequel s'inscrit la directive (UE) 2022/2557

La protection des entités critiques n'est guère un sujet nouveau. En effet, en 2012, le législateur européen s'est saisi pour la première fois de cette thématique à travers l'élaboration de la directive 2008/114/CE,[1] transposée en droit luxembourgeois par un règlement grand-ducal du 12 mars 2012.[2]

1 Directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection, *J.O.U.E.*, L 345 du 23 décembre 2008, p. 75.

2 Règlement grand-ducal du 12 mars 2012 portant application de la directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection, *Mém. A* n° 45, 15 mars 2012, p. 449.

Cette directive visait à établir une procédure harmonisée à l'échelle européenne aux fins du recensement et de la désignation des infrastructures critiques européennes (ICE), c'est-à-dire des infrastructures situées « dans les États membres de l'Union européenne dont l'arrêt ou la destruction aurait un impact considérable sur deux États membres au moins ».[3] Le champ d'application de cette directive était donc limité en ce qu'elle ne visait que les infrastructures dont une défaillance aurait un impact transfrontalier. En outre, la directive ne recensait que les infrastructures dans les secteurs de l'énergie et des transports.

Vu que la directive 2008/114/CE ne s'applique qu'aux infrastructures critiques européennes, le Luxembourg s'est doté, comme de nombreux autres pays européens, d'une loi destinée à assurer la protection des infrastructures critiques nationales.[4] A l'instar du règlement grand-ducal du 12 mars 2012, cette loi attribue au Haut-Commissariat à la Protection nationale (HCPN) la mission de procéder au recensement et à la protection des infrastructures critiques. Cette loi, qui définit l'infrastructure critique comme « tout point, système ou partie de celui-ci qui est indispensable à la sauvegarde des intérêts vitaux ou des besoins essentiels de tout ou partie du pays ou de la population » se distingue fondamentalement du règlement grand-ducal de 2012 en ce qu'il ne prend non seulement en compte les secteurs de l'énergie et des transports, mais aussi ceux des technologies de l'information et de la communication, des finances, de la santé, de l'alimentation, de l'eau, de l'industrie chimique et de l'administration publique.[5] La loi impose aux opérateurs d'une infrastructure critique, dans l'optique de la mise en oeuvre d'un concept de protection nationale efficace, d'informer les autorités en cas d'incident risquant de perturber le fonctionnement de l'infrastructure. Les opérateurs sont par ailleurs tenus d'élaborer, sur base d'une évaluation des risques, des plans de sécurité et de continuité de l'activité qui comportent les mesures visant à prévenir, à atténuer ou à neutraliser le risque d'une discontinuité de la disponibilité du service.

Au niveau européen, la directive 2008/114/CE a fait l'objet d'une évaluation en 2019 qui a montré qu'en raison du caractère de plus en plus interconnecté et transfrontier des services critiques, une protection des entités individuelles n'était plus adéquate. En effet, il faudrait se réorienter sur une approche qui met d'abord l'accent sur la gestion des risques, qui définit ensuite clairement les responsabilités des entités critiques et qui met finalement en place des règles européennes sur la résilience des entités critiques.[6] Ce dernier point était d'autant plus important qu'il y avait une forte fragmentation au niveau du recensement des infrastructures critiques. Puisque chaque État membre procédait à la protection des infrastructures critiques à travers sa législation nationale, il y avait de divergences considérables au niveau des secteurs et catégories d'entités concernées. Partant, une entité pouvait être considérée comme critique dans un État membre, mais pas dans un autre. La directive CER se donnait donc pour but de palier à ces discordances et à créer un niveau élevé d'harmonisation au niveau des secteurs et des catégories d'entités concernées.[7]

La directive CER étend le champ d'application de la directive 2008/114/CE à trois égards. Avant tout, la directive CER ne se limite pas aux entités critiques européennes, mais s'applique à toute entité critique, nationale ou européenne. De surcroît, la directive CER remplace la notion d' « infrastructure critique » par celle d' « entité critique ». En effet, la nouvelle directive ne veut non seulement protéger l'infrastructure, c'est-à-dire l'installation qui sert à fournir le service essentiel, mais elle souhaite mieux équiper les entités qui exploitent ces infrastructures contre les risques qu'elles sont appelées à confronter. Enfin, la directive CER prescrit un recensement dans onze secteurs, à savoir le secteur de l'énergie, des transports, le secteur bancaire, le secteur des infrastructures des marchés financiers, de la santé, de l'eau potable, des eaux résiduaires, des infrastructures numériques, de l'administration publique, de l'espace et de la production. de la transformation et de la distribution de denrées alimentaires.

Notons que la directive CER est en étroite relation avec la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la

---

3 Art. 3, lettre b), du règlement grand-ducal du 12 mars 2012, *o.c.*, (v. note 2).

4 Loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale, *Mém. A* n° 137, 28 juillet 2016, p. 2342.

5 Règlement grand-ducal du 21 février 2018 déterminant les modalités du recensement et de la désignation des infrastructures critiques, *Mém. A* n°152, 1er mars 2018.

6 Consid. (2) directive CER.

7 Consid. (3) directive CER.

directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (*Network and Information Security Directive*, ci-après « directive NIS 2 »).[8] En effet, alors que la directive NIS 2 réglemente la résilience cyber des « entités essentielles » et des « entités importantes », la directive CER se charge de la résilience physique des « entités critiques ». Vu qu'une même entité pourrait à la fois être considérée comme entité essentielle et comme entité critique et en vue d'éviter tout double emploi, les deux directives prévoient une coopération étroite entre les autorités en charge de la mise en oeuvre des deux directives.

Afin d'assurer au mieux la résilience des entités critiques, la directive CER procède par trois étapes. En premier lieu, elle impose aux États membres de mettre en place un cadre stratégique propice à la résilience des entités critiques (2.). Deuxièmement, elle impose aux entités critiques d'évaluer les risques auxquels elles sont exposées et de prendre des mesures techniques et organisationnelles adaptées à ces risques (3.) Enfin, la directive formalise la coopération entre États membres (4.).

2. La mise en place d'un cadre stratégique propice à la résilience des entités critiques

Au lieu de se contenter de renforcer la résilience des entités critiques, la directive cherche à mettre en place un cadre national qui facilite et encourage cette résilience. Ainsi, les États membres ont l'obligation, d'une part, de désigner des autorités compétentes et un point de contact unique et, d'autre part, d'adopter une stratégie pour la résilience des entités critiques et de faire une évaluation des risques.

– Sur le plan national, le Haut-Commissariat à la Protection nationale (HCPN) et la Commission de surveillance du secteur financier (CSSF) sont à considérer comme **autorités compétentes** chargées de veiller à l'application correcte des règles énoncées dans la directive CER. D'un côté, vu l'expérience du HCPN en matière d'infrastructures critiques, il a été jugé opportun de lui confier un rôle majeur dans la mise en oeuvre de la directive CER. Dès lors, le HCPN est responsable du recensement et de la supervision des entités critiques des secteurs de l'énergie, des transports, de la santé, de l'eau potable, des eaux résiduaires, de l'administration publique, de l'espace et de la production, de la transformation, de la distribution de denrées alimentaires et des infrastructures numériques pour lesquelles la CSSF n'est pas compétente. D'un autre côté, vu les spécificités de ces secteurs, la CSSF est en charge du secteur bancaire, du secteur des infrastructures des marchés financiers et des infrastructures numériques, pour les activités qui tombent sous la surveillance de la CSSF. Il est à noter que ce secteur est déjà aujourd'hui soumis à des règles équivalentes à celles inscrites dans la directive CER. L'application de ces règles relève déjà aujourd'hui de la compétence de la CSSF pour les activités qui tombent sous sa surveillance, de sorte qu'il est indiqué de laisser cette compétence auprès de la CSSF.

  La directive CER charge les autorités compétentes de recenser les entités critiques pour les secteurs relevant de leur compétence et d'assurer que ces entités se conforment aux prescriptions de la directive. Par conséquent, la directive leur permet de formuler des instructions contraignantes.

  Bien que la CSSF ait été désignée comme autorité compétente pour le secteur bancaire, le secteur des infrastructures des marchés financiers et le secteur des infrastructures numériques qui tombent sous sa compétence, l'impact de la directive sur ces secteurs reste relativement modeste en termes de nouvelles obligations. Etant donné que ces secteurs sont d'ores et déjà soumis à un grand nombre d'obligations en vertu d'autres législations sectorielles, la directive CER se limite au recensement de ces entités, sans que les chapitres sur les mesures de supervision et d'exécution ne leur soient applicables puisque la directive CER prévoit de telles exemptions pour les secteurs qui doivent respecter des règles équivalentes.
– En ligne avec l'expérience que le HCPN a pu acquérir en matière d'infrastructures critiques, la fonction de **point de contact unique** est assurée par le HCPN. Par conséquent, il revient au HCPN d'exercer une fonction de liaison afin d'assurer la coopération transfrontière avec les autres États membres et l'Union européenne.
– La directive exige par ailleurs que les États membres se dotent d'une **stratégie pour la résilience des entités critiques**. Cette stratégie a pour but de définir les objectifs stratégiques et les priorités à mettre en oeuvre en vue de renforcer la résilience des entités critiques. Vu l'expertise du HCPN en matière d'infrastructures critiques, il reviendra à ce dernier d'élaborer cette stratégie.

---

8 *J.O.U.E.*, L 333 du 27 décembre 2022, p. 80.

– Dernièrement, la directive exige des États membres qu'ils procèdent à une **évaluation des risques** pouvant affecter la fourniture de services essentiels. Cette évaluation des risques sera utilisée ultérieurement pour recenser les entités critiques et pour permettre aux entités critiques de prendre des mesures de résilience adéquates. Etant donné que l'analyse des risques nationale relève déjà aujourd'hui des attributions du HCPN,[9] il a été jugé utile de le charger de cette évaluation.

3. Le renforcement de la résilience des entités critiques

Le deuxième axe de la directive tourne autour des obligations imposées aux entités critiques afin de renforcer leur résilience.

Une entité est recensée comme entité critique si trois conditions sont remplies cumulativement :

– l'entité fournit un ou plusieurs services essentiels ;
– l'entité exerce son activité au Luxembourg et son infrastructure critique se situe sur le territoire du Grand-Duché ; et
– un incident aurait des effets perturbateurs importants. Cet effet perturbateur se mesure à l'aide de critères tels que le nombres d'utilisateurs tributaires du service essentiels, de l'interdépendance entre ce service essentiel et d'autres secteurs critiques ou encore la part de marché de l'entité ou du service essentiel concerné.

Après avoir été recensée comme critique par l'autorité compétente, plusieurs obligations s'imposent aux entités critiques.

– Les entités critiques sont d'abord tenues à faire une **évaluation des risques** qui pourraient perturber la fourniture de leur service essentiel. En ce faisant, les entités critiques prennent notamment en compte l'évaluation des risques élaborée par le HCPN. Cette obligation est similaire à l'analyse des risques que les infrastructures critiques font aujourd'hui dans le contexte de l'élaboration du plan de sécurité et de continuité de l'activité.
– De plus, les entités critiques devront prendre des **mesures techniques, des mesures de sécurité et des mesures organisationnelles** appropriées et proportionnées aux risques préalablement identifiés dans le cadre de leur évaluation des risques. Ces mesures sont également similaires à celles que les entités doivent inscrire dans leur plan de sécurité et de continuité de l'activité.
– La directive donne en outre la possibilité aux entités critiques de demander des **vérifications des antécédents** des personnes qui occupent des fonctions sensibles au sein de l'entité. A l'image du règlement grand-ducal du 28 juillet 2018[10] portant sur les vérification de sécurité effectuées pour le compte des institutions européennes, ces vérifications des antécédents sont effectuées par la Police grand-ducale.
– Finalement, les entités critiques sous soumises à une **obligation de notification**, de sorte que ces entités devront informer les autorités compétentes des incidents qui perturbent ou sont susceptibles de perturber de manière importante la fourniture de leurs services essentiels.

Remarquons que, pour éviter des doubles emplois et des charges inutiles, les dispositions précitées ne s'appliquent pas aux entités soumises à des législations sectorielles qui leur imposeraient des mesures au moins équivalentes en termes de renforcement de leur résilience.

Les autorités compétentes sont en charge de veiller au respect des mesures imposées aux entités critiques. Ainsi, la directive CER leur accorde le pouvoir de formuler des instructions contraignantes, ainsi qu'un véritable pouvoir de sanction.

4. La coopération au niveau européen

Le troisième axe de la directive pivote autour du renforcement de la coopération et de l'échange d'informations au niveau européen.

– D'un côté, la **Commission apporte son soutien** aux États membres et aux entités critiques dans la mise en oeuvre de la directive, notamment en élaborant une vue d'ensemble, au niveau européen,

---

9 Art. 3, para. 1er, lettre a), de la loi modifiée du 23 juillet 2016, *o.c.*, (v. note 4).

10 Règlement grand-ducal du 28 juillet 2018 portant exécution de l'article 26 de la loi du 18 juillet 2018 sur la Police grand-ducale pour les institutions de l'Union européenne, *Mém. A* n° 647, 3 août 2018.

des risques transfrontières et transsectoriels qui pèsent sur la fourniture de services essentiels et en facilitant l'échange d'informations entre États membres et experts dans l'ensemble de l'Union.

– D'un autre côté, la directive instaure le **groupe sur la résilience des entités critiques**, plateforme d'échange pour les experts nationaux et européens. Entre autres, ensemble avec la Commission, ce groupe assiste les États membres dans l'implémentation de la directive et facilite l'échange de bonnes pratiques dans le domaine de la mise en oeuvre de la directive.

Puisque les dispositions de la directive relatives au soutien de la Commission et au groupe sur la résilience des entités critiques se suffisent à elles-mêmes, elles n'ont pas été transposées en droit luxembourgeois.

*

COMMENTAIRE DES ARTICLES

Ad article 1er

D'abord, l'article 1er du projet de loi définit son champ d'application. Vu l'étroite relation entre le présent projet et la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148,[11] ci-après « directive NIS 2 », il convient de veiller à ce que le champ d'application de chacun des deux textes soit clairement délimité. Ainsi, le premier paragraphe pose que la loi sous projet ne s'applique pas aux questions couvertes par la directive NIS 2, qui impose aux entités essentielles et importantes des exigences en matière de cybersécurité.

Le deuxième paragraphe de l'article 1er prévoit que lorsque des dispositions d'actes juridiques sectoriels de l'Union européenne exigent des entités critiques qu'elles prennent des mesures pour renforcer leur résilience, et lorsque ces exigences ont un effet au moins équivalent aux obligations correspondantes prévues par la présente loi, les dispositions pertinentes de la présente loi ne s'appliquent pas, de manière à éviter tout double emploi ou charge inutile. Dans un tel cas, les dispositions pertinentes de cet acte juridique sectoriel s'appliquent.[12]

Remarquons que la terminologie utilisée à l'article 1er, paragraphe 2, de la directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, et abrogeant la directive 2008/114/CE du Conseil, ci-après « directive CER », a été légèrement adapté dans le texte de transposition. En effet, il a été opté, dans un souci de cohérence, pour la terminologie « ont un effet au moins équivalent » reprise de la loi du 28 mai 2019 portant transposition de la directive (UE) 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.[13]

Le dernier paragraphe de l'article 1er souligne l'importance accordée à la protection des données à caractère personnel et prévoit que le présent projet ne déroge aux dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Notons que les auteurs du projet de loi ont fait le choix de ne pas reprendre l'option donnée par la directive d'exclure les secteurs de la sécurité nationale, de la sécurité publique et de la défense du champ d'application du projet de loi vu que déjà aujourd'hui, certaines entités de ces secteurs ont été recensées comme critiques.

---

11 *J.O.U.E.*, L 333 du 27 décembre 2022, p. 80.

12 Consid. (10), directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, et abrogeant la directive 2008/114/CE du Conseil, *J.O.U.E.*, L 333 du 27 décembre 2022, p. 164, ci-après « directive CER ».

13 Loi du 28 mai 2019 portant transposition de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne et modifiant 1° la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'État et 2° la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale, *Mém. A* n°372, 31 mai 2019.

Ad article 2

L'article 2 reprend la définition des termes employés dans le projet de loi. Remarquons que la grande majorité des définitions fait preuve d'une transposition fidèle de la directive CER.

La définition sous l'article 2, point 1, définit l'entité critique, qui a une fonction-clé dans le maintien de fonctions sociétales ou d'activités économiques vitales et qui constitue dès lors l'acteur principal de la directive CER. Une entité critique est une entité publique ou privée :

– appartenant à l'une des catégories qui figurent dans la troisième colonne du tableau de l'annexe,
– fournissant un ou plusieurs services essentiels,
– exerçant ses activités sur le territoire luxembourgeois et son infrastructure critique est située sur ledit territoire, et
– dont un incident aurait des effets perturbateurs importants sur la fourniture par l'entité d'un ou de plusieurs services essentiels ou sur la fourniture d'autres services essentiels dans les secteurs figurant à l'annexe qui dépendent dudit ou desdits services essentiels.

Alors que la directive 2008/114/CE[14] plaçait « l'infrastructure critique » au centre de la directive, la directive CER procède à un changement de paradigme en faisant de « l'entité critique » l'acteur principal de la directive. Ainsi, au lieu d'augmenter la résilience de l'infrastructure critique, qui vise essentiellement l'installation ou l'équipement, cette nouvelle directive veut que l'entité qui exploite cette infrastructure dispose des moyens nécessaires afin de pouvoir faire face aux risques qui pourraient porter préjudice à la fourniture des services essentiels.[15]

Le deuxième point énonce ce que la loi comprend par « résilience ». La résilience des entités critiques est mise au coeur de la directive CER. Les entités critiques doivent être capables de prévenir tout incident qui pourrait perturber la fourniture de leurs services, de s'en protéger, d'y réagir, d'y résister, de l'atténuer, de l'absorber, de s'y adapter et de s'en rétablir, en adoptant une approche basée sur les risques. Tous les risques doivent être pris en compte, notamment les risques naturels, d'origine humaine, y compris ceux qui revêtent un caractère transsectoriel ou transfrontière, les accidents, les catastrophes naturelles, les urgences de santé publique, les menaces hybrides ou encore les menaces terroristes.

Un incident, défini au point 3 de l'article 2, se réfère â un événement qui cause ou est susceptible de causer une perturbation significative dans la fourniture d'un service essentiel. Les entités critiques doivent être capables de prévenir les incidents les touchant ou susceptibles de les toucher.

Le service essentiel est défini au point 5 du même article et constitue « u*n service qui est crucial pour le maintien de fonctions sociétales ou d'activités économiques vitales, de la santé publique et de la sûreté publique, ou de l'environnement* ». Remarquons que, contrairement à la directive CER, le projet de loi rajoute, sous un point 6, la définition du « maintien de fonctions sociétales vitales ». Cette définition a été introduite afin de faire le lien entre le présent projet de loi et la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale.[16] En effet, cette loi relie la notion de la « crise » et de l' « entité critique » en les définissant à travers la sauvegarde des intérêts vitaux et des besoins essentiels de tout ou partie du pays ou de la population. Afin de garder cette cohérence entre les différents domaines d'attribution du Haut-Commissariat à la Protection nationale, le présent projet de loi rajoute les intérêts vitaux et les besoins essentiels du pays et de la population dans la définition des fonctions sociétales vitales.

Le point 9 de l'article 2 reprend la définition de l'entité de l'administration publique. Faute de définition de l'administration publique dans le droit luxembourgeois, la référence au droit national a été omise dans le texte de transposition. En outre, alors que la directive CER exclut les entités de l'administration publique qui exercent leurs activités dans les domaines de la sécurité publique, la défense ou de l'application de la loi du champ d'application de la directive, une telle exclusion n'est pas prévue par le projet de loi. Ainsi, chaque entité étatique qui répond aux critères de l'article 2, point 9, est susceptible d'être recensée comme entité critique, si elle répond en outre aux critères de l'article 7 ci-après.

---

14 Directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection, *J.O.U.E.*, L 345 du 23 décembre 2008.

15 Consid. (2) et (3) directive CER.

16 Loi modifiée du 23 juillet 2016 ponant création d'un Haut-Commissariat a la Protection nationale, *Mém. A* n° 137, 28 juillet 2016, p. 2342.

Ad article 3

L'article 3 détermine les autorités compétentes chargées de veiller à l'application correcte du présent projet de loi. D'une part, vu l'expertise et la compétence de la Commission de surveillance du secteur financier (CSSF) en matière bancaire et financière, il a été jugé cohérent de lui confier le rôle d'autorité compétente pour le secteur bancaire et le secteur des infrastructures des marchés financiers, ainsi que pour le secteur des infrastructures numériques pour les activités qui tombent sous la surveillance de la Commission de surveillance du secteur financier, telles que les activités des PSF de support. D'autre part, vu que le Haut-Commissariat à la Protection nationale (HCPN) est, depuis l'entrée en vigueur du règlement grand-ducal du 12 mars 2012[17] et de la loi du 23 juillet 2016[18], l'autorité compétente en matière d'infrastructures critiques nationales et européennes, la loi sous projet s'insère dans cette logique en lui attribuant la fonction d'autorité compétente pour les secteurs pour lesquels la CSSF n'a aucune compétence (énergie, transports, santé, eau potable, eaux résiduaires, activités des infrastructures numériques pour lesquelles la CSSF n'a aucune compétence, administration publique, espace, production, transformation et distribution de denrées alimentaires, gestion des déchets).

Afin d'assurer une bonne coopération entre les autorités compétentes et d'assurer une approche cohérente en matière de désignation des entités critiques et d'évaluation de leur résilience, le troisième alinéa de l'article 3 prévoit une exception au secret professionnel inscrite dans la loi portant organisation de la CSSF, afin de permettre aux autorités compétentes de s'échanger des informations en cas de besoin.

Ad article 4

A l'instar du règlement grand-ducal du 12 mars 2012,[19] le projet de loi accorde la mission de point de contact unique au HCPN.

En tant que point de contact unique, le HCPN a pour mission de faciliter la coopération et la communication transfrontières et de permettre la mise en oeuvre effective de la présente loi sous projet. Dans la mise en oeuvre de cette mission, le HCPN assure la coordination de la communication et la liaison avec les autorités compétentes nationales, ainsi qu'avec les points de contact uniques des autres États membres et le groupe sur la résilience des entités critiques, constitué au niveau de l'Union européenne.[20]

Ad article 5

L'article 5 prévoit que le HCPN élabore, après consultation de la Commission de surveillance du secteur financier, une stratégie visant à renforcer la résilience des entités critiques couvrant au moins les secteurs et sous-secteurs visés à l'annexe du projet de loi. La stratégie vise à garantir une approche globale de la résilience des entités critiques en définissant les objectifs stratégiques et les mesures politiques à mettre en oeuvre. Dans un souci de cohérence et d'efficacité, la stratégie intégrera harmonieusement les politiques existantes, en s'appuyant sur des stratégies nationales et sectorielles, des plans ou des documents similaires pertinents existants[21], tels que :

– la stratégie nationale de cybersécurité 2021-2025 ;
– la stratégie pour l'adaptation aux effets du changement climatique au Luxembourg 2018-2023 ;
– la stratégie nationale à long terme en matière d'action climat « Vers la neutralité climatique en 2050 ;
– la stratégie nationale en matière d'hydrogène, la stratégie nationale biogaz ;
– la stratégie « Null Offall Lëtzebuerg » ;
– la stratégie pour une mobilité durable (2018-2025) ;
– la stratégie nationale pour les réseaux à ultra-haut débit 2021-2025 ;
– les Lignes directrices de la Défense luxembourgeoise à l'horizon 2035.

---

17 Règlement grand-ducal du 12 mars 2012 portant application de la directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection, *Mém. A* n° 45, 15 mars 2012, p. 449.

18 Loi modifiée du 23 juillet 2016, *o.c.*, (v. note 6).

19 Règlement grand-ducal du 12 mars 2012, *o. c.*, (v. note 7).

20 Consid. (23) directive CER.

21 Consid. (13) directive CER.

Un élément important de la stratégie est le cadre d'action pour une coordination renforcée entre les autorités compétentes en vertu du présent projet de loi et les autorités compétentes en vertu de la directive NIS 2. Afin d'assurer que ces autorités fonctionnent de manière complémentaire, la stratégie a pour objectif d'encourager le partage d'informations sur les risques, menaces et incidents cybernétiques et non-cybernétiques et d'inciter une collaboration au niveau de l'exercice des tâches de supervision.[22]

Cette stratégie fera l'objet d'une révision et d'une mise à jour au moins tous les quatre ans.

Ad. article 6

L'article 6 du présent projet de loi prévoit que le HCPN est compétent pour effectuer une évaluation des risques sur base des services essentiels identifiés par la Commission européenne. En effet, le HCPN est l'unique autorité compétente pour effectuer l'évaluation des risques et ce peu importe le secteur concerné. Cette approche va de pair avec la compétence du HCPN au niveau de la gestion de crise, qui s'étend sur tous secteurs confondus.

Cette évaluation des risques tient d'abord compte de l'analyse des risques générale que le HCPN effectue en vertu de sa loi-cadre[23] et qui prend en considération les risques naturels et d'origine humaine pertinents, y compris ceux qui revêtent un caractère transsectoriel ou transfrontière, les accidents d'envergure, les catastrophes naturelles, les urgences de santé publique, telles que les pandémies et les menaces hybrides et autres menaces antagonistes, telles que le risque terroriste, l'infiltration par les réseaux criminels et le sabotage.

Lorsqu'il procède à une telle évaluation, le HCPN tient aussi compte d'autres évaluations des risques générales ou sectorielles effectuées en vertu d'autres actes juridiques de l'Union et examine la mesure dans laquelle les secteurs dépendent les uns des autres, y compris de secteurs d'autres États membres et de pays tiers. Les résultats de l'évaluation des risques sont utilisés aux fins de recenser les entités critiques.[24]

Ad article 7

L'article 7 décrit le processus de recensement et de désignation des entités critiques pour les secteurs et sous-secteurs visés à l'annexe du projet de loi. Ce processus a pour objet de garantir que toutes les entités critiques soient soumises aux exigences en matière de résilience posées par la présente loi sous projet et de réduire les divergences à cet égard.[25]

A l'instar de la loi du 23 juillet 2016, les entités critiques sont désignées moyennant arrêté grand-ducal.[26]

Plusieurs critères cumulatifs entrent en compte dans le processus de recensement :

– D'abord, ne sont recensées que les entités qui fournissent un ou plusieurs services essentiels, c'est-à-dire « *un service qui est crucial pour le maintien de fonctions sociétales ou d'activités économiques vitales, de la santé publique et de la sûreté publique, ou de l'environnement* ».[27]
– Ensuite, il faut que l'entité exerce ses activités sur le territoire du Grand-Duché et que son infrastructure critique soit située sur ledit territoire. Une entité est considérée comme exerçant des activités sur le territoire de l'État membre dans lequel elle exerce les activités nécessaires pour le ou les services essentiels en question et dans lequel se trouve l'infrastructure critique de cette entité, qui est utilisée pour fournir ce ou ces services.[28]
– Finalement, une entité est critique si un incident avait des effets perturbateurs importants soit sur la fourniture d'un ou de plusieurs services essentiels, soit sur la fourniture d'autres services essentiels dans les secteurs figurant à l'annexe qui dépendent dudit ou desdits services essentiels.

---

22 Consid. (13) directive CER.

23 V. art. 3, para. 1er, point 3, de la loi modifiée du 23 juillet 2016, *o.c.*, (v. note 6).

24 Consid. (15) directive CER.

25 Consid. (16) directive CER.

26 Art. 7 de la loi modifiée du 23 juillet 2016, *o.c.*, (v. note 6).

27 Art. 2, point 5, du projet de loi.

28 Consid. (16) directive CER.

Le deuxième alinéa du paragraphe 2 exige la mise à disposition par les entités critiques de toutes les données nécessaires pour le recensement, la désignation et la protection desdites entités. Dans le but de maintenir une cohérence entre le régime actuel applicable aux infrastructures critiques et le futur régime applicable aux entités critiques, le paragraphe 2 est rédigé en s'inspirant de l'article 6, paragraphe 1er, de la loi portant création d'un Haut-Commissariat à la Protection nationale. L'article précité sera abrogé lorsque le présent projet entrera en vigueur.

Le paragraphe 3 de l'article 7 fixe les critères à prendre en compte afin de déterminer l'importance de l'effet perturbateur causé par un incident en vue du recensement des entités critiques. Les critères en question répondent en grande partie aux critères inscrits dans le règlement grand-ducal du 21 février 2018 déterminant les modalités du recensement et de la désignation des infrastructures critiques. Ces critères sont appréciés et analysés en fonction des spécificités de chaque secteur par un des groupes de travail interministériels qui procèdent à l'identification des infrastructures critiques en vue de leur désignation par arrêté grand-ducal.

Notons que, vu que les infrastructures critiques recensées et désignées en application de la loi modifiée du 23 juillet 2016[29] répondent toutes aux critères ci-avant, celles-ci seront considérées comme entités critiques en vertu de la présente loi sous projet.

Le paragraphe 4 exige, d'une part, que les autorités compétentes dressent une liste des entités recensées et désignées critiques et, d'autre part, que les entités critiques reçoivent une notification les informant de leur statut d'entité critique endéans un mois à compter de leur désignation. En outre, ces entités sont informées des obligations qui leur incombent en vertu des chapitres 4 et 5. Remarquons que les entités critiques des secteurs figurant aux points 3 et 4 de l'annexe, ainsi que les entités critiques figurant au point 8 de l'annexe pour les activités qui tombent sous la surveillance de la Commission de surveillance du secteur financier, ne sont pas soumises à ces obligations. Ce bout de phrase est en étroite relation avec le libellé de l'article 8 et sera donc approfondi dans le commentaire de cet article.

Le cinquième paragraphe de l'article 7 vise le cas spécial de l'entité critique qui fournirait des services essentiels à ou dans six États membres ou plus. En effet, puisque les entités critiques exercent leurs activités dans le cadre d'un réseau de fourniture de services et d'infrastructures de plus en plus interconnecté et fournissent souvent des services essentiels dans plus d'un État membre, certaines de ces entités critiques revêtent une importance particulière pour l'Union et son marché intérieur. Ainsi, afin de tenir compte de cette réalité, la directive et le projet de loi ont introduit la notion d'« entité critique d'importance européenne particulière » et accordent à celle-ci un soutien renforcé au niveau de l'Union, telles que les missions de conseil[30]. Au niveau du recensement, si une entité critique se retrouve à fournir des services essentiels dans six États membres différents au moins, ladite entité en informe, conformément au paragraphe 5, son autorité compétente.

Afin d'assurer la cohérence entre la transposition de la directive CER et la directive NIS 2, les autorités compétentes notifient aux autorités compétentes de la directive NIS 2 l'identité des entités critiques qu'ils ont recensées et désignées.

Finalement, l'article 7 prévoit dans son dernier paragraphe une revue régulière de la liste des entités critiques.

Ad article 8

L'article 8 vise à tenir compte du statut spécial dont jouissent les entités qui tombent sous la surveillance de la Commission de surveillance du secteur financier. En effet, le droit de l'Union et le droit national imposent aux entités concernées des exigences étendues visant à ce que tous les risques auxquels elles sont confrontées soient gérés et à garantir la continuité des activités. Ce droit comprend les règlements (UE) 648/2012,[31] (UE) 575/2013[32] et (UE) 600/2014,[33] ainsi que la loi modifiée du 5 avril

---

29 Loi modifiée du 23 juillet 2016, *o.c.*, (v. note 6).

30 Consid. (35) directive CER.

31 Règlement (UE) 648/2012 du Parlement européen et du Conseil du 4 juillet 2012 sur les produits dérivés de gré à gré, les contreparties centrales et les référentiels centraux, *J.O.U.E.*, L 201 du 27 juillet 2012, p. 1.

32 Règlement (UE) 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) 64812012, *J.O.U.E.*, L 176 du 27 juin 2013, p. 1.

33 Règlement (UE) 600/2014 du Parlement européen et du Conseil du 15 mai 20I4 concernant les marchés d'instruments financiers et modifiant le règlement (UE) 648/2012, *J.O.U.E.*, L 173 du 12 juin 2014, p. 84.

1993 relative au secteur financier[34] et la loi modifiée du 30 mai 2018 relative aux marchés d'instruments financiers.[35] Ce cadre juridique est complété par le règlement (UE) 2022/2554 du Parlement européen et du Conseil,[36] qui fixe des exigences applicables aux entités financières en matière de gestion des risques liés aux technologies de l'information et de la communication (TIC), y compris en matière de protection des infrastructures physiques des TIC. Étant donné que la résilience de ces entités est dès lors entièrement couverte, l'article 10 et les chapitres 4, 5 et 6 de la présente loi sous projet ne devraient pas s'appliquer à ces entités, afin d'éviter des doubles emplois et des charges administratives inutiles.[37]

Toutefois, la directive estime que vu l'importance des services fournis par les entités du secteur financier et bancaire à des entités critiques appartenant à tous les autres secteurs, les autorités compétentes devraient recenser les entités de ces secteurs en tant qu'entités critiques. Par conséquent, les stratégies, les évaluations des risques des autorités compétentes et les mesures de soutien énoncées au chapitre 3 leur seraient entièrement applicables.[38]

En ce qui concerne les infrastructures numériques visées par le point 8 du tableau en annexe, les auteurs du projet de loi estiment que la directive devrait leur être partiellement applicable lorsque leur activité tombe sous la surveillance de la CSSF. Ces activités sont, en effet, entièrement couvertes par les dispositions du secteur financier, énoncées ci-dessus. En ce qui concerne les activités des infrastructures numériques qui ne tombent pas sous la surveillance de la CSSF, la présente loi sous projet leur devrait être pleinement applicable, dans la mesure où la directive CER donne la possibilité aux États membres d'adopter ou de maintenir des dispositions de droit national afin d'atteindre un niveau de résilience plus élevé. Alors qu'il est vrai que ces activités tombent sous l'égide de la loi portant transposition de la directive NIS 2, celle-ci ne visera que la résilience cybernétique.

Si dans le futur, il y avait des législations sectorielles qui s'appliquaient aux infrastructures numériques, dont l'activité ne tombe pas sous la surveillance de la CSSF, et qui avaient un effet au moins équivalent aux obligations du projet de loi sous rubrique, l'article 1er, paragraphe 2, aurait pour effet de dispenser l'application du projet de loi à ces entités.

Ad article 9

Sans préjudice de la propre responsabilité juridique qui incombe aux entités critiques de garantir le respect des obligations prévues par le projet de loi, les autorités compétentes aident les entités critiques à renforcer leur résilience. En particulier, lesdites autorités élaborent des documents d'orientation et des méthodologies, apportent leur soutien à l'organisation d'exercices visant à tester la résilience des entités critiques, dispensent des formations et fournissent des conseils au personnel des entités critiques.[39]

Il est à noter que déjà à l'heure actuelle, le HCPN apporte un soutien aux infrastructures critiques. En effet, sont actuellement en place :

– un guide pour l'élaboration d'un plan de sécurité et de continuité de l'activité ;
– des recommandations sectorielles sur la protection, la continuité de l'activité, la gestion de crise et la résilience ;
– des recommandations sur les mesures de protection, de continuité de l'activité, de gestion de crise et de résilience contenues dans les plans de sécurité et de continuité de l'activité de différents opérateurs d'infrastructures critiques ; des guides pour la protection et la résilience face à des risques spécifiques (intempéries, inondation, …) ;
– des colloques d'échanges sur les retours d'expériences et les leçons apprises entre opérateurs d'infrastructures critiques ;
– des conseils particuliers sur demandes ponctuelles des opérateurs ; et

---

34 *Mém.* A n° 27, 10 avril 1993, p. 462.

35 *Mém.* A n° 446, 31 mai 2018.

36 Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) 1060/2009, (UE) 648/2012, (UE) 600/2014, (UE) 909/2014 et (UE) 2016/1011, *J.O.U.E.*, L 333 du 27 décembre 2022, p. 1.

37 Consid. (21) directive CER.

38 Consid. (21) directive CER.

39 Consid. (25) directive CER.

– le partage de lettres de veille, telles que la newsletter « Critical Infrastructure Resilience : News, Updates and Events » de la Commission européenne, avec les opérateurs d'infrastructures critiques.

Ad article 10

L'article 10 règle la coopération entre États membres dans les cas où une entité critique exerçait ses activités dans plusieurs États membres. Dans cette hypothèse, il importe de transmettre des exigences convergentes aux entités critiques afin que celles-ci puissent augmenter leur résilience sans pour autant accroitre leur charge adminristrative.[40]

Ad article 11

L' article 11 impose aux entités critiques de procéder à une évaluation des risques. En effet, afin de pouvoir augmenter leur résilience, ces entités doivent avoir une connaissance approfondie des risques pertinents auxquels elles sont exposées. À cette fin, elles procèdent à une première évaluation des risques neuf mois suivant la réception de la notification qui les informe qu'elles ont été désignées en tant qu'entité critique. Ensuite, cette évaluation des risques est mise à jour chaque fois que cela s'avère nécessaire compte tenu de leurs circonstances particulières et de l'évolution de ces risques et, en tout cas, tous les quatre ans.[41]

Ad article 12

Après avoir évalué les risques les concernant, l'article 12 du projet de loi invite les entités critiques à mettre en place des mesures techniques, des mesures de sécurité et des mesures organisationnelles appropriées et proportionnées aux risques auxquels elles sont confrontées. Les mesures en question répondent en grande partie aux mesures que les infrastructures critiques doivent déjà aujourd'hui détailler et mettre en place en vertu des plans de continuité et de sécurité de l'activité prévus à l'article 8 de la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale.

D'abord, ces mesures sont destinées à prévenir tout incident et à s'en protéger. En ce qui concerne la protection physique de l'infrastructure, les entités pourraient prendre en considération, par exemple, des clôtures, des barrières, des outils et procédures de surveillance des enceintes, et des équipements de détection et de contrôle des accès.[42] Ensuite, les mesures techniques visent à réagir et à résister aux incidents et devraient servir à faire une gestion adéquate de la sécurité liée au personnel. Finalement, il faut que ces mesures permettent à l'entité de se remettre des incidents. Il découle en outre de l'article que le personnel de l'entité devra être sensibilisé adéquatement des mesures mises en place.

Le deuxième paragraphe stipule que les entités critiques devraient décrire les mesures qu'elles prennent avec un niveau de détail suffisant, eu égard aux risques identifiés, dans un plan de résilience ou dans un ou plusieurs documents équivalents, et appliquer ce plan dans la pratique. A l'instar de ce qui est prévu pour l'évaluation des risques effectuée par les entités critiques et pour éviter les doubles emplois, l'article 12 permet aux entités critiques d'utiliser les mesures prises en vertu d'autres actes juridiques, afin de satisfaire aux exigences du présent article. Notons que la directive énonce quelques exemples de mesures dans les domaines de l'aviation, du transport maritime, du réseau routier et du secteur ferroviaire qui pourraient satisfaire à ces exigences.[43]

Ad article 13

L'article 13 met en place un système de vérification des antécédents pour des catégories spécifiques de personnel employé par les entités critiques, visées dans au paragraphe 1er, afin de pallier au risque que des membres du personnel utilisent, par exemple, de manière abusive leurs fonctions ou encore leurs droits d'accès au sein de l'organisation de l'entité critique.

Plus précisément, à l'instar du système de vérification des antécédents mis en place par la loi modifiée du 18 juillet 2018 sur la Police grand-ducale,[44] le règlement grand-ducal du 28 juillet 2018 portant

---

40 Consid. (26) directive CER.

41 Consid. (28) directive CER.

42 Art. 13, para. 1er, lettre b), directive CER.

43 Consid. (31) directive CER.

44 Art. 26 de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale, *Mém. A* n° 621, 28 juillet 2018.

exécution de l'article 26 de la loi du 18 juillet 2018 sur la Police grand-ducale pour les institutions de l'Union européenne[45] et le projet de loi 7475[46] et son projet de règlement grand-ducal d'exécution,[47] la Police grand-ducale est l'autorité étatique en charge des demandes de vérification des antécédents introduites par les entités critiques. Ainsi, la Police grand-ducale est à considérer comme responsable du traitement au sens de la législation sur la protection des données à caractère personnel. Avec la compétence de la Police grand-ducale, ce système se distingue fondamentalement des procédures de « contrôle d'honorabilité » mises en place par le projet de loi n° 7691[48] qui confient cette mission au Ministre de la Justice, voire au procureur général d'État.

Le paragraphe 1er de l'article 13 reprend la finalité du traitement, à savoir l'évaluation du risque potentiel pour la sécurité de l'entité concernée, et les catégories de personnes occupant une fonction sensible au sein de l'entité pour lesquelles une demande de vérification des antécédents peut être introduite. En vertu de l'article 12, paragraphe 1er, point 5, l'entité critique devra informer l'autorité compétente quelles fonctions considérées « sensibles » au sein de son entité nécessitent une vérification des antécédents. Vu qu'il reviendra à l'autorité compétente, dans sa fonction de supervision, de se prononcer par rapport aux mesures de résilience proposées par l'entité critique en vertu de l'article 12, le texte sous projet précise que les catégories de personnes au sujet desquelles une vérification est demandée devra, préalablement à l'introduction de la demande, faire l'objet d'un avis favorable par l'autorité compétente. Les auteurs du projet de loi veulent ainsi assurer qu'il y ait, à travers les entités critiques, une certaine cohérence par rapport aux catégories de personnes au sujet desquelles une vérification des antécédents est demandée.

Le deuxième paragraphe se base sur le système mis en place par le projet de loi n° 7475 en énumérant les informations qui devront figurer dans le dossier introduit par l'entité critique. Notons que cette énumération a été largement reprise du projet de règlement grand-ducal portant exécution du projet de loi n° 7475.

D'après le troisième paragraphe, la Police grand-ducale informe l'entité critique si la personne concernée a commis ou tenté de commettre une des infractions décrites à l'article 14, paragraphe 3. Notons que le rôle de la Police se limitera à vérifier si la personne a des antécédents et, le cas échéant, d'analyser ces antécédents au regard des trois types de critères. Il s'agit de cette manière d'assurer que la Police n'ait à répondre que par rapport à l'existence des critères ciblés et spécifiques et que l'entité critique n'obtienne pas de données personnelles.

Finalement, le quatrième paragraphe détermine la durée de validité des vérifications et précise les modalités de renouvellement de celles-ci.

Ad article 14

Le premier paragraphe de l'article 14 précise que la Police grand-ducale pourra, afin d'établir l'identité de la personne visée par la vérification des antécédents, prendre contact avec les autorités policières étrangères. En outre, si la personne au sujet de laquelle une vérification est effectuée ne dispose pas de la nationalité luxembourgeoise ou est résidente d'un pays étranger, la Police grand-ducale a le droit d'adresser une demande motivée au procureur général d'État en vue d'obtenir un

---

45 Règlement grand-ducal du 28 juillet 2018 portant exécution de l'article 26 de la loi du 18 juillet 2018 sur la Police grand-ducale pour les institutions de l'Union européenne, *Mém. A* n° 647, 3 août 2018.

46 Projet de loi portant modification de la loi modifiée du 26 juillet 2002 sur la police et sur l'exploitation de l'aéroport de Luxembourg ainsi que sur la construction d'une nouvelle aérogare, *doc. parl.* n° 7475.

47 Projet de règlement grand-ducal relatif à la sûreté de l'aviation civile et aux conditions d'accès à l'aéroport de Luxembourg.

48 Projet de loi portant modification 1° du Code de procédure pénale 2° du Nouveau Code de procédure civile 3° de la loi du 7 juillet 1971 portant en matière répressive et administrative, institution d'experts, de traducteurs et d'interprètes assermentés et complétant les dispositions légales relatives à l'assermentation des experts, traducteurs et interprètes 4° de la loi modifiée du 9 décembre 1976 relative a l'organisation du notariat 5° de la loi modifiée du 20 avril 1977 sur les jeux de hasard et les paris sportifs 6° de la loi modifiée du 7 mars 1980 sur l'organisation judiciaire 7° de la loi modifiée du 7 novembre 1996 portant organisation des juridictions de l'ordre administratif 8° de la loi du 30 décembre 1981 portant indemnisation en cas de détention préventive inopérante 9° de la loi modifiée du 15 mars 1983 sur les armes et munitions 10° de la loi modifiée du 2 mars I984 relative à l'indemnisation de certaines victimes de dommages corporels résultant d'une infraction et à la répression de l'insolvabilité frauduleuse 11° de la loi modifiée du 4 décembre 1990 portant organisation du service des huissiers de justice 12° de la loi du 31 janvier 1998 portant agrément des services d'adoption et définition des obligations leur incombant 13° de la loi du 6 mai 1999 relative à la médiation pénale et portant modification de différentes dispositions a) de la loi modifiée du 7 mars 1980 sur l'organisation judiciaire, b) du code des assurances sociales 14° de la loi du 12 novembre 2002 relative aux activités privées de gardiennage et de surveillance 15° de la loi modifiée du 7 juin 2012 sur les attachés de justice, *doc. parl.* n° 7691[7].

extrait de son casier judiciaire du pays dont elle a la nationalité ou du ou des pays dans lesquels elle a résidé au cours des cinq dernières années.

Selon le deuxième paragraphe, la Police grand-ducale a le droit de consulter tout employeur ou établissement d'éducation antérieur ou actuel, afin de vérifier l'authenticité des informations fournies.

Ensuite, le troisième paragraphe permet à la Police grand-ducale de prendre contact avec la personne au sujet de laquelle une vérification est effectuée afin de demander tout renseignement complémentaire qu'elle juge nécessaire par rapport aux éléments fournis dans la demande de vérification des antécédents.

Enfin, le quatrième paragraphe fait état des critères pris en compte par la Police grand-ducale dans son avis adressé à l'entité critique. Ainsi, la Police grand-ducale indique dans son avis, d'une part, si la personne concernée a commis ou tenté de commettre une des infractions contre la sûreté de l'État ou une des infractions en matière de corruption et, d'autre part, si elle a fait de fausses déclarations dans le cadre de la demande de vérification des antécédents. Remarquons que l'avis de la Police grand-ducale se limite à indiquer si, oui ou non, la personne tombe dans un des trois points énumérés au quatrième paragraphe, sans spécifier quel serait le point concerné ou donner davantage de détails.

Ad article 15

L'article 15 autorise la mise en place d'un système informatique centralisé permettant la gestion administrative des demandes de vérification des antécédents et règle la protection des données personnelles des personnes soumises à une vérification des antécédents. Le projet de loi essaye de trouver un équilibre entre le droit de la personne soumise à la vérification et la nécessité pour la Police grand-ducale d'avoir accès aux vérifications antérieurement effectuées. Ainsi, la loi prévoit que la Police conserve les données concernées pendant une année à partir de la notification de l'avis à l'entité critique.

Ad article 16

L'article 16 met en place un mécanisme de notification d'incidents afin de permettre aux autorités compétentes de réagir rapidement et de manière adéquate aux incidents d'une certaine importance et de disposer d'une vue d'ensemble complète de l'impact, de la nature, de la cause et des conséquences éventuelles d'incidents auxquels les entités critiques sont confrontées.[49]

Ainsi, les entités critiques notifient, sans retard injustifié, aux autorités compétentes les incidents qui perturbent ou sont susceptibles de perturber de manière importante la fourniture de services essentiels. Alors que le texte du projet de loi précise trois critères à prendre en compte pour déterminer l'importance de la perturbation, il est prévu qu'un règlement grand-ducal précisera ces critères pour chaque secteur retenu en annexe.

À moins qu'elles n'en soient empêchées sur le plan opérationnel, les entités critiques présentent une notification initiale au plus tard vingt-quatre heures après avoir pris connaissance d'un incident. La notification initiale ne devrait inclure que les informations strictement nécessaires pour porter l'incident à la connaissance de l'autorité compétente et permettre à l'entité critique de demander une assistance, si nécessaire. Une telle notification devrait indiquer, lorsque cela est possible, la cause présumée de l'incident. La notification initiale est suivie, s'il y a lieu, d'un rapport détaillé au plus tard un mois après l'incident. Le rapport détaillé devrait compléter la notification initiale et fournir une vue d'ensemble plus complète de l'incident.[50]

Ad article 17

Alors que le projet de loi ne reprend le détail des obligations qui incombent à la Commission européenne dans ce contexte, l'article 17 se limite, dans son paragraphe 1er, à définir les entités critiques d'importance européenne particulière et impose à celles-ci d'accorder aux missions de conseil organisées par la Commission accès à leurs informations, systèmes et installations, en son paragraphe 2.

---

49 Consid. (33) directive CER.

50 Consid. (33) directive CER.

Ad article 18

Afin que la bonne application et l'exécution de la présente loi sous projet soient assurées, le premier paragraphe de l'article 18 stipule que les autorités compétentes jouissent du pouvoir d'effectuer des inspections et des audits, de superviser les mesures mises en place par les entités critiques, voire d'exiger des entités critiques qu'elles fournissent des informations et des éléments de preuve concernant les mesures qu'elles ont prises pour respecter leurs obligations et, lorsque c'est nécessaire, d'adresser des injonctions afin qu'il soit remédié aux violations constatées.

Le deuxième alinéa du premier paragraphe encadre les pouvoirs de police administrative prévus par le premier alinéa. Ainsi, les inspections ne peuvent avoir lieu qu'à des plages horaires prédéfinies, moyennant préavis de deux semaines, par un agent des groupes de traitement ou d'indemnité A1 ou A2 de l'autorité compétente. Ces inspections pourront aussi se dérouler en dehors des plages horaires prédéfinies dans le présent projet avec l'accord de l'entité critique. Notons que puisque le chapitre 6 sur la supervision et l'exécution ne s'applique au secteur bancaire, aux infrastructures des marchés financiers et aux infrastructures numériques pour lesquels la CSSF est l'autorité compétente, seul le HCPN sera concerné par ces inspections.

Dans un souci de transparence, il est prévu que lorsqu'ils procèdent à une inspection, les agents du HCPN signalent leur présence à l'agent de liaison désigné par l'entité critique en vertu de l'article 12, paragraphe 3, du projet de loi. L'agent de liaison peut accompagner les agents du HCPN lors de l'inspection. Cet article s'inspire de la loi modifiée du 19 mai 1999[51] qui prévoit des garanties similaires dans le cadre de pouvoirs de contrôle accordés aux agents de la Direction de l'aviation civile.

Finalement, les agents procédant à l'inspection dressent un rapport relatif à l'inspection opérée, qui est transmis à l'agent de liaison de l'entité.

Le deuxième paragraphe fait le lien entre la directive CER et la directive NIS 2. En effet, comme évoqué précédemment, il se pourrait qu'une entité essentielle sous l'égide de la directive NIS 2 soit aussi recensée en tant qu'entité critique. Ainsi, ces entités sont tenues de fournir aux autorités compétentes de la loi sous projet les informations nécessaires pour évaluer leurs mesures de résilience, ainsi que des éléments prouvant la mise en œuvre effective de ces mesures.

Dans un but de cohérence entre le régime actuellement applicable aux infrastructures critiques et le futur régime applicable aux entités critiques, la formulation du paragraphe 2, alinéa 1er, s'inspire du libellé de l'article 6 de la loi portant création d'un Haut-Commissariat à la Protection nationale qui sera abrogé avec l'entrée en vigueur du présent projet.[52] Dans la même lignée, le deuxième alinéa du paragraphe 2 est repris de la même loi du 23 juillet 2016. Cette disposition permettra au HCPN, qui porte la double casquette de gestionnaire de crises et d'autorité compétente en matière d'entités critiques, de faire le lien entre ces deux compétences.

Le troisième paragraphe permet aux autorités compétentes d'adresser des injonctions aux entités critiques afin que celles-ci remédient aux violations constatées au présent projet de loi. A nouveau, cette disposition trace un parallélisme avec l'article 9, paragraphe 2, de la loi du 28 mai 2019,[53] qui impose un régime similaire aux opérateurs de services essentiels. Ainsi, le projet de loi vise à instaurer une égalité de traitement entre entités critiques et opérateurs de services essentiels.

Les pouvoirs dont les autorités compétentes jouissent en vertu des paragraphes 1 à 3 ne peuvent s'exercer que sous réserve de garanties appropriées. Ainsi, ces pouvoirs devront titre exercés de manière objective, transparente et proportionnée, tout en tenant compte des droits et les intérêts légitimes des entités critiques concernées, tels que la protection des secrets commerciaux et d'affaires, le droit d'être entendu, les droits de la défense et le droit à un recours effectif devant une juridiction indépendante.[54]

Le paragraphe 4 de l'article 18 prévoit que lorsqu'elles évaluent le respect par les entités critiques des obligations que leur impose la présente loi sous projet, les autorités compétentes peuvent demander aux autorités compétentes en vertu de la directive NIS 2 d'exercer leurs pouvoirs de supervision et

---

51 Art. 19*bis*, para. 4, de la loi du 19 mai 1999 ayant pour objet a) de réglementer l'accès au marché de l'assistance en escale à l'aéroport de Luxembourg, b) de créer un cadre réglementaire dans le domaine de la sûreté de l'aviation civile, et c) d'instituer une Direction de l'Aviation Civile, *Mém. A* n°57, 21 mai 1999, p. 1339.

52 Loi modifiée du 23 juillet 2016, *o.c.*, (v. note 6), art. 6, al. 1er.

53 Loi du 28 mai 2019 portant transposition de la directive (UE) 2016/1148, *o.c.*, (v. note 3).

54 Art. 21, para. 4, directive CER.

d'exécution à l'égard d'une entité relevant de ladite directive qui a été désignée en tant qu'entité critique en vertu du présent projet de loi.

Ad article 19

Afin d'assurer que la présente loi soit appliquée en pratique, il y a lieu de l'assortir de sanctions administratives adéquates. Ainsi, l'autorité compétente peut décider des sanctions à l'encontre des entités critiques si elles ne se conforment pas aux prescriptions des articles 11, 12, 16 et 18.

Remarquons que les sanctions administratives énumérées dans l'article 19 et la procédure y relative s'inspirent fortement de la législation existante dans le secteur des opérateurs des services essentiels.[55]

Ad article 20

Alors que le la loi du 17 juin 2022[56] avait introduit la possibilité d'allouer une prime d'astreinte d'une valeur de 12 points indiciaires au personnel du Haut-Commissariat à la Protection nationale, il s'est avéré nécessaire de préciser cette disposition davantage. En effet, ne sont visés par cette disposition uniquement les agents qui assurent que le Centre national de crise, qui accueille les cellules de crise en cas d'urgence, soit en tout temps opérationnel.

Ad article 21

L'article 21 du projet de loi procède à des modifications de la loi-cadre du Haut-Commissariat à la Protection nationale afin d'y intégrer le nouveau vocabulaire, d'une part, et de procéder à des adaptations ponctuelles devenues nécessaires, d'autre part.

En ce qui concerne les entités critiques, l'article 21 remplace d'abord la notion d'« infrastructure critique » par celle d' « entité critique » à travers le texte de la loi du Haut-Commissariat à la Protection nationale, afin d'accorder une suite au nouveau vocabulaire introduit par la directive CER. Dans la même optique, le point 3 de l'article 21 reformule et adapte les missions du HCPN en matière d'entités critiques à la terminologie instaurée par la directive. Enfin, le projet de loi abroge les articles 4 à 8 relatifs aux infrastructures critiques. En effet, alors que la législation sur les infrastructures critiques faisait, depuis 2016, partie intégrante de la loi organique du Haut-Commissariat à la Protection nationale, il a été jugé plus logique de transposer la directive CER avec une loi spéciale à part entière, d'autant plus que le HCPN se partagera dorénavant le rôle de l'autorité compétente avec la Commission de surveillance du secteur financier. L'article 9, dernière disposition du chapitre relatif aux infrastructures critiques, restera dans la loi organique du HCPN, puisqu'il règle la situation des entités critiques en cas de crise.

Ad article 22

Finalement, l'article 22 introduit un intitulé de citation, afin de faciliter la référence à la présente loi sous projet.

Annexe

L'annexe du projet de loi a été repris de l'annexe de la directive CER. L'unique différence consiste dans le fait qu'au-delà des secteurs prévus par la directive, l'annexe du projet ajoute la « gestion des déchets » comme douzième secteur. Comme ce secteur est déjà à l'heure actuelle un secteur dans lequel sont recensées des infrastructures critiques[57] et comme ce secteur joue et continuera à jouer un rôle essentiel, il a été décidé de l'ajouter à la liste des secteurs.

*

---

55 Art. 14 de la loi du 28 mai 2019 portant transposition de la directive (UE) 2016/1148, *o.c.*, (v. note 3).

56 Loi du 17 juin 2022 modifiant : 1° la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale ; 2° la loi modifiée du 9 décembre 2005 déterminant les conditions et modalités de nomination de certains fonctionnaires occupant des fonctions dirigeantes dans les administrations et services de l'État ; 3° la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État ; 4° la loi modifiée du 8 avril 2018 sur les marchés publics, *Mém. A* n° 315, 29 juin 2022.

57 Art. 1er, point 6, du règlement grand-ducal du 21 février 2018 déterminant les modalités du recensement et de la désignation des infrastructures critiques, *Mém. A* n°152, 1er mars 2018.

TEXTES LEGISLATIFS COORDONNES

LOI MODIFIEE DU 23 JUILLET 2016

portant création d'un Haut-Commissariat à la Protection nationale et modifiant

a) la loi modifiée du 23 juillet 1952 concernant l'organisation militaire;

b) la loi du 8 décembre 1981 sur les réquisitions en cas de conflit armé, de crise internationale grave ou de catastrophe;

c) la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel;

d) la loi modifiée du 25 juin 2009 sur les marchés publics;

e) la loi modifiée du 9 décembre 2005 déterminant les conditions et modalités de nomination de certains fonctionnaires occupant des fonctions dirigeantes dans les administrations et services de l'Etat;

f) la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'Etat

Chapitre 1er – Objet

Art. 1er. Il est créé une administration dénommée Haut-Commissariat à la Protection nationale, dont les compétences et les mécanismes selon lesquels elle intervient sont déterminés par la présente loi qui régie également l'organisation de la protection des ~~infrastructures critiques~~ entités critiques.

Le Haut-Commissariat à la Protection nationale est placé sous l'autorité du membre du Gouvernement ayant dans ses attributions la Protection nationale.

Chapitre 2 – Définitions

Art. 2. Pour l'application de la présente loi, on entend par

1. « concept de protection nationale » : un concept qui consiste à prévenir les crises, respectivement à protéger le pays et la population contre les effets d'une crise. En cas de survenance d'une crise, il comprend la gestion des mesures et activités destinées à faire face à la crise et à ses effets et à favoriser le retour à l'état normal ;
2. « crise » : tout évènement qui, par sa nature ou ses effets, porte préjudice aux intérêts vitaux ou aux besoins essentiels de tout ou partie du pays ou de la population, qui requiert des décisions urgentes et qui exige une coordination au niveau national des actions du Gouvernement, des administrations, des services et organismes relevant des pouvoirs publics, et, si besoin en est, également au niveau international ;
3. « gestion de crises » : l'ensemble des mesures et activités que le Gouvernement initie, le cas échéant avec le concours des autorités communales concernées, pour faire face à la crise et à ses effets et pour favoriser le retour à l'état normal ;

~~4. « infrastructure critique» : tout point, système ou partie de celui ci qui est indispensable à la sauvegarde des intérêts vitaux ou des besoins essentiels de tout ou partie du pays ou de la population~~
4. « entité critique » : une entité au sens de la loi du XXX sur la résilience des entités critiques ;

4*bis*. « sécurité de l'information » : sécurité autour des réseaux et systèmes d'information non classifiés installés et exploités par les administrations et services de l'État ;

5. « stratégie nationale en matière de sécurité des réseaux et des systèmes d'information » : un cadre prévoyant des objectifs et priorités stratégiques en matière de sécurité des réseaux et des systèmes d'information au niveau national.

Chapitre 3 – Mission et attributions du Haut-Commissariat à la Protection nationale

Art. 3. (1) Le Haut-Commissariat à la Protection nationale a pour mission de mettre en oeuvre le concept de protection nationale tel que défini à l'article 2. Dans le cadre de cette mission, le Haut-Commissariat à la Protection nationale a pour attributions

a) quant aux mesures de prévention de crises :

1. de coordonner les contributions des ministères, administrations et services de l'État ;
2. de coordonner les politiques, les projets et les programmes de recherche ;
3. de procéder à l'analyse des risques et à l'organisation d'une veille ;
4. de coordonner l'organisation des cours de formation et des exercices ;

b) quant aux mesures d'anticipation de crises :

1. de développer et de coordonner une stratégie nationale de gestion de crises ;
2. de définir la typologie, la structure, le corps et le format des plans déclinant les mesures et activités de prévention et de gestion de crises et de coordonner la planification ;
3. de veiller à l'exécution des mesures relatives à la résilience des entités critiques en application de la loi du XXX sur la résilience des entités critiques ; ~~d'initier, de coordonner et de veiller à l'exécution des activités et mesures relatives au recensement, à la désignation et à la protection des infrastructures critiques, qu'elles soient publiques ou privées ;~~
4. de coordonner et d'élaborer une stratégie nationale en matière de sécurité des réseaux et des systèmes d'information ;

c) quant aux mesures de gestion de crises :

1. d'initier, de conduire et de coordonner les tâches de gestion de crises ;
2. de veiller à l'exécution de toutes les décisions prises ;
3. de favoriser le plus rapidement possible le retour à l'état normal ;
4. de préparer un budget commun pour la gestion de crises et de veiller à son exécution ;
5. de veiller à la mise en place et au fonctionnement du Centre national de crise.

Dans le cadre de ses attributions, le Haut-Commissariat à la Protection nationale est le point de contact du Luxembourg auprès des institutions et organisations européennes et internationales et veille â une coopération efficace avec ces entités.

(1*bis*) Le Haut-Commissariat à la Protection nationale est encore chargé des missions suivantes :

a) attributions dans sa fonction d'Agence nationale de la sécurité des systèmes d'information, ci-après « ANSSI » ;

b) attributions dans sa fonction de Centre de traitement des urgences informatiques, ci-après « CERT Gouvernemental » ;

c) attributions dans sa fonction de Service de la communication de crise, ci-après « SCC ».

(1*ter*) Dans sa fonction d'ANSSI, le Haut-Commissariat à la Protection nationale a pour missions :

a) de contribuer à la mise en oeuvre de la politique générale de sécurité de l'information de l'État ;

b) de contribuer à la mise en oeuvre, en concertation avec les administrations et services de l'État, des politiques et lignes directrices de sécurité de l'information portant sur les domaines de la politique générale de sécurité de l'information de l'État et des nouvelles technologies de l'information et de la communication ;

c) d'émettre des recommandations d'implémentation des politiques et lignes directrices de sécurité de l'information et d'assister les administrations et services de l'État au niveau de l'implémentation des mesures proposées ;

d) de définir, en concertation avec les administrations et services de l'État, une approche de gestion des risques, en vue de constituer un plan d'évaluation et d'identification des risques concernant la sécurité de l'information et d'accompagner, à leur demande, les administrations et services de l'État dans l'analyse et la gestion des risques ;

e) de conseiller l'Institut national d'administration publique, respectivement, à leur demande, les administrations et services de l'État dans la définition d'un programme de formation dans le domaine de la sécurité de l'information ;

f) promouvoir la sécurité de l'information par le biais de mesures de sensibilisation ;

g) de conseiller, à leur demande, les établissements publics et les entités critiques ~~infrastructures critiques~~ en matière de sécurité des réseaux et systèmes d'information et des risques y liés ;

h) d'assurer la fonction d'autorité TEMPEST en veillant à la conformité des réseaux et systèmes d'information classifiés aux stratégies et lignes directrices TEMPEST et en approuvant les contre-mesures TEMPEST pour les installations et les produits destinés à protéger des pièces classifiées jusqu'à un certain niveau de classification dans leur environnement opérationnel.

(1*quater*) Dans sa fonction de CERT Gouvernemental, le Haut-Commissariat à la Protection nationale a pour missions :

a) de constituer le point de contact unique dédié au traitement des incidents de sécurité d'envergure affectant les réseaux et les systèmes d'information des administrations et services de l'État et, à leur demande, des établissements publics et des entités critiques ~~infrastructures critiques~~ ;

b) d'assurer un service de veille, de détection, d'alerte et de réaction aux attaques informatiques et aux incidents de sécurité d'envergure affectant les réseaux et systèmes d'information des administrations et services de l'État et, à leur demande, des établissements publics et des entités critiques ~~infrastructures critiques~~ ;

c) d'assurer la fonction de centre national de traitement des urgences informatiques, dénommé CERT National, en

1. opérant comme le point de contact officiel national pour les CERTs nationaux et gouvernementaux étrangers ;
2. opérant comme le point de contact officiel national pour la collecte et la distribution d'informations relatives aux incidents de sécurité qui concernent les réseaux et systèmes d'information implantés au Luxembourg ;
3. relayant les informations collectées aux CERTs sectoriels en charge de la cible d'une attaque ou à défaut de CERT sectoriel, directement à la cible.

d) d'assurer la fonction de centre militaire de traitement des urgences informatiques, dénommé CERT Militaire, en

1. opérant comme le point de contact officiel national pour les CERTs militaires étrangers ;
2. assurant un service de veille, de détection, d'alerte et de réaction aux attaques informatiques et aux incidents de sécurité d'envergure affectant les réseaux et les systèmes d'information de l'armée à partir du territoire du Grand-Duché ;
3. opérant, à partir du territoire du Grand-Duché, une équipe d'intervention spécialisée capable de prendre en charge la réponse aux incidents de sécurité d'envergure liés à ces réseaux et systèmes d'information.

Le Haut-Commissaire à la Protection nationale peut, dans l'intérêt de l'exécution des missions du CERT Gouvernemental, demander leur concours aux agents des administrations et services de l'État.

(1*quinquies*) Dans sa fonction de Service de la communication de crise, le Haut-Commissariat à la Protection nationale a pour missions :

a) de coordonner la communication de crise avant, pendant et après des situations de crise pouvant frapper le territoire national, par l'intermédiaire des médias, l'internet et les réseaux sociaux ;

b) d'effectuer une communication préventive et pédagogique en sensibilisant les médias et le public sur les questions relevant de la protection du pays, de ses sites sensibles et de sa population ;

c) de créer et de maintenir des contacts étroits et réguliers avec les services de communication de crise étrangers.

(2) Les autorités administratives et judiciaires, la Police grand-ducale et le Haut-Commissariat à la Protection nationale veillent à assurer une coopération efficace en matière de communication des informations susceptibles d'avoir un rapport avec leurs missions.

(3) Le Haut-Commissaire à la Protection nationale ou son délégué peuvent, par demande écrite, demander à tout détenteur d'un secret professionnel ou d'un secret protégé par une clause contractuelle la communication des informations couvertes par ce secret si la révélation dudit secret est nécessaire à l'exercice de sa mission de gestion de crises ou de protection des ~~infrastructures critiques~~ entités critiques. Une divulgation d'informations en réponse à une telle demande n'entraîne pour l'organisme ou la personne détenteur des informations secrètes aucune responsabilité.

(4) Les informations qui sont couvertes par le secret de l'instruction relative à une enquête judiciaire concomitante ne peuvent être transmises qu'avec l'accord de la juridiction ou du magistrat saisi du dossier.

Chapitre 4 – La protection des entités critiques
~~Chapitre 4 – La protection des infrastructures critiques~~

~~**Art. 4.** La protection de l'infrastructure critique comprend l'ensemble des activités visant à prévenir, à atténuer ou à neutraliser le risque d'une réduction ou d'une discontinuité de la disponibilité de fournitures ou de services indispensables à la sauvegarde des intérêts vitaux ou des besoins essentiels de tout ou partie du pays ou de la population offerts par l'intermédiaire de l'infrastructure ainsi que le risque externe dont l'infrastructure est susceptible de faire l'objet.~~

~~Un point, système ou partie de celui-ci ne répondant pas à la définition donnée à l'article 2, peut être recensé et classifié comme infrastructure critique lorsque le fonctionnement d'une infrastructure critique en dépend.~~

~~De même peut être recensé et désigné comme infrastructure critique un secteur ou une partie de secteur dont tous les éléments ne répondent pas nécessairement à la définition donnée à l'article 2, mais dont l'ensemble est considéré comme tel.~~

~~**Art. 5.** Les modalités du recensement et de la désignation des infrastructures critiques sont fixées par règlement grand ducal.~~

~~**Art. 6.** Le propriétaire ou opérateur d'une infrastructure critique est tenu de mettre à la disposition du Haut-Commissariat à la Protection nationale toutes les données sollicitées aux fins du recensement, de la désignation et de la protection des infrastructures critiques. Ces données comprennent toutes les informations qui sont nécessaires dans le contexte de la prévention ou de la gestion d'une crise.~~

~~Les données relatives à l'infrastructure critique faisant l'objet d'un enregistrement, d'une communication, d'une déclaration, d'un recensement, d'un classement, d'une autorisation ou d'une notification imposés par la loi ou par la réglementation afférente sont communiquées au Haut-Commissariat à la Protection nationale, sur sa demande, par les départements ministériels, les administrations et services de l'Etat qui détiennent ces données.~~

~~**Art. 7.** La désignation d'une infrastructure critique fait l'objet d'un arrêté grand-ducal.~~

~~**Art. 8.** (1) Le propriétaire ou opérateur d'une infrastructure critique est tenu d'élaborer un plan de sécurité et de continuité de l'activité qui comporte les mesures de sécurité pour la protection de l'infrastructure. Le Haut-Commissariat à la Protection nationale adresse au propriétaire ou à l'opérateur d'une infrastructure critique des recommandations concernant ces mesures de sécurité qui permettent d'en assurer la protection au sens de l'article 4, d'en améliorer la résilience et de faciliter la gestion d'une crise.~~

~~(2) Le propriétaire ou opérateur d'une infrastructure critique est tenu de designer un correspondant pour la sécurité qui exerce la fonction de contact pour les questions liées à la sécurité de l'infrastructure avec le Haut-Commissariat à la Protection nationale.~~

~~(3) Le propriétaire ou opérateur d'une infrastructure critique doit notifier au Haut-Commissariat à la Protection nationale tout incident ayant eu un impact significatif sur la sécurité et la pérennité du fonctionnement de l'infrastructure.~~

~~(4) La structure des plans de sécurité et de continuité de l'activité des infrastructures critiques est fixée par règlement grand-ducal.~~

Art. 9. En cas d'imminence ou de survenance d'une crise, le propriétaire ou opérateur d'une entité critique ~~infrastructure critique~~, qui doit être, sauf en cas d'extrême urgence, dûment averti, est tenu de donner libre accès aux agents du Haut-Commissariat à la Protection nationale aux installations, locaux, terrains, aménagements faisant partie de ~~l'infrastructure~~ l'entité visée par la présente loi et les règlements à prendre en vue de son application.

Les actions de visite ou de contrôle entreprises sur place respectent le principe de proportionnalité.

Les dispositions reprises aux alinéas qui précèdent ne sont pas applicables aux locaux qui servent à l'habitation.

Chapitre 4*bis* – La stratégie nationale en matière de sécurité des réseaux et des systèmes d'information

Art. 9*bis*. Le Haut-Commissariat à la Protection nationale élabore une stratégie nationale en matière de sécurité des réseaux et des systèmes d'information, qui porte, en particulier, sur les points suivants :

a) les objectifs et les priorités de la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information ;

b) un cadre de gouvernance permettant d'atteindre les objectifs et les priorités de la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information, prévoyant notamment les rôles et les responsabilités des organismes publics et des autres acteurs pertinents ;

c) l'inventaire des mesures en matière de préparation, d'intervention et de récupération, y compris la coopération entre les secteurs public et privé ;

d) un aperçu des programmes d'éducation, de sensibilisation et de formation en rapport avec la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information ;

e) un aperçu des plans de recherche et de développement en rapport avec la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information ;

f) un plan d'évaluation des risques permettant d'identifier les risques ;

g) une liste des différents acteurs concernés par la mise en oeuvre de la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information.

Chapitre 5 – Le personnel du Haut-Commissariat à la Protection nationale

Art. 10. La nomination aux fonctions de Haut-Commissaire à la Protection nationale et de Haut-Commissaire à la Protection nationale adjoint se fait par arrêté grand-ducal sur proposition du membre du Gouvernement ayant dans ses attributions la Protection nationale.

Le Haut-Commissaire à la Protection nationale est responsable de la gestion de l'administration. Il en est le chef hiérarchique. Il est assisté d'un Haut-Commissaire à la Protection nationale adjoint auquel il peut déléguer certaines de ses attributions et qui le remplace en cas d'absence.

Art. 11. (1) Le cadre du personnel comprend un Haut-Commissaire à la Protection nationale, un Haut-Commissaire à la Protection nationale adjoint et des fonctionnaires des différentes catégories de traitement telles que prévues par la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État.

(2) Le cadre du personnel peut être complété par des employés et salariés de l'État dans la limite des crédits budgétaires.

Art. 12. Un règlement grand-ducal détermine les modalités d'organisation des stages, des examens de fin de stage et des examens de promotion pour le personnel du Haut-Commissariat à la Protection nationale.

Chapitre 6 – Dispositions spéciales

Art. 13. En cas d'imminence ou de survenance d'une crise, le Conseil de Gouvernement assure la coordination des mesures de réquisition prévues par la loi du 8 décembre 1981 sur les réquisitions en cas de conflit armé, de crise internationale grave ou de catastrophe, par le titre V de la loi modifiée du 31 mai 1999 portant création d'un corps de police grand-ducale et d'une inspection générale de la police, ainsi que par le chapitre 4 de la loi communale modifiée du 13 décembre 1988.

Art. 14. Le Haut-Commissariat à la Protection nationale peut traiter les données personnelles nécessaires à l'exécution de la mission définie à l'article 3. Ces traitements sont soumis à la procédure d'autorisation préalable de la Commission nationale pour la protection des données telle que prévue à l'article 14 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

Chapitre 7 – Dispositions modificatives, transitoires et spéciales

Art. 15. (1) Les fonctionnaires et employés visés à l'article 11 et relevant de la rubrique « Administration générale » telle qu'énoncée à l'article 12 de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État, en service auprès du Haut-Commissariat à la Protection nationale au moment de l'entrée en vigueur de la présente loi, sont intégrés dans le cadre du personnel du Haut-Commissariat à la Protection nationale aux grade et échelon atteints au moment de l'entrée en vigueur de la présente loi.

(2) Les fonctionnaires détachés au Haut-Commissariat à la Protection nationale au moment de la mise en vigueur de la présente loi, intégrés dans le cadre du personnel du Haut-Commissariat à la Protection nationale, et qui d'après la législation en vigueur dans leur service d'origine au moment de leur détachement avaient une perspective de carrière plus favorable pour l'accès aux différentes fonctions de leur carrière, conservent leurs anciennes possibilités d'avancement.

Art. 15bis. (1) Le personnel de l'ANSSI, du CERT Gouvernemental et du SCC est repris dans le cadre du personnel du Haut-Commissariat à la Protection nationale.

(2) Les fonctionnaires disposant d'un grade de substitution ou d'une majoration d'échelon pour postes à responsabilités particulières avant la reprise continuent à en bénéficier par dépassement du nombre limite fixé en vertu des dispositions de l'article 16 de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État aussi longtemps qu'ils restent titulaires d'un poste à responsabilités particulières. Il en est de même des employés qui bénéficient d'une telle majoration sur la base de l'article 29 de la loi modifiée du 25 mars 2015 déterminant le régime et les indemnités des employés de l'État.

Art. 16. À l'article 16 de la loi du 23 juillet 1952 concernant l'organisation militaire, telle qu'elle a été modifiée dans la suite, il est inséré un nouveau point libellé comme suit: « 2) les officiers, les sous-officiers et les caporaux de carrière employés par ordre du Gouvernement auprès du Haut-Commissariat à la Protection nationale. »

L'actuel point 2) devient le point 3).

Art. 17. La loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État est modifiée comme suit :

(1) à l'article 12, paragraphe 1er, alinéa 7, point 11°, les termes « de Haut-Commissaire à la Protection nationale, » sont insérés avant les termes « et de directeur de différentes administrations » ;

(2) dans l'annexe A « Classification des fonctions », Catégorie de traitement A, Groupe de traitement A1, Sous-groupe à attributions particulières, il est ajouté la mention « Haut-Commissaire à la Protection nationale » au grade 17 ;

(3) au paragraphe b) de l'article 17, il est inséré, à la suite des termes « inspecteur général de la sécurité dans la Fonction publique », la mention « Haut-Commissaire à la Protection nationale ».

Art. 18. La loi du 8 décembre 1981 sur les réquisitions en cas de conflit armé, de crise internationale grave ou de catastrophe, est modifiée comme suit :

1) au chapitre I[er], article 1[er], dernière phrase, il est ajouté en fm de phrase: « ou d'une crise, au sens de la loi portant création d'un Haut-Commissariat à la Protection nationale et modifiant a) la loi modifiée du 23 juillet 1952 concernant l'organisation militaire, b) la loi du 8 décembre 1981 sur les réquisitions en cas de conflit armé, de crise internationale grave ou de catastrophe, c) la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, d) la loi modifiée du 25 juin 2009 sur les marchés publics, e) la loi modifiée du 9 décembre 2005 déterminant les conditions et modalités de nomination de certains fonctionnaires occupant des fonctions dirigeantes dans les administrations et services de l'État, f) la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État ».
2) au chapitre IV, article 8 b) in fine, il est ajouté : « 5) Les agents du Haut-Commissariat à la Protection nationale ».

Art. 19. Au chapitre III, article 14 (1) de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, il est ajouté in fine un point (h) :

« h) les traitements concernant la prévention et la gestion de crises conformément à l'article 14 de la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale et modifiant a) la loi modifiée du 23 juillet 1952 concernant l'organisation militaire, b) la loi du 8 décembre 1981 sur les réquisitions en cas de conflit armé, de crise internationale grave ou de catastrophe, c) la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, d) la loi modifiée du 25 juin 2009 sur les marchés publics, e) la loi modifiée du 9 décembre 2005 déterminant les conditions et modalités de nomination de certains fonctionnaires occupant des fonctions dirigeantes dans les administrations et services de l'État, f) la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État. »

Art. 20. À l'article 1[er] de la loi modifiée du 9 décembre 2005 déterminant les conditions et modalités de nomination de certains fonctionnaires occupant des fonctions dirigeantes dans les administrations et services de l'État, telle qu'elle a été modifiée dans la suite, il est inséré un tiret supplémentaire libellé comme suit: « – de Haut-Commissaire à la Protection nationale. »

Art. 21. Au livre I[er], titre III, chapitre III, article 8 (1) de la loi modifiée du 25 juin 2009 sur les marchés publics, il est ajouté in fine un point I) :

« I) pour les marchés de la protection nationale :
   a) pour les fournitures ou services qui sont déclarés secrets ;
   b) pour les fournitures ou services nécessaires à la protection des intérêts vitaux ou des besoins essentiels de tout ou partie du pays ou de la population, et en particulier les fournitures ou services relatifs à la prévention et la gestion de crises ;
   c) pour les fournitures d'effets d'équipement et de matériel d'intervention ainsi que d'effets personnels de protection et de sécurité des membres des unités d'intervention. »

Art. 22. La référence à la présente loi pourra se faire sous une forme abrégée en utilisant les termes « loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale ».

Art. 23. La présente loi entre en vigueur le premier jour du deuxième mois qui suit sa publication au Mémorial.

*

LOI MODIFIEE DU 25 MARS 2015
fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'Etat

Art. 22. […]

(10) Une prime d'astreinte d'une valeur de 12 points indiciaires peut être allouée au personnel du Haut-Commissariat à la Protection nationale soumis à une obligation de permanence ou de présence pour assurer l'opérationnalité permanente du Centre national de crise. Cette prime est attribuée par décision du ministre du ressort et sur proposition du Haut-Commissaire à la Protection nationale.

*

TABLEAU DE CONCORDANCE

Projet de loi	*Directive 2022/2557*
Art. 1, (1)	Art. 1, (2)
Art. 1, (2)	Art. 1, (3)
Art. 1, (3)	Art. 1, (9)
Art. 2, al. 1, 1°	Art. 2, 1)
Art. 2, al. 1, 2°	Art. 2, 2)
Art. 2, al. 1, 3°	Art. 2, 3)
Art. 2, al. 1, 4°	Art. 2, 4)
Art. 2, al. 1, 5°	Art. 2, 5)
Art. 2, al. 1, 6°	Nouveau
Art. 2, al. 1, 7°	Art. 2, 6)
Art. 2, al. 1, 8°	Art. 2, 7)
Art. 2, al. 1, 9°	Art. 2, 10)
Art. 3, al. 1	Art. 9, (1)
Art. 3, al. 2	Art. 9, (1)
Art. 3, al. 3	Nouveau
Art. 4	Art. 9, (2)
Art. 5, al. 1	Art. 4, (1)
Art. 5, al. 2, 1°	Art. 4, (2), al. 1, a)
Art. 5, al. 2, 2°	Art. 4, (2), al. 1, b)
Art. 5, al. 2, 3°	Art. 4, (2), al. 1, c)
Art. 5, al. 2, 4°	Art. 4, (2), al. 1, d)
Art. 5, al. 2, 5°	Art. 4, (2), al. 1, e)
Art. 5, al. 2, 6°	Art. 4, (2), al. 1, f)
Art. 5, al. 2, 7°	Art. 4, (2), al. 1, g)
Art. 5, al. 2, 8°	Art. 4, (2), al. 1, h)
Art. 5, al. 3	Art. 4, (2), al. 2
Art. 6, (1)	Art. 5, (1), al. 1
Art. 6, (2), al. 1, 1°	Art. 5, (1), al. 2
Art. 6, (2), al. 1, 2°	Art. 5, (2), al. 1, a)
Art. 6, (2), al. 1, 3°	Art. 5, (2), al. 1, b)
Art. 6, (2), al. 1, 4°	Art. 5, (2), al. 1, c)

Projet de loi	*Directive 2022/2557*
Art. 6, (2), al. 1, 5°	Art. 5, (2), al. 1, d)
Art. 6, (2). al. 2	Art. 5. (2), al. 2
Art. 6, (3)	Art. 5, (3)
Art. 7, (1), al. 1	Art. 6, (1)
Art. 7, (1), al. 2	Nouveau
Art. 7, (2), al. 1	Art. 6, (2)
Art. 7, (2), al. 1, 1°	Art. 6, (2), a)
Art. 7, (2), al. 1, 2°	Art. 6, (2), b)
Art. 7, (2), al. 1, 3°	Art. 6, (2), c)
Art. 7, (2), al. 2	Nouveau
Art. 7, (3)	Art. 7, (1)
Art. 7, (3), 1°	Art. 7, (1), a)
Art. 7, (3), 2°	Art. 7, (1), b)
Art. 7, (3), 3°	Art. 7, (1), c)
Art. 7, (3), 4°	Art. 7, (1), d)
Art. 7, (3), 5°	Art. 7, (1), e)
Art. 7, (3), 6°	Art. 7, (1), f)
Art. 7, (4), al. 1	Art. 6, (3), al. 1
Art. 7, (4), al. 2	Art. 6, (3), al. 2
Art. 7, (5)	Art. 17, (2), al. 1
Art. 7, (6)	Art. 6, (4)
Art. 7, (7)	Art. 6, (5)
Art. 8	Art. 8
Art. 9, (1)	Art. 10, (1)
Art. 9, (2)	Art. 10, (2)
Art. 10, 1°	Art. 11, (1), a)
Art. 10, 2°	Art. 11, (1), b)
Art. 10, 3°	Art. 11, (1), c)
Art. 11, (1)	Art. 12, (1)
Art. 11 (2), al. 1	Art. 12, (2), al. 1
Art. 11 (2), al. 2	Art. 12, (2), al. 2
Art. 12, (1), al. 1	Art. 13, (1), al. 1
Art. 12, (1), al. 1, 1°	Art. 13, (1), al. 1, a)
Art. 12, (1), al. 1, 2°	Art. 13, (1), al. 1, b)
Art. 12, (1), al. 1, 3°	Art. 13, (1), al. 1, c)
Art. 12, (1), al. 1, 4°	Art. 13, (1), al. 1, d)
Art. 12, (1), al. 1, 5°	Art. 13, (1), al. 1, e)
Art. 12, (1), al. 1, 6°	Art. 13, (1), al. 1, f)
Art. 12, (1), al. 2	Art. 13, (1), al. 2
Art. 12, (2)	Art. 13, (2)
Art. 12, (3)	Art. 13, (3)
Art. 13, (1), al. 1	Art. 14, (1) & (2)

Projet de loi	*Directive 2022/2557*
Art. 13, (1), al. 1, 1°	Art. 14, (1), a)
Art. 13, (1), al. 1, 2°	Art. 14, (1), b)
Art. 13, (1), al. 1, 3°	Art. 14, (1), c)
Art. 13, (1), al. 2	Nouveau
Art. 13, (2), al. 1, 1°	Nouveau
Art. 13, (2), al. 1, 2°	Nouveau
Art. 13, (2), al. 1, 3°	Nouveau
Art. 13, (2), al. 1, 4°	Nouveau
Art. 13, (2), al. 1, 5°	Nouveau
Art. 13, (2), al. 1, 6°	Nouveau
Art. 13, (2), al. 1, 7°	Nouveau
Art. 13, (2), al. 1, 8°	Nouveau
Art. 13, (2), al. 1, 9°	Nouveau
Art. 13, (2), al. 1, 10°	Nouveau
Art. 13, (2), al. 1, 11°	Nouveau
Art. 13, (2), al. 2	Nouveau
Art. 13, (2), al. 3	Nouveau
Art. 13, (3)	Nouveau
Art. 13, (4), al. 1	Nouveau
Art. 13, (4), al. 2	Nouveau
Art. 14, (1)	Nouveau
Art. 14, (2)	Nouveau
Art. 14, (3)	Nouveau
Art. 14, (4), 1°	Nouveau
Art. 14, (4), 2°	Nouveau
Art. 14, (4), 3°	Nouveau
Art. 15, (1)	Nouveau
Art. 15, (2)	Nouveau
Art. 16, (1), al. 1	Art. 15, (1), al. 1
Art. 16, (1), al. 1, 1°	Art. 15, (1), al. 1, a)
Art. 16, (1), al. 1, 2°	Art. 15, (1), al. 1, b)
Art. 16, (1), al. 1, 3°	Art. 15, (1), al. 1, c)
Art. 16, (1), al. 2	Nouveau
Art. 16, (2)	Art. 15, (2)
Art. 16, (3), al. 1	Art. 15, (3), al. 1
Art. 16, (3), al. 2	Art. 15, (3), al. 2
Art. 16, (4)	Art. 15, (4)
Art. 17, (1), 1°	Art. 17, (1), a)
Art. 17, (1), 2°	Art. 17, (1), b)
Art. 17, (1), 3°	Art. 17. (1), c)
Art. 17, (2)	Art. 18, (7)
Art. 18, (1), al. 1, 1°	Art. 21, (1), a)

Projet de loi	*Directive 2022/2557*
Art. 18, (1), al. 1, 2°	Art. 21, (1), a)
Art. 18, (1), al. 1, 3°	Art. 21, (1), b)
Art. 18, (1), al. 2	Nouveau
Art. 18, (1), al. 3	Nouveau
Art. 18, (1), al. 4	Nouveau
Art. 18, (2), al. 1, 1°	Art. 21, (2), al. 1, a)
Art. 18, (2), al. 1, 2°	Art. 21, (2), al. 1, b)
Art. 18, (2), al. 2	Nouveau
Art. 18, (2), al. 3	Art. 21, (2), al. 2
Art. 18, (3)	Art. 21, (3)
Art. 18, (4)	Art. 21, (5)
Art. 19, (1), 1°	Art. 22
Art. 19, (1), 2°	Art. 22
Art. 19, (1), 3°	Art. 22
Art. 19, (2)	Art. 22
Art. 19, (3)	Art. 22
Art. 19, (4)	Art. 22
Art. 19, (5)	Art. 22
Art. 20	Nouveau
Art. 21, 1°	Nouveau
Art. 21, 2°	Nouveau
Art. 21, 3°	Nouveau
Art. 21, 4°	Nouveau
Art. 21, 5°	Nouveau
Art. 21, 6°	Nouveau
Art. 22	Nouveau

Directive 2022/2557	*Projet de loi*
Art. 1, (1), a)	
Art. 1, (1), b)	
Art. 1, (1), c), i)	
Art. 1, (1), c), ii)	
Art. 1, (1), c), iii)	
Art. 1, (1), d)	
Art. 1, (1), e)	
Art. 1, (2)	Art. 1, (1)
Art. 1, (3)	Art. 1, (2)
Art. 1, (4)	
Art. 1, (5)	
Art. 1, (6)	
Art. 1, (7)	
Art. 1, (8)	

Directive 2022/2557	*Projet de loi*
Art. 1, (9)	Art. 1, (3)
Art. 2, 1)	Art. 2, 1°
Art. 2, 2)	Art. 2, 2°
Art. 2, 3)	Art. 2, 3°
Art. 2, 4)	Art. 2, 4°
Art. 2, 5)	Art. 2, 5°
Art. 2, 6)	Art. 2, 7°
Art. 2, 7)	Art. 2, 8°
Art. 2, 8)	
Art. 2, 9)	
Art. 2, 10)	Art. 2, 9°
Art. 3	
Art. 4, (1)	Art. 5, al. 1
Art. 4. (2), al. 1, a)	Art. 5, al. 2, 1°
Art. 4, (2), al. 1, b)	Art. 5, al. 2, 2°
Art. 4, (2), al. 1, c)	Art. 5, al. 2, 3°
Art. 4, (2), al. 1, d)	Art. 5, al. 2, 4°
Art. 4, (2), al. 1, e)	Art. 5, al. 2, 5°
Art. 4, (2), al. 1, f)	Art. 5, al. 2, 6°
Art. 4, (2), al. 1, g)	Art. 5, al. 2, 7°
Art. 4, (2), al. 1, h)	Art. 5, al. 2, 8°
Art. 4, (2), al. 2	Art. 5, al. 3
Art. 4, (3)	
Art. 5, (1), al. 1	Art. 6, (1)
Art. 5, (1), al. 2	Art. 6, (2), al. 1, 1°
Art. 5, (2), al. 1, a)	Art. 6, (2), al. 1, 2°
Art. 5, (2), al. 1, b)	Art. 6, (2). al. 1, 3°
Art. 5, (2), al. 1, c)	Art. 6, (2), al. 1, 4°
Art. 5, (2), al. 1, d)	Art. 6, (2), al. 1, 5°
Art. 5, (2), al. 2	Art. 6, (2), al. 2
Art. 5, (3)	Art. 6, (3)
Art. 5, (4)	
Art. 5, (5)	
Art. 6, (1)	Art. 7, (1), al. 1
Art. 6, (2), a)	Art. 7, (2), al. 1, 1°
Art. 6, (2), b)	Art. 7, (2), al. 1, 2°
Art. 6, (2), c)	Art. 7, (2), al. 1, 3°
Art. 6, (3), al. 1	Art. 7, (4), al. 1
Art. 6, (3), al. 2	Art. 7, (4), al. 2
Art. 6, (4)	Art. 7, (6)
Art. 6, (5)	Art. 7, (7)
Art. 6, (6)	

Directive 2022/2557	*Projet de loi*
Art. 7, (1), a)	Art. 7, (3), 1°
Art. 7, (1), b)	Art. 7, (3), 2°
Art. 7, (1), c)	Art. 7, (3), 3°
Art. 7, (1), d)	Art. 7, (3), 4°
Art. 7, (1), e)	Art. 7, (3), 5°
Art. 7, (1), f)	Art. 7, (3), 6°
Art. 7, (2), al. 1, a)	
Art. 7, (2), al. 1, b)	
Art. 7, (2), al. 1, c)	
Art. 7, (2), al. 2	
Art. 7, (2), al. 3	
Art. 7, (3)	
Art. 8	Art. 8
Art. 9, (1), al. 1	Art. 3, al. 1, al. 2
Art. 9, (1), al. 2	
Art. 9, (1), al. 3	
Art. 9, (2)	Art. 4
Art. 9, (3), al. 1	
Art. 9, (3), al. 2	
Art. 9, (4)	
Art. 9, (5)	
Art. 9, (6)	
Art. 9, (7)	
Art. 9, (8)	
Art. 10, (1)	Art. 9, (1)
Art. 10, (2)	Art. 9, (2)
Art. 10, (3)	
Art. 11, (1), a)	Art. 10, 1°
Art. 11, (1), b)	Art. 10, 2°
Art. 11, (1), c)	Art. 10, 3°
Art. 11, (2)	
Art. 12, (1)	Art. 11, (1)
Art. 12, (2), al. 1	Art. 11, (2), al. 1
Art. 12, (2), al. 2	Art. 11, (2), al. 2
Art. 13, (1), al. 1, a)	Art. 12, (1), al. 1, 1°
Art. 13, (1), al. 1, b)	Art. 12, (1), al. 1, 2°
Art. 13, (1), al. 1, c)	Art. 12, (1), al. 1, 3°
Art. 13, (1), al. 1, d)	Art. 12, (1), al. 1, 4°
Art. 13, (1), al. 1, e)	Art. 12, (1), al. 1, 5°
Art. 13, (1), al. 1, f)	Art. 12, (1), al. 1, 6°
Art. 13, (1), al. 2	Art. 12, (1), al. 2
Art. 13, (2)	Art. 12, (2)

Directive 2022/2557	*Projet de loi*
Art. 13, (3)	Art. 12, (3)
Art. 13, (4)	
Art. 13, (5)	
Art. 13, (6)	
Art. 14, (1), a)	Art. 13, (1), al. 1, 1°
Art. 14, (1), b)	Art. 13, (1), al. 1, 1°
Art. 14, (1), c)	Art. 13, (1), al. 1, 3°
Art. 14, (2)	Art. 13 – art. 15
Art. 14, (3), al. 1, a)	Art. 13 – art. 15
Art. 14, (3), al. 1, b)	Art. 13 – art. 15
Art. 14, (3), al. 2	Art. 13 – art. 15
Art. 15, (1), al. 1, a)	Art. 16, (1), al. 1, 1°
Art. 15, (1), al. 1, b)	Art. 16, (1), al. 1, 2°
Art. 15, (1), al. 1, c)	Art. 16, (1), al. 1, 3°
Art. 15, (1), al. 2	
Art. 15, (2)	Art. 16, (2)
Art. 15, (3), al. 1	Art. 16, (3), al. 1
Art. 15, (3), al. 2	Art. 16, (3), al. 2
Art. 15, (4)	Art. 16, (4)
Art. 16	
Art. 17, (1), a)	Art. 17, (1), 1°
Art. 17, (1), b)	Art. 17, (1), 2°
Art. 17, (1), c)	Art. 17, (1), 3°
Art. 17, (2), al. 1	Art. 7, (5)
Art. 17, (2), al. 2	
Art. 17, (3)	
Art. 17, (4)	
Art. 18, (1)	
Art. 18, (2)	
Art. 18, (3), a)	
Art. 18, (3), b)	
Art. 18, (3), c)	
Art. 18, (4), al. 1	
Art. 18, (4), al. 2	
Art. 18, (4), al. 3	
Art. 18, (4), al. 4	
Art. 18, (5), al. 1	
Art. 18, (5), al. 2	
Art. 18, (6)	
Art. 18, (7)	Art. 17, (2)
Art. 18, (8)	
Art. 18, (9)	

Directive 2022/2557	*Projet de loi*
Art. 18, (10)	
Art. 19, (1)	
Art. 19, (2), al. 1	
Art. 19, (2), al. 2	
Art. 19, (3), a)	
Art. 19, (3), b)	
Art. 19, (3), c)	
Art. 19, (3), d)	
Art. 19, (3), e)	
Art. 19, (3), f)	
Art. 19, (3), g)	
Art. 19, (3), h)	
Art. 19, (3), i)	
Art. 19, (3), j)	
Art. 19, (4)	
Art. 19, (5)	
Art. 19, (6)	
Art. 19, (7)	
Art. 20, (1)	
Art. 20, (2)	
Art. 20, (3)	
Art. 21, (1), a)	Art. 18, (1), al. 1, 1° et 2°
Art. 21, (1), b)	Art. 18, (1), al. 1, 3°
Art. 21, (2), al. 1, a)	Art. 18, (2), al. 1, 1°
Art. 21, (2), al. 1, b)	Art. 18, (2), al. 1, 2°
Art. 21, (2), al. 2	Art. 18, (2), al. 3
Art. 21, (3)	Art. 18, (3)
Art. 21, (4)	
Art. 21, (5)	Art. 18, (4)
Art. 22	Art. 19
Art. 23, (1)	
Art. 23, (2)	
Art. 23, (3)	
Art. 23, (4)	
Art. 23, (5)	
Art. 23, (6)	
Art. 24, (1)	
Art. 24, (2)	
Art. 25, al. 1	
Art. 25, al. 2	
Art. 26, (1), al. 1	
Art. 26, (1), al. 2	

Directive 2022/2557	*Projet de loi*
Art. 26, (2)	
Art. 27	
Art. 28	
Art. 29	

*

FICHE FINANCIERE

(article 79 de la loi modifiée du 8 juin 1999 sur le Budget,
la Comptabilité et la Trésorerie de l'État)

Les frais supplémentaires engendrés par le projet de loi sont :

1. les frais liés au recrutement de personnel au sein de la Police grand-ducale afin de procéder aux vérifications des antécédents. Le nombre d'agents à recruter auprès de la Police grand-ducale pour effectuer les vérifications des antécédents est évaluée à ce stade à trois personnes. Le nombre exact ne pourra être précisé qu'ultérieurement, au moment de la mise en oeuvre du système et du volume de demandes à traiter ;
2. les frais en relation avec la mise en place d'un système informatique centralisé pour la gestion des demandes de vérification des antécédents (autour de 230 000 EUR) ;
3. les frais liés au recrutement de personnel afin de compléter le service chargé de la protection des entités critiques auprès du HCPN. Ce besoin en personnel est évalué à 3 fonctionnaires/employés A1 pour l'année 2024, 4 fonctionnaires/employés A1 pour l'année 2025, 3 fonctionnaires/employés A1 pour l'année 2026 et 1 fonctionnaire/employé A1 pour l'année 2027. Ces renforcements en effectif ont été demandés dans le cadre du numerus clausus.

*

DIRECTIVE (UE) 2022/2557 DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 14 décembre 2022

sur la résilience des entités critiques, et abrogeant la directive 2008/114/CE du Conseil

(Texte présentant de l'intérêt pour l'EEE)

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 114,

vu la proposition de la Commission européenne,

après transmission du projet d'acte législatif aux parlements nationaux,

vu l'avis du Comité économique et social européen ([1]),

vu l'avis du Comité des régions ([2]),

statuant conformément à la procédure législative ordinaire ([3]),

considérant ce qui suit:

(1) Les entités critiques, en tant que fournisseurs de services essentiels, jouent un rôle indispensable dans le maintien de fonctions sociétales ou d'activités économiques vitales dans le marché intérieur, dans le contexte d'une économie de l'Union de plus en plus interdépendante. Par conséquent, il est essentiel de fixer un cadre de l'Union visant tant à renforcer la résilience des entités critiques dans le marché intérieur en établissant des règles minimales harmonisées qu'à les aider au moyen de mesures de soutien et de supervision cohérentes et spécifiques.

(2) La directive 2008/114/CE ([4]) du Conseil établit une procédure de désignation des infrastructures critiques européennes dans les secteurs de l'énergie et des transports dont la perturbation ou la destruction aurait un impact transfrontière significatif sur deux États membres au moins. Cette directive vise exclusivement la protection de ces infrastructures. Toutefois, l'évaluation de la directive 2008/114/CE réalisée en 2019 a montré qu'en raison de la nature de plus en plus interconnectée et transfrontière des activités faisant appel à des infrastructures critiques, les mesures de protection portant sur des biens individuels ne suffisent pas à elles seules pour empêcher toute perturbation. Par conséquent, il est nécessaire de réorienter l'approche en vue de faire en sorte que les risques soient mieux pris en compte, que le rôle et les obligations des entités critiques, en tant que fournisseurs de services essentiels au fonctionnement du marché intérieur, soient mieux définis et cohérents, et que des règles de l'Union

([1]) JO C 286 du 16.7.2021, p. 170.
([2]) JO C 440 du 29.10.2021, p. 99.
([3]) Position du Parlement européen du 22 novembre 2022 (non encore parue au Journal officiel) et décision du Conseil du 8 décembre 2022.
([4]) Directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection (JO L 345 du 23.12.2008, p. 75).

soient adoptées afin de renforcer la résilience des entités critiques. Les entités critiques devraient être en mesure de renforcer leur capacité à prévenir les incidents susceptibles de perturber la fourniture de services essentiels, à s'en protéger, à y réagir, à y résister, à les atténuer, à les absorber, à s'y adapter et à s'en remettre.

(3) Si un certain nombre de mesures prises au niveau de l'Union, telles que le programme européen de protection des infrastructures critiques, et au niveau national visent à soutenir la protection des infrastructures critiques dans l'Union, il convient d'en faire davantage pour que les entités qui exploitent ces infrastructures soient mieux équipées pour faire face aux risques pesant sur leurs activités qui pourraient entraîner une perturbation de la fourniture de services essentiels. Il convient aussi d'en faire davantage pour mieux équiper ces entités, car les menaces forment un paysage dynamique, qui comprend des menaces hybrides et terroristes en évolution, et des interdépendances croissantes entre les infrastructures et les secteurs. En outre, il existe un risque physique accru lié aux catastrophes naturelles et au changement climatique, qui augmente la fréquence et l'ampleur des phénomènes météorologiques extrêmes et entraîne des changements à long terme des conditions climatiques moyennes, susceptibles de réduire la capacité, l'efficacité et la durée de vie de certains types d'infrastructures si des mesures d'adaptation au changement climatique ne sont pas mises en place. De plus, le marché intérieur est caractérisé par une fragmentation en ce qui concerne le recensement des entités critiques, les secteurs et les catégories d'entités concernés n'étant pas systématiquement reconnus comme critiques dans tous les États membres. La présente directive devrait donc instaurer un niveau élevé d'harmonisation en ce qui concerne les secteurs et les catégories d'entités relevant de son champ d'application.

(4) Si certains secteurs de l'économie, tels que les secteurs de l'énergie et des transports, sont déjà réglementés par des actes juridiques sectoriels de l'Union, ces actes juridiques contiennent des dispositions qui portent uniquement sur certains aspects de la résilience des entités actives dans ces secteurs. Afin de traiter de manière globale la résilience des entités qui sont critiques pour le bon fonctionnement du marché intérieur, la présente directive crée un cadre général applicable à la résilience des entités critiques en ce qui concerne tous les risques, qu'ils soient naturels ou d'origine humaine, accidentels ou intentionnels.

(5) Les interdépendances croissantes entre les infrastructures et les secteurs sont le résultat d'un réseau de fourniture de services de plus en plus transfrontière et interdépendant, qui utilise des infrastructures clés dans toute l'Union dans les secteurs de l'énergie, des transports, des banques, de l'eau potable, des eaux usées, de la production, de la transformation et de la distribution de denrées alimentaires, de la santé, de l'espace, des infrastructures du marché financier et des infrastructures numériques, et de certains aspects du secteur de l'administration publique. Le secteur spatial relève du champ d'application de la présente directive pour ce qui est de la fourniture de certains services qui dépendent d'infrastructures terrestres détenues, gérées et exploitées par des États membres ou par des parties privées; par conséquent, les infrastructures détenues, gérées ou exploitées par ou au nom de l'Union dans le cadre de son programme spatial ne relèvent pas du champ d'application de la présente directive.

En ce qui concerne le secteur de l'énergie, et plus particulièrement les procédés de production et de transport de l'électricité (en ce qui concerne la fourniture d'électricité), il est entendu que, lorsque cela est jugé approprié, la production d'électricité peut englober les éléments des centrales nucléaires servant au transport de l'électricité, tout en excluant les éléments strictement nucléaires, qui relèvent du droit de l'Union, y compris les actes juridiques pertinents de l'Union concernant l'énergie nucléaire, et des traités. Le processus de recensement des entités critiques dans le secteur alimentaire devrait refléter de manière adéquate la nature du marché intérieur dans ce secteur et les règles étendues de l'Union relatives aux principes généraux et aux prescriptions générales de la législation alimentaire et à ceux en matière de sécurité des denrées alimentaires. Par conséquent, afin de garantir une approche proportionnée et de tenir dûment compte du rôle et de l'importance de ces entités au niveau national, il convient de ne recenser parmi les entreprises du secteur alimentaire que les entités critiques, qu'elles soient à but lucratif ou non et qu'elles soient publiques ou privées, qui se consacrent exclusivement à la logistique, à la distribution en gros, ainsi qu'à la production et à la transformation industrielles à grande échelle et détenant une part de marché importante, comme observé au niveau national. Ces interdépendances signifient que toute perturbation de services essentiels, même initialement limitée à une entité ou un secteur, peut produire des effets en cascade plus larges, entraînant éventuellement une incidence négative à long terme et de grande ampleur sur la fourniture de services dans l'ensemble du marché intérieur. Les crises majeures, telles que la pandémie de COVID-19, ont mis en évidence la vulnérabilité de nos sociétés de plus en plus interdépendantes face à des risques à faible probabilité de survenance, mais à fort impact.

(6) Les entités participant à la fourniture de services essentiels sont de plus en plus soumises à des exigences divergentes imposées par le droit national. Le fait que certains États membres imposent des exigences de sécurité moins strictes à ces entités non seulement entraîne des niveaux de résilience différents mais risque également d'avoir une incidence négative sur le maintien de fonctions sociétales ou d'activités économiques vitales dans l'ensemble de l'Union, et entrave le bon fonctionnement du marché intérieur. Les investisseurs et les entreprises peuvent se fier et faire confiance aux entités critiques qui sont résilientes, et la fiabilité et la confiance constituent la clé de voûte d'un marché intérieur performant. Des types d'entités similaires sont considérés comme critiques dans certains États membres mais pas dans d'autres, et ceux qui sont recensés comme critiques sont soumis à des exigences différentes selon les États membres. Il en résulte une charge administrative supplémentaire et inutile pour les entreprises exerçant des activités transfrontières, notamment pour les entreprises actives dans des États membres imposant des exigences plus strictes. Un cadre de l'Union aurait donc également pour effet de créer des conditions équitables pour les entités critiques dans toute l'Union.

(7) Il est nécessaire d'établir des règles minimales harmonisées afin de garantir la fourniture de services essentiels dans le marché intérieur, de renforcer la résilience des entités critiques et d'améliorer la coopération transfrontière entre les autorités compétentes. Il importe que ces règles soient à l'épreuve du temps en ce qui concerne leur conception et leur mise en œuvre, tout en offrant la souplesse nécessaire. Il est également crucial d'améliorer la capacité des entités critiques à fournir des services essentiels face à un ensemble diversifié de risques.

(8) Afin d'atteindre un niveau élevé de résilience, les États membres devraient recenser les entités critiques qui seront soumises à des exigences et à une supervision spécifiques, et qui bénéficieront d'un soutien et de conseils particuliers face à tous les risques pertinents.

(9) Compte tenu de l'importance de la cybersécurité pour la résilience des entités critiques et dans un souci d'uniformité, il convient de veiller à une approche cohérente, chaque fois que cela est possible, entre la présente directive et la directive (UE) 2022/2555 du Parlement européen et du Conseil ([5]). Compte tenu de la fréquence plus élevée et des caractéristiques particulières des risques en matière de cybersécurité, la directive (UE) 2022/2555 impose des exigences complètes à un grand nombre d'entités afin de garantir leur cybersécurité. Étant donné que la cybersécurité est suffisamment traitée dans la directive (UE)2022/2555, les questions qu'elle couvre devraient être exclues du champ d'application de ladite directive, sans préjudice du régime particulier applicable aux entités du secteur des infrastructures numériques.

(10) Lorsque des dispositions d'actes juridiques sectoriels de l'Union exigent des entités critiques qu'elles prennent des mesures pour renforcer leur résilience et lorsque ces exigences sont reconnues par les États membres comme étant au moins équivalentes aux obligations correspondantes prévues par la présente directive, les dispositions pertinentes de la présente directive ne devraient pas s'appliquer, de manière à éviter tout double emploi et une charge inutile. Dans un tel cas, les dispositions pertinentes de ces actes juridiques de l'Union devraient s'appliquer. Lorsque les dispositions pertinentes de la présente directive ne s'appliquent pas, les dispositions relatives à la supervision et à l'exécution des règles prévues par la présente directive ne devraient pas non plus s'appliquer.

(11) La présente directive n'affecte pas la compétence des États membres et de leurs autorités pour ce qui est de l'autonomie administrative ou la responsabilité qui leur incombe en matière de sauvegarde de la sécurité nationale et de la défense ou leur pouvoir de garantir d'autres fonctions essentielles de l'État, notamment celles qui ont pour objet d'assurer la sécurité publique, l'intégrité territoriale et le maintien de l'ordre public. L'exclusion des entités de l'administration publique du champ d'application de la présente directive devrait s'appliquer aux entités qui exercent leurs activités principalement dans les domaines de la sécurité nationale, de la sécurité publique, de la défense ou de l'application de la loi, y compris la détection des infractions pénales ainsi que les enquêtes et les poursuites en la matière. Toutefois, les entités de l'administration publique dont les activités ne sont que marginalement liées à ces domaines devraient relever du champ d'application de la présente directive. Aux fins de la présente directive, les entités disposant de compétences réglementaires ne sont pas considérées comme exerçant des activités dans le domaine de l'application de la loi et elles ne sont, par conséquent, pas exclues du champ d'application de la présente directive pour ce motif. Les entités de l'administration publique qui sont établies conjointement avec un pays tiers conformément à un accord international sont exclues du champ d'application de la présente directive. La présente directive ne s'applique pas aux missions diplomatiques et consulaires des États membres dans les pays tiers.

([5]) Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (voir page 80 du présent Journal officiel).

Certaines entités critiques exercent des activités dans les domaines de la sécurité nationale, de la sécurité publique, de la défense ou de l'application de la loi, y compris la détection des infractions pénales ainsi que les enquêtes et les poursuites en la matière, ou fournissent des services exclusivement à des entités de l'administration publique qui exercent des activités principalement dans ces domaines. Compte tenu de la responsabilité qui incombe aux États membres en matière de sauvegarde de la sécurité nationale et de la défense, les États membres devraient pouvoir décider que les obligations incombant aux entités critiques prévues dans la présente directive ne s'appliquent pas, en tout ou en partie, auxdites entités critiques si les services qu'elles fournissent ou les activités qu'elles exercent sont principalement liés aux domaines de la sécurité nationale, de la sécurité publique, de la défense ou de l'application de la loi, y compris la détection des infractions pénales ainsi que les enquêtes et les poursuites en la matière. Les entités critiques dont les services ou les activités ne sont que marginalement liés à ces domaines devraient relever du champ d'application de la présente directive. Aucun État membre ne devrait être tenu de fournir des informations dont la divulgation serait contraire aux intérêts essentiels de sa sécurité nationale. Les règles de l'Union ou les règles nationales visant à protéger les informations classifiées et les accords de non-divulgation sont pertinents à cet égard.

(12) Afin de ne pas compromettre la sécurité nationale ou la sécurité et les intérêts commerciaux des entités critiques, les informations sensibles devraient être consultées, échangées et traitées avec prudence et en accordant une attention particulière aux canaux de transmission et aux capacités de stockage utilisés.

(13) Afin de garantir une approche globale de la résilience des entités critiques, chaque État membre devrait disposer d'une stratégie pour renforcer la résilience des entités critiques (ci-après dénommée «stratégie»). La stratégie devrait définir les objectifs stratégiques et les mesures politiques à mettre en œuvre. Dans un souci de cohérence et d'efficacité, la stratégie devrait être conçue de manière à intégrer harmonieusement les politiques existantes, en s'appuyant, chaque fois que cela est possible, sur des stratégies nationales et sectorielles, des plans ou des documents similaires existants pertinents. Afin de mettre en place une approche globale, les États membres devraient veiller à ce que leur stratégie prévoie un cadre d'action pour une coordination renforcée entre les autorités compétentes en vertu de la présente directive et les autorités compétentes en vertu de la directive (UE) 2022/2555 dans le contexte du partage d'informations sur les risques, menaces et incidents en matière de cybersécurité et les risques, menaces et incidents non liés à la cybersécurité, et dans le contexte de l'exercice des tâches de supervision. Lorsqu'ils mettent en place leur stratégie, les États membres devraient tenir dûment compte de la nature hybride des menaces pesant sur les entités critiques.

(14) Les États membres devraient communiquer leur stratégie et les mises à jour substantielles de celle-ci à la Commission, notamment pour permettre à cette dernière d'évaluer la bonne application de la présente directive en ce qui concerne les approches stratégiques à l'égard de la résilience des entités critiques à l'échelon national. Les stratégies pourraient être communiquées en tant qu'informations classifiées. La Commission devrait établir un rapport de synthèse sur les stratégies communiquées par les États membres, qui servirait de base aux échanges visant à recenser les bonnes pratiques et les questions d'intérêt commun dans le cadre d'un groupe sur la résilience des entités critiques. Les informations agrégées figurant dans le rapport de synthèse, qu'elles soient classifiées ou non, étant par nature sensibles, la Commission devrait gérer le rapport de synthèse en étant dûment consciente de la question de la sécurité des entités critiques, des États membres et de l'Union. Le rapport de synthèse et les stratégies devraient être protégés contre les actes illicites ou malveillants et ne devraient être accessibles qu'aux personnes autorisées afin d'atteindre les objectifs de la présente directive. La communication des stratégies et de leurs mises à jour substantielles devrait également aider la Commission à comprendre l'évolution des approches à l'égard de la résilience des entités critiques et à alimenter le suivi de l'impact et de la valeur ajoutée de la présente directive, que la Commission doit réexaminer périodiquement.

(15) Les mesures prises par les États membres pour recenser les entités critiques et contribuer à garantir leur résilience devraient suivre une approche fondée sur les risques qui se concentre sur les entités les plus importantes pour l'exercice de fonctions sociétales ou d'activités économiques vitales. Afin de garantir une telle approche ciblée, chaque État membre devrait procéder, dans un cadre harmonisé, à une évaluation des risques naturels et d'origine humaine pertinents, y compris les risques de nature transsectorielle ou transfrontière, pouvant affecter la fourniture de services essentiels, y compris les accidents, les catastrophes naturelles, les urgences de santé publique telles que les pandémies et les menaces hybrides ou autres menaces antagonistes, lesquelles comprennent les infractions terroristes, l'infiltration par les réseaux criminels et le sabotage (ci-après dénommée «évaluation des risques d'État membre»). Lorsqu'ils procèdent à une telle évaluation, les États membres devraient tenir compte d'autres évaluations des risques générales ou sectorielles effectuées en vertu d'autres actes juridiques de l'Union et examiner la mesure dans laquelle les secteurs dépendent les uns des autres, y compris de secteurs d'autres États membres et de pays tiers. Les résultats de l'évaluation des risques d'État membre devraient être utilisés aux fins de recenser les entités critiques

et d'aider ces entités à satisfaire aux exigences auxquelles elles sont soumises en matière de résilience. La présente directive ne s'applique qu'aux États membres et aux entités critiques qui exercent leurs activités au sein de l'Union. Néanmoins, l'expertise et les connaissances générées par les autorités compétentes, notamment au moyen d'évaluations des risques, et par la Commission, notamment au moyen de diverses formes de soutien et de coopération, pourraient être utilisées, le cas échéant et conformément aux instruments juridiques applicables, dans l'intérêt des pays tiers, notamment ceux qui se trouvent dans le voisinage direct de l'Union, en alimentant la coopération existante en matière de résilience.

(16) Afin de garantir que toutes les entités concernées sont soumises aux exigences en matière de résilience de la présente directive et de réduire les divergences à cet égard, il importe d'établir des règles harmonisées permettant un recensement cohérent des entités critiques dans l'ensemble de l'Union, tout en permettant aux États membres de tenir suffisamment compte du rôle et de l'importance de ces entités à l'échelon national. Lorsqu'il applique les critères établis dans la présente directive, chaque État membre devrait recenser les entités qui fournissent un ou plusieurs services essentiels et qui exploitent et possèdent des infrastructures critiques situées sur son territoire. Une entité devrait être considérée comme exerçant des activités sur le territoire de l'État membre dans lequel elle exerce les activités nécessaires pour le ou les services essentiels en question et dans lequel se trouve l'infrastructure critique de cette entité, qui est utilisée pour fournir ce ou ces services. Lorsqu'aucune entité ne remplit ces critères dans un État membre, cet État membre ne devrait pas être tenu de recenser des entités critiques dans le secteur ou sous-secteur correspondant. Dans un souci d'efficacité, d'efficience, de cohérence et de sécurité juridique, il convient d'établir des règles appropriées en ce qui concerne la notification des entités qui ont été recensées en tant qu'entités critiques.

(17) Les États membres devraient communiquer à la Commission, selon des modalités qui répondent aux objectifs de la présente directive, une liste des services essentiels, le nombre d'entités critiques recensées pour chacun des secteurs et sous-secteurs figurant en annexe et pour le ou les services essentiels fournis par chaque entité et, s'ils sont appliqués, les seuils. Il devrait être possible de présenter les seuils tels quels ou sous une forme agrégée, c'est-à-dire que les informations peuvent prendre la forme de moyennes par zone géographique, par année, par secteur, par sous-secteur, ou par tout autre critère, et peuvent comporter des données sur la portée des indicateurs fournis.

(18) Des critères devraient être fixés afin de déterminer l'importance de l'effet perturbateur causé par un incident. Ces critères devraient se fonder sur les critères énoncés dans la directive (UE) 2016/1148 du Parlement européen et du Conseil ([6]) afin de tirer parti des efforts déployés par les États membres pour recenser les opérateurs de services essentiels tels qu'ils sont définis dans ladite directive et de l'expérience acquise à cet égard. Des crises majeures, telles que la pandémie de COVID-19, ont mis en lumière l'importance de garantir la sécurité de la chaîne d'approvisionnement et ont montré comment sa perturbation peut avoir des incidences économiques et sociétales négatives dans un grand nombre de secteurs et au-delà des frontières. Par conséquent, les États membres devraient également tenir compte des effets sur la chaîne d'approvisionnement, dans la mesure du possible, lorsqu'ils déterminent la mesure dans laquelle d'autres secteurs et sous-secteurs dépendent du service essentiel fourni par une entité critique.

(19) Conformément au droit de l'Union et au droit national applicables, y compris le règlement (UE) 2019/452 du Parlement européen et du Conseil ([7]), qui établit un cadre pour le filtrage des investissements directs étrangers dans l'Union, il convient de reconnaître la menace potentielle que représente la participation étrangère dans des infrastructures critiques au sein de l'Union, parce que les services, l'économie, la liberté de circulation et la sécurité des citoyens de l'Union dépendent du bon fonctionnement des infrastructures critiques.

(20) La directive (UE) 2022/2555 impose aux entités appartenant au secteur des infrastructures numériques qui pourraient être recensées en tant qu'entités critiques en vertu de la présente directive de prendre des mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information et de signaler les cybermenaces et les incidents importants. Étant donné que les menaces pesant sur la sécurité des réseaux et des systèmes d'information peuvent avoir des origines différentes, la directive (UE) 2022/2555 applique une approche tous risques qui inclut la résilience des réseaux et des systèmes d'information ainsi que des composants et environnements physiques de ces systèmes.

([6]) Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (JO L 194 du 19.7.2016, p. 1).

([7]) Règlement (UE) 2019/452 du Parlement européen et du Conseil du 19 mars 2019 établissant un cadre pour le filtrage des investissements directs étrangers dans l'Union (JO L 79 I du 21.3.2019, p. 1).

Les exigences établies par la directive (UE) 2022/2555 à cet égard étant au moins équivalentes aux obligations correspondantes établies par la présente directive, les obligations établies à l'article 11 et aux chapitres III, IV et VI de la présente directive ne devraient pas s'appliquer aux entités appartenant au secteur des infrastructures numériques de manière à éviter tout double emploi et des charges administratives inutiles. Toutefois, compte tenu de l'importance des services fournis par les entités appartenant au secteur des infrastructures numériques à des entités critiques appartenant à tous les autres secteurs, les États membres devraient recenser, sur la base des critères et selon la procédure prévus dans la présente directive, les entités appartenant au secteur des infrastructures numériques en tant qu'entités critiques. Par conséquent, les stratégies, les évaluations des risques d'États membres et les mesures de soutien énoncées au chapitre II de la présente directive devraient s'appliquer. Les États membres devraient pouvoir adopter ou maintenir des dispositions de droit national afin d'atteindre un niveau de résilience plus élevé pour ces entités critiques, à condition que ces dispositions soient compatibles avec le droit de l'Union applicable.

(21) Le droit de l'Union relatif aux services financiers impose aux entités financières des exigences étendues visant à ce que tous les risques auxquels elles sont confrontées soient gérés, y compris les risques opérationnels, et à garantir la continuité des activités. Ce droit comprend les règlements (UE) nº 648/2012 ([8]), (UE) nº 575/2013 ([9]) et (UE) nº 600/2014 ([10]) du Parlement européen et du Conseil et les directive 2013/36/UE ([11]) et 2014/65/UE ([12]) du Parlement européen et du Conseil. Ce cadre juridique est complété par le règlement (UE) 2022/2554 du Parlement européen et du Conseil ([13]), qui fixe des exigences applicables aux entités financières en matière de gestion des risques liés aux technologies de l'information et de la communication (TIC), y compris en matière de protection des infrastructures physiques des TIC. Étant donné que la résilience de ces entités est dès lors entièrement couverte, l'article 11 et les chapitres III, IV et VI de la présente directive ne devraient pas s'appliquer à ces entités, afin d'éviter des doubles emplois et des charges administratives inutiles.

Toutefois, compte tenu de l'importance des services fournis par les entités du secteur financier à des entités critiques appartenant à tous les autres secteurs, les États membres devraient recenser, sur la base des critères et selon la procédure prévus dans la présente directive, les entités du secteur financier en tant qu'entités critiques. Par conséquent, les stratégies, les évaluations des risques d'États membres et les mesures de soutien énoncées au chapitre II de la présente directive devraient s'appliquer. Les États membres devraient pouvoir adopter ou maintenir des dispositions de droit national afin d'atteindre un niveau de résilience plus élevé pour ces entités critiques, à condition que ces dispositions soient compatibles avec le droit de l'Union applicable.

(22) Les États membres devraient désigner ou mettre en place des autorités chargées de surveiller l'application des règles de la présente directive et, si nécessaire, de les faire respecter, et veiller à ce que ces autorités disposent des pouvoirs et des ressources adéquats. Compte tenu des différences entre les structures de gouvernance nationales, afin de préserver les dispositifs sectoriels existants ou les organismes de surveillance et de réglementation de l'Union, et afin d'éviter les doubles emplois, les États membres devraient pouvoir désigner ou mettre en place plus d'une autorité compétente. Lorsque les États membres désignent ou mettent en place plusieurs autorités compétentes, ils devraient définir clairement les tâches respectives des autorités concernées et veiller à ce qu'elles coopèrent de manière harmonieuse et efficace. Toutes les autorités compétentes devraient également coopérer plus généralement avec d'autres autorités concernées, tant au niveau de l'Union qu'au niveau national.

([8]) Règlement (UE) nº 648/2012 du Parlement européen et du Conseil du 4 juillet 2012 sur les produits dérivés de gré à gré, les contreparties centrales et les référentiels centraux (JO L 201 du 27.7.2012, p. 1).

([9]) Règlement (UE) nº 575/2013 du Parlement européen et du Conseil du 26 juin 2013 concernant les exigences prudentielles applicables aux établissements de crédit et modifiant le règlement (UE) nº 648/2012 (JO L 176 du 27.6.2013, p. 1).

([10]) Règlement (UE) nº 600/2014 du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant le règlement (UE) nº 648/2012 (JO L 173 du 12.6.2014, p. 84).

([11]) Directive 2013/36/UE du Parlement européen et du Conseil du 26 juin 2013 concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement, modifiant la directive 2002/87/CE et abrogeant les directives 2006/48/CE et 2006/49/CE (JO L 176 du 27.6.2013, p. 338).

([12]) Directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE (JO L 173 du 12.6.2014, p. 349).

([13]) Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 et (UE) 2016/1011 (voir page 1 du présent Journal officiel).

(23) Afin de faciliter la coopération et la communication transfrontières et de permettre la mise en œuvre effective de la présente directive, et sans préjudice des exigences posées par des actes juridiques sectoriels de l'Union, chaque État membre devrait désigner un point de contact unique chargé de coordonner les questions liées à la résilience des entités critiques et à la coopération transfrontière au niveau de l'Union (ci-après dénommé «point de contact unique»), s'il y a lieu au sein d'une autorité compétente. Il convient que chaque point de contact unique assure la coordination de la communication et la liaison, s'il y a lieu, avec les autorités compétentes de son État membre, avec les points de contact uniques des autres États membres et avec le groupe sur la résilience des entités critiques.

(24) Les autorités compétentes en vertu de la présente directive et les autorités compétentes en vertu de la directive (UE) 2022/2555 devraient coopérer et échanger des informations sur les risques, menaces et incidents en matière de cybersécurité ainsi que sur les risques, menaces et incidents non liés à la cybersécurité affectant les entités critiques, et sur les mesures pertinentes prises par les autorités compétentes en vertu de la présente directive et les autorités compétentes en vertu de la directive (UE) 2022/2555 Il importe que les États membres veillent à ce que les exigences prévues par la présente directive et la directive (UE) 2022/2555 soient mises en œuvre de manière complémentaire et à ce que les entités critiques ne soient pas soumises à une charge administrative supérieure à ce qui est nécessaire pour atteindre les objectifs de la présente directive et de ladite directive.

(25) Les États membres devraient aider les entités critiques, y compris celles qui sont qualifiées de petites ou moyennes entreprises, à renforcer leur résilience, dans le respect des obligations qui incombent aux États membres en vertu de la présente directive, sans préjudice de la propre responsabilité juridique qui incombe aux entités critiques de garantir le respect de ces obligations et, ce faisant, éviter d'imposer une charge administrative excessive. En particulier, les États membres pourraient élaborer des documents d'orientation et des méthodologies, apporter leur soutien à l'organisation d'exercices visant à tester la résilience des entités critiques et dispenser des formations et fournir des conseils au personnel des entités critiques. Lorsque cela est nécessaire et justifié par des objectifs d'intérêt public, les États membres pourraient fournir des ressources financières et devraient faciliter le partage volontaire d'informations et l'échange de bonne pratiques entre les entités critiques, sans préjudice de l'application des règles de concurrence prévues par le traité sur le fonctionnement de l'Union européenne.

(26) En vue de renforcer la résilience des entités critiques recensées par les États membres et afin de réduire la charge administrative qui pèse sur ces entités critiques, les autorités compétentes devraient se consulter, chaque fois que cela est approprié, aux fins d'assurer l'application cohérente de la présente directive. Ces consultations devraient être engagées à la demande de toute autorité compétente concernée, et viser à assurer une approche convergente en ce qui concerne les entités critiques interconnectées qui utilisent des infrastructures critiques physiquement connectées entre deux ou plusieurs États membres, qui appartiennent aux mêmes groupes ou structures d'entreprise, ou qui ont été recensées dans un État membre et qui fournissent des services essentiels à ou dans d'autres États membres.

(27) Lorsque des dispositions du droit de l'Union ou du droit national exigent que les entités critiques évaluent les risques pertinents aux fins de la présente directive et qu'elles prennent des mesures pour garantir leur propre résilience, ces exigences devraient être suffisamment prises en considération aux fins de surveiller le respect de la présente directive par les entités critiques.

(28) Les entités critiques devraient avoir une connaissance approfondie des risques pertinents auxquels elles sont exposées et être tenues de les analyser. À cette fin, elles devraient procéder à des évaluations des risques chaque fois que cela s'avère nécessaire compte tenu de leurs circonstances particulières et de l'évolution de ces risques et, en tout cas, tous les quatre ans, afin d'évaluer tous les risques pertinents qui pourraient perturber la fourniture de leurs services essentiels (ci-après dénommée «évaluation des risques d'entité critique»). Lorsque les entités critiques ont procédé à d'autres évaluations des risques ou établi des documents en vertu d'obligations prévues par d'autres actes juridiques qui sont pertinents pour leur évaluation des risques d'entité critique, elles devraient pouvoir utiliser ces évaluations et documents pour satisfaire aux exigences énoncées dans la présente directive en ce qui concerne les évaluations des risques d'entités critiques. Une autorité compétente devrait pouvoir déclarer qu'une évaluation des risques existante réalisée par une entité critique qui porte sur les risques pertinents et le degré pertinent de dépendance respecte, en tout ou en partie, les obligations prévues par la présente directive.

(29) Les entités critiques devraient adopter des mesures techniques, des mesures de sécurité et des mesures organisationnelles appropriées et proportionnées aux risques auxquels elles sont confrontées, de manière à prévenir tout incident, à s'en protéger, à y réagir, à y résister, à l'atténuer, à l'absorber, à s'y adapter et à s'en remettre. Bien que les entités critiques soient tenues de prendre ces mesures conformément à la présente directive, les détails et la portée de ces mesures devraient refléter de manière appropriée et proportionnée les différents risques que chaque entité critique a recensés dans le cadre de son évaluation des risques d'entité critique et les spécificités de cette entité. Pour favoriser une approche cohérente de l'Union, la Commission devrait, après consultation du groupe sur la résilience des entités critiques, adopter des lignes directrices non contraignantes afin de préciser davantage ces mesures techniques, ces mesures de sécurité et ces mesures organisationnelles. Les États membres devraient veiller à ce que chaque entité critique désigne un agent de liaison ou une personne ayant une fonction équivalente en tant que point de contact avec les autorités compétentes.

(30) Dans un souci d'efficacité et de responsabilité, les entités critiques devraient décrire les mesures qu'elles prennent avec un niveau de détail suffisant pour atteindre les objectifs d'efficacité et de responsabilité, eu égard aux risques identifiés, dans un plan de résilience ou dans un ou plusieurs documents équivalents, et appliquer ce plan dans la pratique. Lorsqu'une entité critique a déjà pris des mesures techniques, des mesures de sécurité et des mesures organisationnelles et établi des documents en vertu d'autres actes juridiques qui sont pertinents aux fins des mesures de renforcement de la résilience au titre de la présente directive, elle devrait pouvoir, afin d'éviter les doubles emplois, utiliser ces mesures et documents pour satisfaire aux exigences en ce qui concerne les mesures de résilience au titre de la présente directive. Afin d'éviter les doubles emplois, une autorité compétente devrait pouvoir déclarer comme conformes, en tout ou en partie, aux exigences de la présente directive des mesures de résilience existantes prises par une entité critique qui répondent à son obligation de prendre des mesures techniques, des mesures de sécurité et des mesures organisationnelles.

(31) Les règlements (CE) nº 725/2004 ([14]) et (CE) nº 300/2008 ([15]) du Parlement européen et du Conseil et la directive 2005/65/CE du Parlement européen et du Conseil ([16]) définissent des exigences applicables aux entités des secteurs de l'aviation et du transport maritime afin de prévenir les incidents causés par des actes illicites, d'y résister et d'en atténuer les conséquences. Bien que les mesures requises par la présente directive soient plus larges en ce qui concerne les risques pris en compte et les types de mesures devant être prises, les entités critiques de ces secteurs devraient prendre en considération dans leur plan de résilience ou dans des documents équivalents les mesures prises en application de ces autres actes juridiques de l'Union. Les entités critiques doivent également prendre en considération la directive 2008/96/CE du Parlement européen et du Conseil ([17]), qui instaure une évaluation de l'ensemble du réseau routier pour cartographier les risques d'accidents et une inspection de sécurité routière ciblée, afin de déterminer les conditions dangereuses, les défauts et les problèmes qui augmentent le risque d'accidents et de blessures, sur la base de visites sur place de routes existantes ou de tronçons de route existants. Veiller à la protection et à la résilience des entités critiques est de la plus haute importance pour le secteur ferroviaire et, lorsqu'elles mettent en œuvre des mesures de résilience au titre de la présente directive, les entités critiques sont encouragées à se référer aux lignes directrices non contraignantes et aux documents de bonnes pratiques élaborés dans le cadre de groupes de travail sectoriels, tels que la plateforme de l'Union européenne en matière de sûreté des voyageurs ferroviaires créée par la décision 2018/C 232/03 de la Commission ([18]).

(32) Le risque que des membres du personnel des entités critiques ou de leurs contractants utilisent de manière abusive, par exemple leurs droits d'accès au sein de l'organisation de l'entité critique pour nuire et causer un préjudice est de plus en plus préoccupant. Les États membres devraient par conséquent préciser les conditions dans lesquelles les entités critiques sont autorisées, dans des cas dûment motivés et compte tenu des évaluations des risques d'États membres, à présenter des demandes de vérification des antécédents des personnes appartenant à des catégories spécifiques de leur personnel. Il convient de veiller à ce que les autorités concernées évaluent ces demandes dans un délai raisonnable et les traitent conformément au droit national et aux procédures nationales, et au droit de l'Union pertinent et applicable, y compris en matière de protection des données à caractère personnel. Afin de confirmer l'identité d'une personne faisant l'objet d'une vérification des antécédents, il convient que les États membres exigent une preuve de son identité, comme un passeport, une carte d'identité nationale ou une forme d'identification numérique, conformément au droit applicable.

([14]) Règlement (CE) nº 725/2004 du Parlement européen et du Conseil du 31 mars 2004 relatif à l'amélioration de la sûreté des navires et des installations portuaires (JO L 129 du 29.4.2004, p. 6).

([15]) Règlement (CE) nº 300/2008 du Parlement européen et du Conseil du 11 mars 2008 relatif à l'instauration de règles communes dans le domaine de la sûreté de l'aviation civile et abrogeant le règlement (CE) nº 2320/2002 (JO L 97 du 9.4.2008, p. 72).

([16]) Directive 2005/65/CE du Parlement européen et du Conseil du 26 octobre 2005 relative à l'amélioration de la sûreté des ports (JO L 310 du 25.11.2005, p. 28).

([17]) Directive 2008/96/CE du Parlement européen et du Conseil du 19 novembre 2008 concernant la gestion de la sécurité des infrastructures routières (JO L 319 du 29.11.2008, p. 59).

([18]) Décision de la Commission du 29 juin 2018 portant création de la plateforme de l'Union européenne en matière de sûreté des voyageurs ferroviaires 2018/C 232/03 (JO C 232 du 3.7.2018, p. 10).

Les vérifications des antécédents devraient également comprendre une vérification des casiers judiciaires de la personne concernée. Les États membres devraient utiliser le système européen d'information sur les casiers judiciaires conformément aux procédures prévues dans la décision-cadre 2009/315/JAI du Conseil ([19]) et, si cela est pertinent et applicable, dans le règlement (UE) 2019/816 du Parlement européen et du Conseil ([20]) aux fins d'obtenir des informations provenant des casiers judiciaires détenus par d'autres États membres. Les États membres pourraient aussi, et si cela est pertinent et applicable, s'appuyer sur le système d'information Schengen de deuxième génération (SIS II) établi par le règlement (UE) 2018/1862 du Parlement européen et du Conseil ([21]), sur des éléments de renseignement et sur toutes autres informations objectives disponibles qui pourraient être nécessaires pour déterminer si la personne concernée convient pour le poste pour lequel l'entité critique a demandé une vérification des antécédents.

(33) Il convient de mettre en place un mécanisme de notification de certains incidents afin de permettre aux autorités compétentes de réagir rapidement et de manière adéquate aux incidents et de disposer d'une vue d'ensemble complète de l'impact, de la nature, de la cause et des conséquences éventuelles d'incidents auxquels les entités critiques sont confrontées. Les entités critiques devraient notifier sans retard injustifié aux autorités compétentes les incidents qui perturbent ou sont susceptibles de perturber de manière importante la fourniture de services essentiels. À moins qu'elles n'en soient empêchées sur le plan opérationnel, les entités critiques devraient présenter une notification initiale au plus tard vingt-quatre heures après avoir pris connaissance d'un incident. La notification initiale ne devrait inclure que les informations strictement nécessaires pour porter l'incident à la connaissance de l'autorité compétente et permettre à l'entité critique de demander une assistance, si nécessaire. Une telle notification devrait indiquer, lorsque cela est possible, la cause présumée de l'incident. Les États membres devraient veiller à ce que l'obligation de présenter cette notification initiale ne détourne pas les ressources de l'entité critique des activités liées à la gestion de l'incident, qui devraient être prioritaires. La notification initiale devrait être suivie, s'il y a lieu, d'un rapport détaillé au plus tard un mois après l'incident. Le rapport détaillé devrait compléter la notification initiale et fournir une vue d'ensemble plus complète de l'incident.

(34) Il convient que la normalisation demeure un processus essentiellement conduit par le marché. Toutefois, il pourrait être approprié dans certaines situations d'exiger le respect de certaines normes. Les États membres devraient, lorsque cela est utile, promouvoir l'utilisation de normes européennes et internationales et de spécifications techniques pertinentes pour les mesures de sécurité et les mesures de résilience applicables aux entités critiques.

(35) Si les entités critiques exercent généralement leurs activités dans le cadre d'un réseau de fourniture de services et d'infrastructures de plus en plus interconnecté et fournissent souvent des services essentiels dans plus d'un État membre, certaines de ces entités critiques revêtent une importance particulière pour l'Union et son marché intérieur car elles fournissent des services essentiels à ou dans six États membres ou plus, et pourraient donc bénéficier d'un soutien spécifique au niveau de l'Union. Il y a donc lieu d'établir des règles relatives aux missions de conseil destinées à ces entités critiques d'importance européenne particulière. Ces règles sont sans préjudice des dispositions relatives à la supervision et à l'exécution des règles énoncées dans la présente directive.

(36) Sur demande motivée de la Commission ou d'un ou de plusieurs États membres auxquels ou dans lesquels le service essentiel est fourni, lorsque des informations supplémentaires sont nécessaires pour pouvoir conseiller une entité critique en vue du respect de ses obligations au titre de la présente directive ou pour évaluer le respect de ces obligations par une entité critique d'importance européenne particulière, l'État membre qui a désigné une entité critique d'importance européenne particulière en tant qu'entité critique devrait fournir certaines informations à la Commission, conformément à la présente directive. En accord avec l'État membre qui a désigné l'entité critique d'importance européenne particulière en tant qu'entité critique, la Commission devrait pouvoir organiser une mission de conseil afin d'évaluer les mesures mises en place par cette entité. Afin de garantir la bonne exécution de ces missions de conseil, il convient d'établir des règles complémentaires, notamment en ce qui concerne l'organisation et le déroulement des missions de conseil, les actions de suivi à entreprendre et les obligations incombant aux entités critiques d'importance européenne particulière concernées. Sans préjudice de la nécessité

([19]) Décision-cadre 2009/315/JAI du Conseil du 26 février 2009 concernant l'organisation et le contenu des échanges d'informations extraites du casier judiciaire entre les États membres (JO L 93 du 7.4.2009, p. 23).

([20]) Règlement (UE) 2019/816 du Parlement européen et du Conseil du 17 avril 2019 portant création d'un système centralisé permettant d'identifier les États membres détenant des informations relatives aux condamnations concernant des ressortissants de pays tiers et des apatrides (ECRIS-TCN), qui vise à compléter le système européen d'information sur les casiers judiciaires, et modifiant le règlement (UE) 2018/1726 (JO L 135 du 22.5.2019, p. 1).

([21]) Règlement (UE) 2018/1862 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, modifiant et abrogeant la décision 2007/533/JAI du Conseil, et abrogeant le règlement (CE) nº 1986/2006 du Parlement européen et du Conseil et la décision 2010/261/UE de la Commission (JO L 312 du 7.12.2018, p. 56).

pour l'État membre dans lequel la mission de conseil est menée et pour l'entité critique concernée de respecter les règles prévues par la présente directive, les missions de conseil devraient être menées sous réserve des règles détaillées du droit dudit État membre, par exemple en ce qui concerne les conditions précises à remplir pour obtenir l'accès aux locaux ou aux documents pertinents et les voies de recours juridictionnel. L'expertise spécifique requise pour de telles missions de conseil pourrait, selon les besoins, être demandée par l'intermédiaire du centre de coordination de la réaction d'urgence institué par la décision nº 1313/2013/UE du Parlement européen et du Conseil ([22]).

(37) Afin de soutenir la Commission et de faciliter la coopération entre les États membres et l'échange d'informations, y compris des bonnes pratiques, sur les questions liées à la présente directive, il convient de créer un groupe sur la résilience des entités critiques, en tant que groupe d'experts de la Commission. Les États membres devraient s'efforcer de veiller à ce que les représentants désignés de leurs autorités compétentes au sein du groupe sur la résilience des entités critiques coopèrent de manière efficace et efficiente, y compris en désignant des représentants qui disposent d'une habilitation de sécurité, s'il y a lieu. Le groupe sur la résilience des entités critiques devrait commencer à s'acquitter de ses tâches dès que possible, de manière à mettre à disposition des moyens supplémentaires pour une coopération appropriée pendant la période de transposition de la présente directive. Le groupe sur la résilience des entités critiques devrait interagir avec d'autres groupes de travail d'experts sectoriels pertinents.

(38) Le groupe sur la résilience des entités critiques devrait coopérer avec le groupe de coopération créé par la directive (UE) 2022/2555 afin de soutenir un cadre global pour la cyberrésilience et la résilience non liée à la cybersécurité des entités critiques. Le groupe sur la résilience des entités critiques et le groupe de coopération institué par la directive (UE) 2022/2555 devraient entretenir un dialogue régulier afin de promouvoir la coopération entre les autorités compétentes en vertu de la présente directive et les autorités compétentes en vertu de la directive (UE) 2022/2555 et de faciliter l'échange d'informations, notamment sur des sujets présentant un intérêt pour les deux groupes.

(39) Afin d'atteindre les objectifs de la présente directive, et sans préjudice de la responsabilité juridique qui incombe aux États membres et aux entités critiques de veiller au respect de leurs obligations respectives qui y sont énoncées, la Commission devrait, lorsqu'elle le juge approprié, soutenir les autorités compétentes et les entités critiques afin de faciliter le respect par celles-ci de leurs obligations respectives. Lorsqu'elle apporte un soutien aux États membres et aux entités critiques dans la mise en œuvre des obligations prévues dans la présente directive, la Commission devrait s'appuyer sur les structures et outils existants, tels que ceux relevant du mécanisme de protection civile de l'Union, établi par la décision nº 1313/2013/UE, et du réseau européen de référence pour la protection des infrastructures critiques. En outre, elle devrait informer les États membres des ressources disponibles au niveau de l'Union, par exemple au sein du Fonds pour la sécurité intérieure, établi par le règlement (UE) 2021/1149 du Parlement européen et du Conseil ([23]), d'Horizon Europe, établi par le règlement (UE) 2021/695 du Parlement européen et du Conseil ([24]), ou d'autres instruments pertinents pour la résilience des entités critiques.

(40) Les États membres devraient veiller à ce que leurs autorités compétentes disposent de certains pouvoirs spécifiques pour assurer la bonne application et l'exécution de la présente directive à l'égard des entités critiques, lorsque ces entités relèvent de leur compétence comme il est précisé dans la présente directive. Ces pouvoirs devraient comprendre notamment le pouvoir d'effectuer des inspections et des audits, le pouvoir de superviser, le pouvoir d'exiger des entités critiques qu'elles fournissent des informations et des éléments de preuve concernant les mesures qu'elles ont prises pour respecter leurs obligations et, lorsque c'est nécessaire, le pouvoir d'adresser des injonctions afin qu'il soit remédié aux violations constatées. Lorsqu'ils adressent de telles injonctions, les États membres ne devraient pas exiger de mesures allant au-delà de ce qui est nécessaire et proportionné pour garantir le respect par l'entité critique concernée des obligations qui lui incombent, compte tenu, notamment, de la gravité de la violation et de la capacité économique de l'entité critique concernée. Plus généralement, ces pouvoirs devraient

([22]) Décision nº 1313/2013/UE du Parlement européen et du Conseil du 17 décembre 2013 relative au mécanisme de protection civile de l'Union (JO L 347 du 20.12.2013, p. 924).

([23]) Règlement (UE) 2021/1149 du Parlement européen et du Conseil du 7 juillet 2021 établissant le Fonds pour la sécurité intérieure (JO L 251 du 15.7.2021, p. 94).

([24]) Règlement (UE) 2021/695 du Parlement européen et du Conseil du 28 avril 2021 portant établissement du programme-cadre pour la recherche et l'innovation «Horizon Europe» et définissant ses règles de participation et de diffusion, et abrogeant les règlements (UE) nº 1290/2013 et (UE) nº 1291/2013 (JO L 170 du 12.5.2021, p. 1).

s'accompagner de garanties appropriées et effectives, devant être précisées dans le droit national conformément à la Charte des droits fondamentaux de l'Union européenne. Lorsqu'elles évaluent le respect par les entités critiques des obligations que leur impose la présente directive, les autorités compétentes en vertu de la présente directive devraient pouvoir demander aux autorités compétentes en vertu de la directive (UE) 2022/2555 d'exercer leurs pouvoirs de supervision et d'exécution à l'égard d'une entité relevant de ladite directive qui a été désignée en tant qu'entité critique en vertu de la présente directive. Les autorités compétentes en vertu de la directive (UE) 2022/2555 devraient coopérer et échanger des informations à cette fin.

(41) Afin que la présente directive soit appliquée de manière effective et cohérente, il convient de déléguer à la Commission le pouvoir d'adopter des actes conformément à l'article 290 du traité sur le fonctionnement de l'Union européenne en vue de compléter la présente directive en dressant une liste des services essentiels. Cette liste devrait être utilisée par les autorités compétentes aux fins de la réalisation d'évaluations des risques d'États membres et du recensement des entités critiques en vertu de la présente directive. Compte tenu de l'approche fondée sur une harmonisation minimale suivie par la présente directive, cette liste n'est pas exhaustive et les États membres pourraient la compléter en y ajoutant d'autres services essentiels au niveau national afin de tenir compte des spécificités nationales en ce qui concerne la fourniture de services essentiels. Il importe particulièrement que la Commission procède aux consultations appropriées durant son travail préparatoire, y compris au niveau des experts, et que ces consultations soient menées conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016 «Mieux légiférer» ([25]). En particulier, pour assurer leur égale participation à la préparation des actes délégués, le Parlement européen et le Conseil reçoivent tous les documents au même moment que les experts des États membres, et leurs experts ont systématiquement accès aux réunions des groupes d'experts de la Commission traitant de la préparation des actes délégués.

(42) Afin d'assurer des conditions uniformes d'exécution de la présente directive, il convient de conférer des compétences d'exécution à la Commission. Ces compétences devraient être exercées conformément au règlement (UE) nº 182/2011 du Parlement européen et du Conseil ([26]).

(43) Étant donné que les objectifs de la présente directive, à savoir garantir que les services essentiels au maintien de fonctions sociétales ou d'activités économiques vitales soient fournis sans entrave dans le marché intérieur et améliorer la résilience des entités critiques qui fournissent de tels services, ne peuvent pas être atteints de manière suffisante par les États membres mais peuvent en raison des effets de l'action l'être mieux au niveau de l'Union, celle-ci peut prendre des mesures, conformément au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité énoncé audit article, la présente directive n'excède pas ce qui est nécessaire pour atteindre ces objectifs.

(44) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 du Parlement européen et du Conseil ([27]) et a rendu un avis le 11 août 2021.

(45) Il convient donc d'abroger la directive 2008/114/CE,

([25]) JO L 123 du 12.5.2016, p. 1.

([26]) Règlement (UE) nº 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission (JO L 55 du 28.2.2011, p. 13).

([27]) Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

ONT ADOPTÉ LA PRÉSENTE DIRECTIVE:

CHAPITRE I

DISPOSITIONS GÉNÉRALES

Article premier

Objet et champ d'application

1. La présente directive:

a) impose aux États membres l'obligation d'adopter des mesures spécifiques visant à garantir que les services qui sont essentiels au maintien de fonctions sociétales ou d'activités économiques vitales, dans le champ d'application de l'article 114 du traité sur le fonctionnement de l'Union européenne, soient fournis sans entrave dans le marché intérieur, en particulier l'obligation de recenser les entités critiques et l'obligation d' aider les entités critiques à s'acquitter des obligations qui leur incombent;

b) impose aux entités critiques des obligations visant à renforcer leur résilience et leur capacité à fournir les services visés au point a) dans le marché intérieur;

c) établit des règles relatives:

   i) à la supervision des entités critiques;

   ii) à l'exécution des règles;

   iii) au recensement des entités critiques d'importance européenne particulière, ainsi qu'aux missions de conseil pour évaluer les mesures que ces entités ont mises en place pour satisfaire aux obligations qui leur incombent en vertu du chapitre III;

d) établit des procédures communes en matière de coopération et d'établissement de rapports sur l'application de la présente directive;

e) prévoit des mesures visant à atteindre un niveau élevé de résilience des entités critiques afin de garantir la fourniture de services essentiels dans l'Union et d'améliorer le fonctionnement du marché intérieur.

2. La présente directive ne s'applique pas aux questions couvertes par la directive (UE) 2022/2555, sans préjudice de l'article 8 de la présente directive. La sécurité physique et la cybersécurité des entités critiques étant liées, les États membres veillent à ce que la présente directive et la directive (UE) 2022/2555 soient mises en œuvre de manière coordonnée.

3. Lorsque des dispositions d'actes juridiques sectoriels de l'Union exigent des entités critiques qu'elles adoptent des mesures pour renforcer leur résilience, et lorsque ces exigences sont reconnues par les États membres comme étant au moins équivalentes aux obligations correspondantes prévues par la présente directive, les dispositions pertinentes de la présente directive, y compris les dispositions relatives à la supervision et à l'exécution prévues au chapitre VI, ne s'appliquent pas.

4. Sans préjudice de l'article 346 du traité sur le fonctionnement de l'Union européenne, les informations qui sont confidentielles en application de règles de l'Union ou de règles nationales, telles que les règles relatives au secret des affaires, ne peuvent faire l'objet d'un échange avec la Commission et d'autres autorités concernées conformément à la présente directive que si cet échange est nécessaire à l'application de la présente directive. Les informations échangées se limitent à ce qui est nécessaire et proportionné à l'objectif de cet échange. L'échange d'informations préserve la confidentialité desdites informations ainsi que la sécurité et les intérêts commerciaux des entités critiques, tout en respectant la sécurité des États membres.

5. La présente directive est sans préjudice de la responsabilité des États membres en matière de sauvegarde de la sécurité nationale et de la défense et de leur pouvoir de garantir d'autres fonctions essentielles de l'État, notamment celles qui ont pour objet d'assurer l'intégrité territoriale de l'État et le maintien de l'ordre public.

6. La présente directive ne s'applique pas aux entités de l'administration publique qui exercent leurs activités dans les domaines de la sécurité nationale, de la sécurité publique, de la défense ou de l'application de la loi, y compris la détection des infractions pénales ainsi que les enquêtes et les poursuites en la matière.

7. Les États membres peuvent décider que l'article 11 et les chapitres III, IV et VI, en tout ou en partie, ne s'appliquent pas à certaines entités critiques qui exercent des activités dans les domaines de la sécurité nationale, de la sécurité publique, de la défense ou de l'application de la loi, y compris la détection des infractions pénales ainsi que les enquêtes et les poursuites en la matière, ou qui fournissent des services exclusivement aux entités de l'administration publique visées au paragraphe 6 du présent article.

8. Les obligations prévues dans la présente directive n'impliquent pas la fourniture d'informations dont la divulgation serait contraire aux intérêts essentiels des États membres en matière de sécurité nationale, de sécurité publique ou de défense.

9. La présente directive est sans préjudice du droit de l'Union relatif à la protection des données à caractère personnel, en particulier le règlement (UE) 2016/679 du Parlement européen et du Conseil ([28]) et la directive 2002/58/CE du Parlement européen et du Conseil ([29]).

Article 2

Définitions

Aux fins de la présente directive, on entend par:

1) «entité critique», une entité publique ou privée qui a été désignée par un État membre conformément à l'article 6 comme appartenant à l'une des catégories qui figurent dans la troisième colonne du tableau de l'annexe;

2) «résilience», la capacité d'une entité critique à prévenir tout incident, à s'en protéger, à y réagir, à y résister, à l'atténuer, à l'absorber, à s'y adapter et à s'en rétablir;

3) «incident», un événement qui perturbe ou est susceptible de perturber de manière importante la fourniture d'un service essentiel, y compris lorsqu'il affecte les systèmes nationaux qui préservent l'état de droit;

4) «infrastructure critique», un bien, une installation, un équipement, un réseau ou un système, ou une partie d'un bien, d'une installation, d'un équipement, d'un réseau ou d'un système, qui est nécessaire à la fourniture d'un service essentiel;

5) «service essentiel», un service qui est crucial pour le maintien de fonctions sociétales ou d'activités économiques vitales, de la santé publique et de la sûreté publique, ou de l'environnement;

6) «risque», le potentiel de perte ou de perturbation causé par un incident, à exprimer comme la combinaison de l'ampleur de cette perte ou de cette perturbation et la probabilité que l'incident se produise;

7) «évaluation des risques», l'ensemble du processus permettant de déterminer la nature et l'étendue d'un risque en déterminant et en analysant les menaces, les vulnérabilités et les dangers potentiels pertinents qui pourraient conduire à un incident et en évaluant la perte ou la perturbation potentielle de la fourniture d'un service essentiel causée par cet incident;

8) «norme», une norme au sens de l'article 2, point 1), du règlement (UE) nº 1025/2012 du Parlement européen et du Conseil ([30]);

([28]) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

([29]) Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO L 201 du 31.7.2002, p. 37).

([30]) Règlement (UE) nº 1025/2012 du Parlement européen et du Conseil du 25 octobre 2012 relatif à la normalisation européenne, modifiant les directives 89/686/CEE et 93/15/CEE du Conseil ainsi que les directives 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE et 2009/105/CE du Parlement européen et du Conseil et abrogeant la décision 87/95/CEE du Conseil et la décision nº 1673/2006/CE du Parlement européen et du Conseil (JO L 316 du 14.11.2012, p. 12).

9) «spécification technique», une spécification technique au sens de l'article 2, point 4), du règlement (UE) nº 1025/2012;

10) «entité de l'administration publique», une entité reconnue comme telle dans un État membre conformément au droit national, à l'exclusion de l'organisation judiciaire, des parlements et des banques centrales, qui satisfait aux critères suivants:

a) elle a été créée pour satisfaire des besoins d'intérêt général et n'a pas de caractère industriel ou commercial;

b) elle est dotée de la personnalité juridique ou est juridiquement habilitée à agir pour le compte d'une autre entité dotée de la personnalité juridique;

c) elle est financée majoritairement par les autorités de l'État ou d'autres organismes de droit public de niveau central, ou sa gestion est soumise à un contrôle de la part de ces autorités ou organismes, ou son organe d'administration, de direction ou de surveillance est composé, pour plus de la moitié, de membres désignés par les autorités de l'État ou d'autres organismes de droit public de niveau central;

d) elle a le pouvoir d'adresser à des personnes physiques ou morales des décisions administratives ou réglementaires affectant leurs droits en matière de mouvements transfrontières des personnes, des biens, des services ou des capitaux.

Article 3

Harmonisation minimale

La présente directive ne fait pas obstacle à l'adoption ou au maintien par les États membres de dispositions de droit national afin d'atteindre un niveau plus élevé de résilience des entités critiques, à condition que ces dispositions soient compatibles avec les obligations des États membres prévues par le droit de l'Union.

CHAPITRE II

CADRES NATIONAUX POUR LA RÉSILIENCE DES ENTITÉS CRITIQUES

Article 4

Stratégie pour la résilience des entités critiques

1. À la suite d'une consultation qui est, dans la mesure du possible en pratique, ouverte aux parties prenantes concernées, chaque État membre adopte, au plus tard le 17 janvier 2026, une stratégie visant à renforcer la résilience des entités critiques (ci-après dénommée «stratégie»). La stratégie définit des objectifs stratégiques et des mesures politiques, en s'appuyant sur des stratégies nationales et sectorielles, des plans ou des documents similaires pertinents existants, en vue d'atteindre et de maintenir un niveau élevé de résilience des entités critiques et de couvrir au moins les secteurs figurant à l'annexe.

2. Chaque stratégie contient au moins les éléments suivants:

a) les objectifs stratégiques et les priorités aux fins de renforcer la résilience globale des entités critiques, compte tenu des dépendances et des interdépendances transfrontières et transsectorielles;

b) un cadre de gouvernance permettant d'atteindre les objectifs stratégiques et les priorités, y compris une description des rôles et des responsabilités des différentes autorités, entités critiques et autres parties participant à la mise en œuvre de la stratégie;

c) une description des mesures nécessaires pour renforcer la résilience globale des entités critiques, y compris une description de l'évaluation des risques visée à l'article 5;

d) une description du processus par lequel les entités critiques sont recensées;

e) une description du processus de soutien aux entités critiques conformément au présent chapitre, y compris les mesures visant à renforcer la coopération entre le secteur public, d'une part, et le secteur privé et les entités publiques et privées, d'autre part;

f) une liste des principales autorités et parties prenantes concernées, autres que les entités critiques, participant à la mise en œuvre de la stratégie;

g) un cadre d'action pour la coordination entre les autorités compétentes en vertu de la présente directive (ci-après dénommées «autorités compétentes») et les autorités compétentes en vertu de la directive (UE) 2022/2555 aux fins du partage d'informations sur les risques, menaces et incidents en matière de cybersécurité ainsi que sur les risques, menaces et incidents non liés à la cybersécurité, et de l'exercice des tâches de supervision;

h) une description des mesures déjà en place visant à faciliter la mise en œuvre des obligations prévues au chapitre III de la présente directive par les petites et moyennes entreprises au sens de l'annexe de la recommandation 2003/361/CE de la Commission ([31]) que les États membres concernés ont recensées en tant qu'entités critiques.

À la suite d'une consultation qui est, dans la mesure du possible en pratique, ouverte aux parties prenantes concernées, les États membres mettent à jour leur stratégie au moins tous les quatre ans.

3. Les États membres communiquent leur stratégie et leurs mises à jour substantielles à la Commission dans un délai de trois mois à compter de leur adoption.

Article 5

Évaluation des risques par les États membres

1. La Commission est habilitée à adopter un acte délégué, conformément à l'article 23, au plus tard le 17 novembre 2023, afin de compléter la présente directive en établissant une liste non exhaustive de services essentiels dans les secteurs et les sous-secteurs figurant à l'annexe. Les autorités compétentes utilisent ladite liste des services essentiels pour effectuer une évaluation des risques (ci-après dénommée «évaluation des risques d'État membre») au plus tard le 17 janvier 2026, puis selon les besoins, et au moins tous les quatre ans. Les autorités compétentes utilisent les évaluations des risques d'États membres aux fins de recenser les entités critiques conformément à l'article 6 et pour aider les entités critiques à adopter des mesures en vertu de l'article 13.

Les évaluations des risques d'États membres rendent compte des risques naturels et d'origine humaine pertinents, y compris ceux qui revêtent un caractère transsectoriel ou transfrontière, des accidents, des catastrophes naturelles, des urgences de santé publique et des menaces hybrides ou autres menaces antagonistes, lesquelles comprennent les infractions terroristes prévues par la directive (UE) 2017/541 du Parlement européen et du Conseil ([32]).

2. Lorsqu'ils procèdent à des évaluations des risques d'États membres, les États membres tiennent compte au moins des éléments suivants:

a) l'évaluation des risques générale effectuée en vertu de l'article 6, paragraphe 1, de la décision nº 1313/2013/UE;

b) d'autres évaluations des risques pertinentes effectuées conformément aux exigences des actes juridiques sectoriels pertinents de l'Union, y compris les règlements (UE) 2017/1938 ([33]) et (UE) 2019/941 ([34]) du Parlement européen et du Conseil, ainsi que les directives 2007/60/CE ([35]) et 2012/18/UE ([36]) du Parlement européen et du Conseil;

([31]) Recommandation 2003/361/CE de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises (JO L 124 du 20.5.2003, p. 36).

([32]) Directive (UE) 2017/541 du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil (JO L 88 du 31.3.2017, p. 6).

([33]) Règlement (UE) 2017/1938 du Parlement européen et du Conseil du 25 octobre 2017 concernant des mesures visant à garantir la sécurité de l'approvisionnement en gaz naturel et abrogeant le règlement (UE) nº 994/2010 (JO L 280 du 28.10.2017, p. 1).

([34]) Règlement (UE) 2019/941 du Parlement européen et du Conseil du 5 juin 2019 sur la préparation aux risques dans le secteur de l'électricité et abrogeant la directive 2005/89/CE (JO L 158 du 14.6.2019, p. 1).

([35]) Directive 2007/60/CE du Parlement européen et du Conseil du 23 octobre 2007 relative à l'évaluation et à la gestion des risques d'inondation (JO L 288 du 6.11.2007, p. 27).

([36]) Directive 2012/18/UE du Parlement européen et du Conseil du 4 juillet 2012 concernant la maîtrise des dangers liés aux accidents majeurs impliquant des substances dangereuses, modifiant puis abrogeant la directive 96/82/CE du Conseil (JO L 197 du 24.7.2012, p. 1).

c) les risques pertinents découlant de la mesure dans laquelle les secteurs figurant à l'annexe dépendent les uns des autres, y compris de la mesure dans laquelle ils dépendent d'entités situées dans d'autres États membres et des pays tiers, et l'incidence qu'une perturbation importante dans un secteur peut avoir sur d'autres secteurs, y compris tout risque importante pour les citoyens et le marché intérieur;

d) toute information sur les incidents notifiés conformément à l'article 15.

Aux fins du premier alinéa, point c), les États membres coopèrent avec les autorités compétentes d'autres États membres et les autorités compétentes de pays tiers, s'il y a lieu.

3. Les États membres mettent à la disposition des entités critiques qu'ils ont recensées conformément à l'article 6, s'il y a lieu par l'intermédiaire de leur point de contact unique, les éléments pertinents des évaluations des risques d'États membres. Les États membres veillent à ce que les informations fournies aux entités critiques aident ces dernières à réaliser leurs évaluations des risques en vertu de l'article 12, et à adopter des mesures pour garantir leur résilience en vertu de l'article 13.

4. Dans un délai de trois mois à compter de la réalisation d'une évaluation des risques d'État membre, l'État membre fournit à la Commission des informations pertinentes sur les types de risques recensés suivant cette évaluation des risques d'État membre et les résultats de l'évaluation des risques d'État membre, par secteur et sous-secteur figurant à l'annexe.

5. La Commission, en coopération avec les États membres, élabore un modèle commun facultatif de rapport aux fins du respect du paragraphe 4.

Article 6

Recensement des entités critiques

1. Au plus tard le 17 juillet 2026, chaque État membre recense les entités critiques pour les secteurs et sous-secteurs figurant à l'annexe.

2. Lorsqu'un État membre recense les entités critiques en vertu du paragraphe 1, il tient compte des résultats de son évaluation des risques d'État membre et de sa stratégie et applique tous les critères suivants:

a) l'entité fournit un ou plusieurs services essentiels;

b) l'entité exerce ses activités sur le territoire dudit État membre et son infrastructure critique est située sur ledit territoire; et

c) un incident aurait des effets perturbateurs importants, déterminés conformément à l'article 7, paragraphe 1, sur la fourniture par l'entité d'un ou de plusieurs services essentiels ou sur la fourniture d'autres services essentiels dans les secteurs figurant à l'annexe qui dépendent dudit ou desdits services essentiels.

3. Chaque État membre dresse une liste des entités critiques recensées en vertu du paragraphe 2 et veille à ce que ces entités critiques reçoivent notification de ce qu'elles ont été recensées en tant qu'entités critiques dans un délai d'un mois à compter de ce recensement. Les États membres informent ces entités critiques des obligations qui leur incombent en vertu des chapitres III et IV et de la date à partir de laquelle ces obligations leur sont applicables, sans préjudice de l'article 8. Les États membres informent les entités critiques des secteurs figurant aux points 3, 4 et 8 du tableau de l'annexe qu'elles ne sont soumises à aucune des obligations prévues aux chapitres III et IV, sauf mesures nationales contraires.

Le chapitre III s'applique aux entités critiques concernées dix mois suivant la date de la notification visée au premier alinéa du présent paragraphe.

4. Les États membres veillent à ce que leurs autorités compétentes en vertu de la présente directive notifient aux autorités compétentes en vertu de la directive (UE) 2022/2555 l'identité des entités critiques qu'ils ont recensées en vertu du présent article dans un délai d'un mois à compter dudit recensement. Cette notification précise, le cas échéant, que les entités critiques concernées sont des entités des secteurs figurant aux points 3, 4 et 8 du tableau de l'annexe de la présente directive et qu'elles ne sont soumises à aucune des obligations prévues aux chapitres III et IV de la présente directive.

5. Si nécessaire et en tout état de cause au moins tous les quatre ans, les États membres réexaminent et, s'il y a lieu, mettent à jour la liste des entités critiques recensées visées au paragraphe 3. Lorsque ces mises à jour entraînent le recensement d'entités critiques supplémentaires, les paragraphes 3 et 4 s'appliquent à ces entités critiques supplémentaires. En outre, les États membres veillent à ce que les entités qui ne sont plus recensées en tant qu'entités critiques à la suite d'une telle mise à jour reçoivent notification en temps utile de ce fait et du fait qu'elles ne sont plus soumises aux obligations prévues au chapitre III à compter de la date de réception de cette notification.

6. La Commission élabore, en coopération avec les États membres, des recommandations et des lignes directrices non contraignantes pour soutenir les États membres dans leur recensement des entités critiques.

Article 7

Effet perturbateur important

1. Lorsqu'ils déterminent l'importance d'un effet perturbateur visé à l'article 6, paragraphe 2, point c), les États membres prennent en compte les critères suivants:

a) le nombre d'utilisateurs tributaires du service essentiel fourni par l'entité concernée;

b) la mesure dans laquelle les autres secteurs et sous-secteurs figurant à l'annexe dépendent du service essentiel en question;

c) l'impact que des incidents pourraient avoir, du point de vue de l'ampleur et de la durée, sur les activités économiques et sociétales, l'environnement, la sûreté et la sécurité publiques, ou la santé de la population;

d) la part de marché de l'entité sur le marché du ou des services essentiels concernés;

e) la zone géographique susceptible d'être affectée par un incident, y compris toute incidence transfrontière, compte tenu de la vulnérabilité associée au degré d'isolement de certains types de zones géographiques, telles que les régions insulaires, les régions éloignées ou les zones montagneuses;

f) l'importance que revêt l'entité pour le maintien d'un niveau suffisant de service essentiel, compte tenu de la disponibilité de solutions de rechange pour la fourniture de ce service essentiel.

2. Après le recensement des entités critiques en vertu de l'article 6, paragraphe 1, chaque État membre communique les informations suivantes à la Commission, sans retard injustifié:

a) une liste de services essentiels dans ledit État membre lorsqu'il existe des services essentiels supplémentaires par rapport à la liste des services essentiels visée à l'article 5, paragraphe 1;

b) le nombre d'entités critiques recensées pour chaque secteur et sous-secteur figurant à l'annexe et pour chaque service essentiel;

c) les seuils éventuellement appliqués en vue de préciser un ou plusieurs des critères du paragraphe 1.

Les seuils visés au premier alinéa, point c), peuvent être présentés tels quels ou sous une forme agrégée.

Les États membres communiquent ensuite les informations visées au premier alinéa, chaque fois que cela est nécessaire et au moins tous les quatre ans.

3. Après consultation du groupe sur la résilience des entités critiques visé à l'article 19, la Commission adopte des lignes directrices non contraignantes pour faciliter l'application des critères visés au paragraphe 1 du présent article, en tenant compte des informations visées au paragraphe 2 du présent article.

Article 8

Entités critiques des secteurs des banques, des infrastructures des marchés financiers et des infrastructures numériques

Les États membres veillent à ce que l'article 11 et les chapitres III, IV et VI ne s'appliquent pas aux entités critiques qu'ils ont recensées dans les secteurs figurant aux points 3, 4 et 8 du tableau de l'annexe. Les États membres peuvent adopter ou maintenir des dispositions de droit national afin d'atteindre un niveau de résilience plus élevé pour ces entités critiques à condition que ces dispositions soient compatibles avec le droit de l'Union applicable.

Article 9

Autorités compétentes et point de contact unique

1. Chaque État membre désigne ou met en place une ou plusieurs autorités compétentes chargées de veiller à l'application correcte des règles énoncées dans la présente directive au niveau national et, si nécessaire, de les faire respecter.

En ce qui concerne les entités critiques des secteurs figurant aux points 3 et 4 du tableau de l'annexe de la présente directive, les autorités compétentes sont, en principe, les autorités compétentes visées à l'article 46 du règlement (UE) 2022/2554 En ce qui concerne les entités critiques du secteur figurant au point 8 du tableau de l'annexe de la présente directive, les autorités compétentes sont, en principe, les autorités compétentes en vertu de la directive (UE) 2022/2555. Les États membres peuvent désigner une autorité compétente différente pour les secteurs figurant aux points 3, 4 et 8 du tableau de l'annexe de la présente directive conformément aux cadres nationaux existants.

Lorsqu'ils désignent ou mettent en place plus d'une autorité compétente, les États membres définissent clairement les tâches de chacune des autorités concernées et veillent à ce qu'elles coopèrent efficacement pour accomplir les tâches qui leur incombent en vertu de la présente directive, y compris en ce qui concerne la désignation et les activités du point de contact unique visé au paragraphe 2.

2. Chaque État membre désigne ou met en place un point de contact unique, chargé d'exercer une fonction de liaison afin d'assurer la coopération transfrontière avec les points de contact uniques des autres États membres et avec le groupe sur la résilience des entités critiques visé à l'article 19 (ci-après dénommé «point de contact unique»). S'il y a lieu, un État membre désigne son point de contact unique au sein d'une autorité compétente. S'il y a lieu, un État membre peut prévoir que son point de contact unique exerce également une fonction de liaison avec la Commission et assure la coopération avec les pays tiers.

3. Au plus tard le 17 juillet 2028, et tous les deux ans par la suite, les points de contact uniques présentent à la Commission et au groupe sur la résilience des entités critiques visé à l'article 19 un rapport de synthèse sur les notifications qu'ils ont reçues, mentionnant le nombre de notifications, la nature des incidents signalés et les mesures prises conformément à l'article 15, paragraphe 3.

La Commission, en coopération avec le groupe sur la résilience des entités critiques, élabore un modèle commun de rapport. Les autorités compétentes peuvent utiliser, à titre volontaire, ce modèle commun de rapport aux fins de la présentation des rapports de synthèse visés au premier alinéa.

4. Chaque État membre veille à ce que son autorité compétente et son point de contact unique disposent des pouvoirs et des ressources financières, humaines et techniques nécessaires pour accomplir, de manière efficace et efficiente, les tâches qui leur sont assignées.

5. Chaque État membre veille à ce que son autorité compétente consulte, chaque fois que cela est approprié, et conformément au droit de l'Union et au droit national, les autres autorités nationales concernées, y compris celles chargées de la protection civile, de l'application de la loi et de la protection des données à caractère personnel, et les entités critiques et les parties intéressées concernées, et à ce qu'elle coopère avec celles-ci.

6. Chaque État membre veille à ce que son autorité compétente en vertu de la présente directive coopère et échange des informations avec les autorités compétentes en vertu de la directive (UE) 2022/2555 sur les risques, menaces et incidents en matière de cybersécurité et sur les risques, menaces et incidents non liés à la cybersécurité affectant les entités critiques, y compris en ce qui concerne les mesures pertinentes que son autorité compétente et les autorités compétentes en vertu de la directive (UE) 2022/2555 ont prises.

7. Dans les trois mois à compter de la désignation ou de la mise en place de l'autorité compétente et du point de contact unique, chaque État membre notifie à la Commission leur identité et les tâches et responsabilités qui leur incombent en vertu de la présente directive, leurs coordonnées, ainsi que toute modification ultérieure y relative. Les États membres informent la Commission lorsqu'ils décident de désigner une autorité autre que les autorités compétentes visées au paragraphe 1, deuxième alinéa, en tant qu'autorités compétentes à l'égard des entités critiques des secteurs figurant aux points 3, 4 et 8 du tableau de l'annexe. Chaque État membre rend publique l'identité de son autorité compétente et de son point de contact unique.

8. La Commission met une liste des points de contact uniques à la disposition du public.

Article 10

Soutien des États membres aux entités critiques

1. Les États membres aident les entités critiques à renforcer leur résilience. Dans ce cadre, ils peuvent élaborer des documents d'orientation et des méthodologies, apporter leur soutien à l'organisation d'exercices visant à tester leur résilience et dispenser des conseils et des formations au personnel des entités critiques. Sans préjudice des règles applicables en matière d'aides d'État, les États membres peuvent fournir des ressources financières aux entités critiques, lorsque cela est nécessaire et justifié par des objectifs d'intérêt général.

2. Chaque État membre veille à ce que son autorité compétente coopère et échange des informations et des bonnes pratiques avec les entités critiques des secteurs figurant à l'annexe.

3. Les États membres facilitent le partage volontaire d'informations entre les entités critiques sur les questions couvertes par la présente directive, conformément au droit de l'Union et au droit national en matière, en particulier, d'informations classifiées et sensibles, de concurrence et de protection des données à caractère personnel.

Article 11

Coopération entre États membres

1. Chaque fois que cela est approprié, les États membres se consultent mutuellement au sujet des entités critiques aux fins d'assurer l'application cohérente de la présente directive. Ces consultations ont lieu en particulier au sujet des entités critiques qui:

a) utilisent des infrastructures critiques qui sont physiquement connectées entre deux États membres ou plus;

b) font partie de structures d'entreprise qui sont connectées ou liées à des entités critiques dans d'autres États membres;

c) ont été recensées en tant qu'entités critiques dans un État membre et fournissent des services essentiels à ou dans d'autres États membres.

2. Les consultations visées au paragraphe 1 visent à renforcer la résilience des entités critiques et, si possible, à réduire la charge administrative pesant sur celles-ci.

CHAPITRE III

RÉSILIENCE DES ENTITÉS CRITIQUES

Article 12

Évaluation des risques par les entités critiques

1. Nonobstant le délai énoncé à l'article 6, paragraphe 3, deuxième alinéa, les États membres veillent à ce que les entités critiques procèdent à une évaluation des risques dans un délai de neuf mois suivant la réception de la notification visée à l'article 6, paragraphe 3, selon les besoins par la suite et au moins tous les quatre ans, sur la base des évaluations des risques d'États membres et d'autres sources d'informations pertinentes, afin d'évaluer tous les risques pertinents qui pourraient perturber la fourniture de leur services essentiels (ci-après dénommée «évaluation des risques d'entité critique»).

2. Les évaluations des risques d'entités critiques rendent compte de tous les risques naturels et d'origine humaine pertinents, susceptibles d'entraîner un incident, y compris ceux qui revêtent un caractère transsectoriel ou transfrontière, des accidents, des catastrophes naturelles, des urgences de santé publique et des menaces hybrides et autres menaces antagonistes, lesquelles comprennent les infractions terroristes prévues par la directive (UE) 2017/541. Une évaluation des risques d'entité critique tient compte de la mesure dans laquelle d'autres secteurs figurant à l'annexe dépendent du service essentiel fourni par l'entité critique et de la mesure dans laquelle cette entité critique dépend des services essentiels fournis par d'autres entités de ces autres secteurs, y compris s'il y a lieu, dans les États membres voisins et les pays tiers.

Lorsqu'une entité critique a réalisé d'autres évaluations des risques ou établi des documents en vertu d'obligations prévues dans d'autres actes juridiques qui sont pertinents pour son évaluation des risques d'entité critique, elle peut utiliser ces évaluations et documents pour satisfaire aux exigences énoncées dans le présent article. Dans l'exercice de ses fonctions de supervision, l'autorité compétente peut déclarer qu'une évaluation des risques existante réalisée par une entité critique qui porte sur les risques et le degré de dépendance visés au premier alinéa du présent paragraphe respecte, en tout ou en partie, les obligations prévues par le présent article.

Article 13

Mesures de résilience des entités critiques

1. Les États membres veillent à ce que les entités critiques prennent des mesures techniques, des mesures de sécurité et des mesures organisationnelles appropriées et proportionnées pour garantir leur résilience, sur la base des informations pertinentes fournies par les États membres concernant l'évaluation des risques d'État membre et les résultats de l'évaluation des risques d'entité critique, y compris des mesures nécessaires pour:

a) prévenir la survenance d'incidents, en tenant dûment compte de mesures de réduction des risques de catastrophe et d'adaptation au changement climatique;

b) assurer une protection physique adéquate de leurs locaux et infrastructures critiques, en prenant dûment en considération, par exemple, des clôtures, des barrières, des outils et procédures de surveillance des enceintes, et des équipements de détection et de contrôle des accès;

c) réagir et résister aux conséquences des incidents et les atténuer, en prenant dûment en considération la mise en œuvre de procédures et protocoles de gestion des risques et des crises et de procédures d'alerte;

d) se rétablir d'incidents, en prenant dûment en considération des mesures assurant la continuité des activités et la détermination d'autres chaînes d'approvisionnement, afin de reprendre la fourniture du service essentiel;

e) assurer une gestion adéquate de la sécurité liée au personnel, en prenant dûment en considération des mesures telles que la définition des catégories de personnel qui exerce des fonctions critiques, l'établissement de droits d'accès aux locaux, aux infrastructures critiques et aux informations sensibles, la mise en place de procédures de vérification des antécédents conformément à l'article 14, la désignation des catégories de personnes tenues de faire l'objet de telles vérifications des antécédents et la définition d'exigences et de qualifications appropriées en matière de formation;

f) sensibiliser le personnel concerné aux mesures visées aux points a) à e), en tenant dûment compte des séances de formation, du matériel d'information et des exercices.

Aux fins du premier alinéa, point e), les États membres veillent à ce que les entités critiques tiennent compte du personnel des prestataires de services extérieurs lorsqu'ils définissent les catégories de personnel qui exerce des fonctions critiques.

2. Les États membres veillent à ce que les entités critiques aient mis en place et appliquent un plan de résilience ou un ou plusieurs documents équivalents, qui décrivent les mesures prises en application du paragraphe 1. Lorsque les entités critiques ont élaboré des documents ou pris des mesures en vertu d'obligations prévues dans d'autres actes juridiques qui sont pertinents pour les mesures visées au paragraphe 1, elles peuvent utiliser ces documents et mesures pour satisfaire aux exigences énoncées dans le présent article. Dans l'exercice de ses fonctions de supervision, l'autorité compétente peut déclarer que des mesures existantes de renforcement de la résilience prises par une entité critique qui portent, de manière appropriée et proportionnée, sur les mesures techniques, les mesures de sécurité et les mesures organisationnelles visées au paragraphe 1 respectent, en tout ou en partie, les obligations prévues par le présent article.

3. Les États membres veillent à ce que chaque entité critique désigne un agent de liaison ou une personne ayant une fonction équivalente en tant que point de contact avec les autorités compétentes.

4. À la demande de l'État membre qui a déterminé l'entité critique et avec l'accord de l'entité critique concernée, la Commission organise des missions de conseil, conformément aux modalités prévues à l'article 18, paragraphes 6, 8 et 9, afin de conseiller l'entité critique concernée en vue du respect des obligations qui lui incombent en vertu du chapitre III. La mission de conseil communique ses conclusions à la Commission, audit État membre et à l'entité critique concernée.

5. Après consultation du groupe sur la résilience des entités critiques visé à l'article 19, la Commission adopte des lignes directrices non contraignantes afin de préciser davantage les mesures techniques, les mesures de sécurité et les mesures organisationnelles qui peuvent être prises en vertu du paragraphe 1 du présent article.

6. La Commission adopte des actes d'exécution afin d'établir les spécifications techniques et méthodologiques nécessaires relatives à l'application des mesures visées au paragraphe 1 du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 24, paragraphe 2.

Article 14

Vérification des antécédents

1. Les États membres précisent les conditions dans lesquelles une entité critique est autorisée, dans des cas dûment motivés et compte tenu de l'évaluation des risques d'État membre, à présenter des demandes de vérification des antécédents des personnes:

a) qui occupent des fonctions sensibles au sein de l'entité critique ou au bénéfice de celle-ci, notamment en ce qui concerne la résilience de l'entité critique;

b) qui sont autorisées à avoir un accès direct ou à distance aux locaux et aux systèmes d'information ou de contrôle de l'entité critique, y compris en lien avec sa sécurité;

c) dont le recrutement est envisagé à des postes répondant aux critères énoncés au point a) ou b).

2. Les demandes visées au paragraphe 1 du présent article sont évaluées dans un délai raisonnable et traitées conformément au droit national et aux procédures nationales, ainsi qu'au droit de l'Union pertinent et applicable, y compris le règlement (UE) 2016/679 et la directive (UE) 2016/680 du Parlement européen et du Conseil ([37]). Les vérifications des antécédents sont proportionnées et strictement limitées à ce qui est nécessaire. Elles sont effectuées dans le seul but d'évaluer un risque potentiel pour la sécurité de l'entité critique concernée.

3. À tout le moins, une vérification des antécédents visée au paragraphe 1:

a) corrobore l'identité de la personne qui fait l'objet d'une demande de vérification des antécédents;

b) vérifie les casiers judiciaires de cette personne en ce qui concerne des infractions qui seraient pertinentes pour un poste déterminé;

Lors de la vérification des antécédents, les États membres, recourent au système européen d'information sur les casiers judiciaires conformément aux procédures prévues dans la décision-cadre 2009/315/JAI et, si cela est pertinent et applicable, dans le règlement (UE) 2019/816, aux fins de l'obtention des informations issues des casiers judiciaires détenus par d'autres États membres. Les autorités centrales visées à l'article 3, paragraphe 1, de la décision-cadre 2009/315/JAI et à l'article 3, point 5, du règlement (UE) 2019/816 répondent aux demandes d'informations dans un délai de dix jours ouvrables à compter de la date de réception de la demande conformément à l'article 8, paragraphe 1, de la décision-cadre 2009/315/JAI.

([37]) Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO L 119 du 4.5.2016, p. 89).

Article 15

Notification d'incidents

1. Les États membres veillent à ce que les entités critiques notifient sans retard injustifié à l'autorité compétente les incidents qui perturbent ou sont susceptibles de perturber de manière importante la fourniture de services essentiels. Les États membres veillent à ce que, sauf à être dans l'incapacité de le faire pour des raisons opérationnelles, les entités critiques présentent une première notification au plus tard 24 heures après avoir pris connaissance d'un incident, suivie, s'il y a lieu, d'un rapport détaillé au plus tard un mois après. Afin de déterminer l'importance de la perturbation, les paramètres suivants sont, en particulier, pris en compte:

a) le nombre et la proportion d'utilisateurs affectés par la perturbation;

b) la durée de la perturbation;

c) la zone géographique concernée par la perturbation, en tenant compte de son éventuel isolement géographique.

Lorsqu'un incident a ou pourrait avoir un impact important sur la continuité de la fourniture de services essentiels à ou dans six États membres ou plus, les autorités compétentes des États membres affectés par l'incident notifient ledit incident à la Commission.

2. Les notifications visées au paragraphe 1, premier alinéa, comprennent toutes les informations disponibles nécessaires pour permettre à l'autorité compétente de comprendre la nature, la cause et les conséquences possibles de l'incident, y compris toute information disponible nécessaire pour déterminer tout impact transfrontière de l'incident. Ces notifications n'ont pas pour effet de soumettre les entités critiques à une responsabilité accrue.

3. Sur la base des informations fournies par une entité critique dans une notification visée au paragraphe 1, l'autorité compétente concernée, par l'intermédiaire du point de contact unique, informe le point de contact unique des autres États membres affectés lorsque l'incident a ou pourrait avoir un impact important sur les entités critiques et sur la continuité de la fourniture de services essentiels à ou dans un ou plusieurs autres États membres.

Les points de contact uniques qui envoient et reçoivent des informations en vertu du premier alinéa traitent ces informations, conformément au droit de l'Union ou au droit national, de manière à en respecter la confidentialité et à préserver la sécurité et les intérêts commerciaux de l'entité critique concernée.

4. Dès que possible après la réception d'une notification visée au paragraphe 1, l'autorité compétente concernée fournit à l'entité critique concernée des informations de suivi pertinentes, y compris des informations qui pourraient aider ladite entité critique à réagir efficacement à l'incident en question. Les États membres informent le public lorsqu'ils estiment qu'il serait dans l'intérêt général de le faire.

Article 16

Normes

Afin de favoriser la mise en œuvre convergente de la présente directive, les États membres encouragent, lorsque c'est utile et sans imposer ni créer de discriminations en faveur de l'utilisation d'un type particulier de technologie, le recours à des normes et des spécifications techniques européennes et internationales pertinentes pour les mesures de sécurité et les mesures de résilience applicables aux entités critiques.

CHAPITRE IV

ENTITÉS CRITIQUES D'IMPORTANCE EUROPÉENNE PARTICULIÈRE

Article 17

Recensement des entités critiques d'importance européenne particulière

1. Une entité est considérée comme une entité critique d'importance européenne particulière lorsqu'elle:

a) a été désignée en tant qu'entité critique conformément à l'article 6, paragraphe 1;

b) fournit les mêmes services essentiels ou des services essentiels similaires à ou dans six États membres ou plus; et

c) elle a fait l'objet d'une notification conformément au paragraphe 3 du présent article.

2. Les États membres veillent à ce qu'une entité critique, à la suite de la notification visée à l'article 6, paragraphe 3, informe son autorité compétente lorsqu'elle fournit des services essentiels à ou dans six États membres ou plus. En pareil cas, les États membres veillent à ce que l'entité critique informe son autorité compétente au sujet des services essentiels qu'elle fournit à ou dans ces États membres et au sujet des États membres auxquels ou dans lesquels elle fournit ces services essentiels. Les États membres notifient à la Commission, sans retard injustifié, l'identité de ces entités critiques et les informations qu'elles fournissent au titre du présent paragraphe.

La Commission consulte l'autorité compétente de l'État membre qui a déterminé une entité critique visée au premier alinéa, l'autorité compétente des autres États membres concernés et l'entité critique en question. Lors de ces consultations, chaque État membre informe la Commission lorsqu'il estime que les services qui sont fournis audit État membre par l'entité critique sont des services essentiels.

3. Lorsque la Commission établit, sur la base des consultations visées au paragraphe 2 du présent article, que l'entité critique concernée fournit des services essentiels à ou dans six États membres ou plus, la Commission notifie à ladite entité critique, par l'intermédiaire de son autorité compétente, qu'elle est considérée comme une entité critique d'importance européenne particulière et l'informe des obligations qui lui incombent en vertu du présent chapitre et de la date à partir de laquelle ces obligations lui sont applicables. Une fois que la Commission informe l'autorité compétente de sa décision de considérer une entité critique comme une entité critique d'importance européenne particulière, l'autorité compétente transmet ladite notification à ladite entité critique sans retard injustifié.

4. Le présent chapitre s'applique à l'entité critique d'importance européenne particulière concernée à compter de la date de réception de la notification visée au paragraphe 3 du présent article.

Article 18

Missions de conseil

1. À la demande de l'État membre qui a désigné une entité critique d'importance européenne particulière en tant qu'entité critique en vertu de l'article 6, paragraphe 1, la Commission organise une mission de conseil afin d'évaluer les mesures mises en place par ladite entité pour satisfaire aux obligations qui lui incombent en vertu du chapitre III.

2. De sa propre initiative ou à la demande d'un ou de plusieurs États membres auxquels ou dans lesquels le service essentiel est fourni et à condition que l'État membre qui a désigné une entité critique d'importance européenne particulière en tant qu'entité critique en vertu de l'article 6, paragraphe 1, y consente, la Commission organise une mission de conseil visée au paragraphe 1.

3. Sur demande motivée de la Commission ou d'un ou de plusieurs des États membres auxquels ou dans lesquels le service essentiel est fourni, l'État membre qui a désigné une entité critique d'importance européenne particulière en tant qu'entité critique en vertu de l'article 6, paragraphe 1, communique à la Commission ce qui suit:

a) les éléments pertinents de l'évaluation des risques d'entité critique;

b) une liste des mesures pertinentes prises conformément à l'article 13;

c) toute mesure de supervision ou d'exécution, y compris des évaluations du respect des obligations qui ont été faites ou des injonctions qui ont été émises, prise par son autorité compétente en vertu des articles 21 et 22 à l'égard de ladite entité critique.

4. La mission de conseil communique ses conclusions à la Commission, à l'État membre qui a désigné une entité critique d'importance européenne particulière en tant qu'entité critique en vertu de l'article 6, paragraphe 1, aux États membres auxquels ou dans lesquels le service essentiel est fourni et à l'entité critique concernée, dans un délai de trois mois à compter de la fin de la mission de conseil.

Les États membres auxquels ou dans lesquels le service essentiel est fourni analysent le rapport visé au premier alinéa et, lorsque cela est nécessaire, conseillent la Commission quant à la question du respect par l'entité critique d'importance européenne particulière concernée des obligations qui lui incombent en vertu du chapitre III et, s'il y a lieu, quant aux mesures qui pourraient être prises pour améliorer la résilience de ladite entité critique.

Sur la base des conseils visés au deuxième alinéa du présent paragraphe, la Commission communique à l'État membre qui a désigné une entité critique d'importance européenne particulière en tant qu'entité critique en vertu de l'article 6, paragraphe 1, aux États membres auxquels ou dans lesquels le service essentiel est fourni et à ladite entité critique son avis quant à la question du respect par ladite entité critique des obligations qui lui incombent en vertu du chapitre III et, le cas échéant, quant aux mesures qui pourraient être prises pour améliorer la résilience de ladite entité critique.

L'État membre qui a désigné une entité critique d'importance européenne particulière en tant qu'entité critique en vertu de l'article 6, paragraphe 1, veille à ce que son autorité compétente et l'entité critique concernée tiennent compte de l'avis visé au troisième alinéa du présent paragraphe, et fournit à la Commission et aux États membres auxquels ou dans lesquels le service essentiel est fourni des informations sur les mesures qu'il a adoptées à la suite de cet avis.

5. Chaque mission de conseil est composée d'experts de l'État membre dans lequel se situe l'entité critique d'importance européenne particulière, d'experts des États membres auxquels ou dans lesquels le service essentiel est fourni et de représentants de la Commission. Ces États membres peuvent proposer des candidats à la participation à une mission de conseil. À la suite d'une consultation de l'État membre qui a désigné une entité critique d'importance européenne particulière en tant qu'entité critique en vertu de l'article 6, paragraphe 1, la Commission sélectionne et nomme les membres de chaque mission de conseil sur la base de leurs compétences professionnelles et en veillant, lorsque cela est possible, à une représentation géographique équilibrée de tous ces États membres. Chaque fois que cela est nécessaire, les membres de la mission de conseil disposent d'une habilitation de sécurité en cours de validité et au niveau approprié. La Commission prend en charge les coûts liés à la participation à des missions de conseil.

La Commission organise le programme de chaque mission de conseil, en concertation avec les membres de la mission de conseil en question et en accord avec l'État membre qui a désigné une entité critique d'importance européenne particulière en tant qu'entité critique en vertu de l'article 6, paragraphe 1.

6. La Commission adopte un acte d'exécution établissant les règles relatives aux modalités de procédure pour les demandes d'organisation de missions de conseil, le traitement de ces demandes, la conduite et les rapports des missions de conseil et pour le traitement de la communication de l'avis de la Commission visé au paragraphe 4, troisième alinéa, et des mesures prises, en tenant dûment compte de la confidentialité et du caractère commercial sensible des informations concernées. Cet acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 24, paragraphe 2.

7. Les États membres veillent à ce que les entités critiques d'importance européenne particulière accordent aux missions de conseil l'accès aux informations, systèmes et installations relatifs à la fourniture de leurs services essentiels nécessaires à l'exécution de la mission de conseil concernée.

8. Les missions de conseil sont menées dans le respect du droit national applicable de l'État membre dans lequel elles ont lieu, en respectant la responsabilité de cet État membre en matière de sécurité nationale et la protection de ses intérêts dans le domaine de la sécurité.

9. Lorsqu'elle organise des missions de conseil, la Commission tient compte des rapports de toute inspection qu'elle a effectuée en vertu des règlements (CE) nº 725/2004 et (CE) nº 300/2008, ainsi que des rapports de tout suivi qu'elle a effectué en vertu de la directive 2005/65/CE à l'égard de l'entité critique concernée.

10. La Commission informe le groupe sur la résilience des entités critiques visé à l'article 19 chaque fois qu'une mission de conseil est organisée. L'État membre dans lequel la mission de conseil a été menée et la Commission informent également le groupe sur la résilience des entités critiques des principales conclusions de la mission de conseil et des enseignements tirés en vue de favoriser l'apprentissage mutuel.

CHAPITRE V

COOPÉRATION ET RAPPORTS

Article 19

Groupe sur la résilience des entités critiques

1. Un groupe sur la résilience des entités critiques est institué. Le groupe sur la résilience des entités critiques soutient la Commission et facilite la coopération entre les États membres et l'échange d'informations sur les questions relatives à la présente directive.

2. Le groupe sur la résilience des entités critiques est composé de représentants des États membres et de la Commission qui, s'il y a lieu, disposent d'une habilitation de sécurité. Lorsque cela est pertinent pour l'exécution de ses tâches, le groupe sur la résilience des entités critiques peut inviter des parties prenantes concernées à participer à ses travaux. Lorsque le Parlement européen le demande, la Commission peut inviter des experts du Parlement européen à assister aux réunions du groupe sur la résilience des entités critiques.

Le représentant de la Commission préside le groupe sur la résilience des entités critiques.

3. Le groupe sur la résilience des entités critiques est chargé des tâches suivantes:

a) soutenir la Commission pour ce qui est d'aider les États membres à renforcer leur capacité à contribuer à garantir la résilience des entités critiques conformément à la présente directive;

b) analyser les stratégies afin de recenser les bonnes pratiques en ce qui concerne les stratégies;

c) faciliter l'échange de bonnes pratiques concernant le recensement des entités critiques par les États membres en vertu de l'article 6, paragraphe 1, y compris pour ce qui est des dépendances transfrontières et transsectorielles et en ce qui concerne les risques et incidents;

d) s'il y a lieu, contribuer, sur les questions relatives à la présente directive, aux documents relatifs à la résilience au niveau de l'Union;

e) contribuer à l'élaboration des lignes directrices visées à l'article 7, paragraphe 3, et à l'article 13, paragraphe 5, et, sur demande, de tout acte délégué ou de tout acte d'exécution adopté en vertu de la présente directive;

f) analyser les rapports de synthèse visés à l'article 9, paragraphe 3, en vue de promouvoir le partage des bonnes pratiques concernant les mesures prises conformément à l'article 15, paragraphe 3;

g) échanger les bonnes pratiques concernant la notification d'incidents visée à l'article 15;

h) examiner les rapports de synthèse des missions de conseil et les enseignements tirés conformément à l'article 18, paragraphe 10;

i) échanger des informations et les bonnes pratiques en matière d'innovation, de recherche et de développement concernant la résilience des entités critiques conformément à la présente directive;

j) s'il y a lieu, procéder à des échanges d'informations sur des questions relatives à la résilience des entités critiques avec les institutions, organes et organismes de l'Union concernés.

4. Au plus tard le 17 janvier 2025, puis tous les deux ans, le groupe sur la résilience des entités critiques établit un programme de travail prévoyant les actions à entreprendre pour réaliser ses objectifs et ses tâches. Ce programme de travail est cohérent avec les exigences et les objectifs de la présente directive.

5. Le groupe sur la résilience des entités critiques se réunit régulièrement et en tout état de cause au moins une fois par an avec le groupe de coopération institué en vertu de la directive (UE) 2022/2555 afin de promouvoir et de faciliter la coopération et l'échange d'informations.

6. La Commission peut adopter des actes d'exécution fixant les modalités de procédure nécessaires au fonctionnement du groupe sur la résilience des entités critiques, dans le respect de l'article 1er, paragraphe 4. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 24, paragraphe 2.

7. La Commission remet au groupe sur la résilience des entités critiques un rapport de synthèse concernant les informations communiquées par les États membres en vertu de l'article 4, paragraphe 3, et de l'article 5, paragraphe 4, au plus tard le 17 janvier 2027, puis chaque fois que cela est nécessaire et au moins tous les quatre ans.

Article 20

Soutien de la Commission aux autorités compétentes et aux entités critiques

1. La Commission aide, s'il y a lieu, les États membres et les entités critiques à respecter les obligations qui leur incombent en vertu de la présente directive. La Commission élabore une vue d'ensemble, au niveau de l'Union, des risques transfrontières et transsectoriels pesant sur la fourniture de services essentiels, organise les missions de conseil visées à l'article 13, paragraphe 4, et à l'article 18, et facilite l'échange d'informations entre États membres et experts dans l'ensemble de l'Union.

2. La Commission complète les activités des États membres visées à l'article 10 en élaborant des bonnes pratiques, des documents d'orientation et des méthodes, et des activités de formation et des exercices transfrontières pour tester la résilience des entités critiques.

3. La Commission informe les États membres des ressources financières à leur disposition au niveau de l'Union pour renforcer la résilience des entités critiques.

CHAPITRE VI

SUPERVISION ET EXÉCUTION

Article 21

Supervision et exécution

1. Afin d'évaluer le respect des obligations découlant de la présente directive par les entités qu'ils ont recensées en tant qu'entités critiques en vertu de l'article 6, paragraphe 1, de la présente directive, les États membres veillent à ce que les autorités compétentes disposent des pouvoirs et des moyens nécessaires pour:

a) procéder à des inspections sur place de l'infrastructure critique et des locaux utilisés par l'entité critique pour fournir ses services essentiels et à la supervision à distance des mesures prises par les entités critiques conformément à l'article 13;

b) effectuer ou ordonner des audits portant sur ces entités critiques.

2. Les États membres veillent à ce que les autorités compétentes disposent des pouvoirs et des moyens pour exiger que, lorsque l'exécution des tâches qui leur incombent en vertu de la présente directive le requiert, les entités en vertu de la directive (UE) 2022/2555 que les États membres ont recensées en tant qu'entités critiques en vertu de la présente directive fournissent, dans un délai raisonnable fixé par ces autorités:

a) les informations nécessaires pour évaluer si les mesures prises par ces entités pour garantir leur résilience satisfont aux exigences énoncées à l'article 13;

b) la preuve de la mise en œuvre effective de ces mesures, y compris les résultats d'un audit effectué par un auditeur indépendant et qualifié sélectionné par ladite entité et effectué à ses frais.

Lorsqu'elles requièrent ces informations, les autorités compétentes mentionnent la finalité de la demande et précisent les informations exigées.

3. Sans préjudice de la possibilité d'imposer des sanctions conformément à l'article 22, les autorités compétentes peuvent, à la suite des mesures de supervision visées au paragraphe 1 du présent article ou de l'évaluation des informations visées au paragraphe 2 du présent article, enjoindre aux entités critiques concernées de prendre les mesures nécessaires et proportionnées pour remédier à toute violation constatée de la présente directive, dans un délai raisonnable fixé par lesdites autorités, et de leur fournir des informations sur les mesures prises. Ces injonctions tiennent compte, notamment, de la gravité de la violation.

4. Les États membres veillent à ce que les pouvoirs prévus aux paragraphes 1, 2 et 3 ne puissent être exercés que sous réserve de garanties appropriées. Ces garanties font en sorte, en particulier, que les pouvoirs soient exercés de manière objective, transparente et proportionnée et que les droits et les intérêts légitimes des entités critiques concernées, tels que la protection des secrets commerciaux et d'affaires, soient dûment préservés, ce qui comprend le droit d'être entendu, les droits de la défense et le droit à un recours effectif devant une juridiction indépendante.

5. Les États membres veillent à ce que, lorsqu'une autorité compétente en vertu de la présente directive évalue le respect par une entité critique de ses obligations en vertu du présent article, ladite autorité compétente en informe les autorités compétentes des États membres concernés en vertu de la directive (UE) 2022/2555 À cette fin, les États membres veillent à ce que les autorités compétentes en vertu de la présente directive puissent demander aux autorités compétentes en vertu de la directive (UE) 2022/2555 d'exercer leurs pouvoirs de supervision et d'exécution à l'égard d'une entité relevant de ladite directive qui a été désignée en tant qu'entité critique en vertu de la présente directive. À cette fin, les États membres veillent à ce que les autorités compétentes en vertu de la présente directive coopèrent et échangent des informations avec les autorités compétentes en vertu de la directive (UE) 2022/2555

Article 22

Sanctions

Les États membres déterminent le régime des sanctions applicables aux violations des dispositions nationales adoptées conformément à la présente directive et prennent toutes les mesures nécessaires pour assurer la mise en œuvre de ces sanctions. Ces sanctions doivent être effectives, proportionnées et dissuasives. Les États membres informent la Commission, au plus tard le 17 octobre 2024 du régime ainsi déterminé et des mesures ainsi prises, de même que, sans retard, de toute modification apportée ultérieurement à ce régime ou à ces mesures.

CHAPITRE VII

ACTES DÉLÉGUÉS ET ACTES D'EXÉCUTION

Article 23

Exercice de la délégation

1. Le pouvoir d'adopter des actes délégués conféré à la Commission est soumis aux conditions fixées au présent article.

2. Le pouvoir d'adopter des actes délégués visé à l'article 5, paragraphe 1, est conféré à la Commission pour une période de cinq ans à compter du 16 janvier 2023.

3. La délégation de pouvoir visée à l'article 5, paragraphe 1, peut être révoquée à tout moment par le Parlement européen ou le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est précisée. La révocation prend effet le jour suivant celui de la publication de ladite décision au *Journal officiel de l'Union européenne* ou à une date ultérieure qui est précisée dans ladite décision. Elle ne porte pas atteinte à la validité des actes délégués déjà en vigueur.

4. Avant l'adoption d'un acte délégué, la Commission consulte les experts désignés par chaque État membre, conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016 «Mieux légiférer».

5. Aussitôt qu'elle adopte un acte délégué, la Commission le notifie au Parlement européen et au Conseil simultanément.

6. Un acte délégué adopté en vertu de l'article 5, paragraphe 1, n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de deux mois à compter de la notification de cet acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de leur intention de ne pas exprimer d'objections. Ce délai est prolongé de deux mois à l'initiative du Parlement européen ou du Conseil.

Article 24

Comité

1. La Commission est assistée par un comité. Ledit comité est un comité au sens du règlement (UE) nº 182/2011.

2. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) nº 182/2011 s'applique.

CHAPITRE VIII

DISPOSITIONS FINALES

Article 25

Rapports et réexamen

Au plus tard le 17 juillet 2027, la Commission présente au Parlement européen et au Conseil un rapport évaluant la mesure dans laquelle chaque État membre a pris les dispositions nécessaires pour se conformer à la présente directive.

La Commission réexamine périodiquement le fonctionnement de la présente directive et fait rapport au Parlement européen et au Conseil. Ce rapport évalue en particulier la valeur ajoutée de la présente directive, son impact en vue de garantir la résilience des entités critiques et détermine si l'annexe de la présente directive devrait être modifiée. La Commission présente le premier rapport de ce type au plus tard le 17 juin 2029. Aux fins de l'établissement des rapports au titre du présent article, la Commission tient compte des documents pertinents du groupe sur la résilience des entités critiques.

Article 26

Transposition

1. Les États membres adoptent et publient, au plus tard le 17 octobre 2024, les dispositions nécessaires pour se conformer à la présente directive. Ils en informent immédiatement la Commission.

Ils appliquent ces dispositions à partir du 18 octobre 2024.

2. Lorsque les États membres adoptent les dispositions visées au paragraphe 1, celles-ci contiennent une référence à la présente directive ou sont accompagnées d'une telle référence lors de leur publication officielle. Les modalités de cette référence sont arrêtées par les États membres.

Article 27

Abrogation de la directive 2008/114/CE

La directive 2008/114/CE est abrogée avec effet au 18 octobre 2024.

Les références faites à la directive abrogée s'entendent comme faites à la présente directive.

Article 28

Entrée en vigueur

La présente directive entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Article 29

Destinataires

Les États membres sont destinataires de la présente directive.

Fait à Strasbourg, le 14 décembre 2022.

Par le Parlement européen	*Par le Conseil*
La présidente	*Le président*
R. METSOLA	M. BEK

ANNEXE

SECTEURS, SOUS-SECTEURS ET CATÉGORIES D'ENTITÉS

Secteurs	Sous-secteurs	Catégories d'entités
1. Énergie	a) Électricité	— Entreprises d'électricité au sens de l'article 2, point 57), de la directive (UE) 2019/944 du Parlement européen et du Conseil ([1]), qui assurent la fonction de «fourniture» au sens de l'article 2, point 12), de ladite directive
		— Gestionnaires de réseau de distribution au sens de l'article 2, point 29), de la directive (UE) 2019/944
		— Gestionnaires de réseau de transport au sens de l'article 2, point 35), de la directive (UE) 2019/944
		— Producteurs au sens de l'article 2, point 38), de la directive (UE) 2019/944
		— Opérateurs désignés du marché de l'électricité au sens de l'article 2, point 8), du règlement (UE) 2019/943 du Parlement européen et du Conseil ([2])
		— Acteurs du marché au sens de l'article 2, point 25), du règlement (UE) 2019/943, qui fournissent des services d'agrégation, de participation active de la demande ou de stockage d'énergie au sens de l'article 2, points 18), 20) et 59), de la directive (UE) 2019/944
	b) Réseaux de chaleur et de froid	— Opérateurs de réseaux de chaleur ou de réseaux de froid au sens de l'article 2, point 19), de la directive (UE) 2018/2001 du Parlement européen et du Conseil ([3])
	c) Pétrole	— Exploitants d'oléoducs
		— Exploitants d'installations de production, de raffinage, de traitement, de stockage et de transport de pétrole
		— Entités centrales de stockage au sens de l'article 2, point f), de la directive 2009/119/CE du Conseil ([4])

Secteurs	Sous-secteurs	Catégories d'entités
	d) Gaz	— Entreprises de fourniture au sens de l'article 2, point 8), de la directive 2009/73/CE du Parlement européen et du Conseil ([5])
		— Gestionnaires de réseau de distribution au sens de l'article 2, point 6), de la directive 2009/73/CE
		— Gestionnaires de réseau de transport au sens de l'article 2, point 4), de la directive 2009/73/CE
		— Gestionnaires d'installation de stockage au sens de l'article 2, point 10), de la directive 2009/73/CE
		— Gestionnaires d'installation de GNL au sens de l'article 2, point 12), de la directive 2009/73/CE
		— Entreprises de gaz naturel au sens de l'article 2, point 1), de la directive 2009/73/CE
		— Exploitants d'installations de raffinage et de traitement de gaz naturel
	e) Hydrogène	— Exploitants de systèmes de production, de stockage et de transport d'hydrogène
2. Transports	a) Transports aériens	— Transporteurs aériens au sens de l'article 3, point 4), du règlement (CE) nº 300/2008 utilisés à des fins commerciales
		— Entités gestionnaires d'aéroports au sens de l'article 2, point 2), de la directive 2009/12/CE du Parlement européen et du Conseil ([6]), aéroports au sens de l'article 2, point 1), de ladite directive, y compris les aéroports du réseau central énumérés à l'annexe II, section 2, du règlement (UE) nº 1315/2013 du Parlement européen et du Conseil ([7]), et entités exploitant les installations annexes se trouvant dans les aéroports
		— Services du contrôle de la circulation aérienne assurant les services du contrôle de la circulation aérienne au sens de l'article 2, point 1), du règlement (CE) n° 549/2004 du Parlement européen et du Conseil ([8])

Secteurs	Sous-secteurs	Catégories d'entités
	b) Transports ferroviaires	— Gestionnaires de l'infrastructure au sens de l'article 3, point 2), de la directive 2012/34/UE du Parlement européen et du Conseil ([9])
		— Entreprises ferroviaires au sens de l'article 3, point 1), de la directive 2012/34/UE et exploitants d'installations de services au sens de l'article 3, point 12), de ladite directive
	c) Transports par eau	— Sociétés de transport par voie d'eau intérieure, maritime et côtier de passagers et de fret telles qu'elles sont définies pour le domaine du transport maritime visé à l'annexe I du règlement (CE) nº 725/2004, à l'exclusion des navires exploités à titre individuel par ces sociétés
		— Entités gestionnaires des ports au sens de l'article 3, point 1), de la directive 2005/65/CE, y compris les installations portuaires au sens de l'article 2, point 11), du règlement (CE) nº 725/2004, ainsi que les entités exploitant des ateliers et des équipements à l'intérieur des ports
		— Exploitants de services de trafic maritime (STM) au sens de l'article 3, point o), de la directive 2002/59/CE du Parlement européen et du Conseil ([10])
	d) Transports routiers	— Autorités routières au sens de l'article 2, point 12), du règlement délégué (UE) 2015/962 de la Commission ([11]) chargées du contrôle de la gestion de la circulation, à l'exclusion des entités publiques pour lesquelles la gestion de la circulation ou l'exploitation des systèmes de transport intelligents constituent une partie non essentielle de leur activité générale
		— Exploitants de systèmes de transport intelligents au sens de l'article 4, point 1), de la directive 2010/40/UE du Parlement européen et du Conseil ([12])
	e) Transports publics	— Opérateurs de services publics au sens de l'article 2, point d), du règlement (CE) nº 1370/2007 du Parlement européen et du Conseil ([13])
3. Secteur bancaire		— Établissements de crédit au sens de l'article 4, point 1), du règlement (UE) nº 575/2013
4. Infrastructures des marchés financiers		— Exploitants de plates-formes de négociation au sens de l'article 4, point 24), de la directive 2014/65/UE
		— Contreparties centrales au sens de l'article 2, point 1), du règlement (UE) nº 648/2012

Secteurs	Sous-secteurs	Catégories d'entités
5. Santé		— Prestataires de soins de santé au sens de l'article 3, point g), de la directive 2011/24/UE du Parlement européen et du Conseil ([14])
		— Laboratoires de référence de l'UE visés à l'article 15 du règlement (UE) 2022/2371 du Parlement européen et du Conseil ([15])
		— Entités exerçant des activités de recherche et de développement dans le domaine des médicaments au sens de l'article 1er, point 2), de la directive 2001/83/CE du Parlement européen et du Conseil ([16])
		— Entités fabriquant des produits pharmaceutiques de base et des préparations pharmaceutiques au sens de la NACE Rév. 2, section C, division 21
		— Entités fabriquant des dispositifs médicaux considérés comme critiques en cas d'urgence de santé publique (liste des dispositifs médicaux critiques en cas d'urgence de santé publique) au sens de l'article 22 du règlement (UE) 2022/123 du Parlement européen et du Conseil ([17])
		— Entités titulaires d'une autorisation de distribution au sens de l'article 79 de la directive 2001/83/CE
6. Eau potable		— Fournisseurs et distributeurs d'eaux destinées à la consommation humaine au sens de l'article 2, point 1) a), de la directive (UE) 2020/2184 du Parlement européen et du Conseil ([18]), à l'exclusion des distributeurs pour lesquels la distribution d'eaux destinées à la consommation humaine constitue une partie non essentielle de leur activité générale de distribution d'autres produits et biens
7. Eaux résiduaires		— Entreprises collectant, évacuant ou traitant les eaux urbaines résiduaires, des eaux ménagères usées ou des eaux industrielles usées au sens de l'article 2, points 1), 2) et 3), de la directive 91/271/CEE du Conseil ([19]), à l'exclusion des entreprises pour lesquelles la collecte, l'évacuation ou le traitement des eaux urbaines résiduaires, des eaux ménagères usées ou des eaux industrielles usées constituent une partie non essentielle de leur activité générale

Secteurs	Sous-secteurs	Catégories d'entités
8. Infrastructures numériques		— Fournisseurs de points d'échange internet au sens de l'article 6, point 18), de la directive (UE) 2022/2555
		— Fournisseurs de services DNS au sens de l'article 6, point 20), de la directive (UE) 2022/2555, à l'exclusion des opérateurs de serveurs racines de noms de domaines
		— Registres de noms de domaines de premier niveau au sens de l'article 6, point 21), de la directive (UE) 2022/2555
		— Fournisseurs de services d'informatique en nuage au sens de l'article 6, point 30), de la directive (UE) 2022/2555
		— Fournisseurs de services de centre de données au sens de l'article 6, point 31), de la directive (UE) 2022/2555
		— Fournisseurs de réseaux de diffusion de contenu au sens de l'article 6, point 32), de la directive (UE) 2022/2555
		— Prestataires de services de confiance au sens de l'article 3, point 19), du règlement (UE) nº 910/2014 du Parlement européen et du Conseil ([20])
		— Fournisseurs de réseaux de communications électroniques publics au sens de l'article 2, point 8), de la directive (UE) 2018/1972 du Parlement européen et du Conseil ([21])
		— Fournisseurs de services de communications électroniques au sens de l'article 2, point 4), de la directive (UE) 2018/1972 dans la mesure où leurs services sont accessibles au public
9. Administration publique		— Entités de l'administration publique des pouvoirs publics centraux définies comme telles par un État membre conformément au droit national
10. Espace		— Exploitants d'infrastructures au sol, détenues, gérées et exploitées par des États membres ou par des parties privées, qui soutiennent la fourniture de services spatiaux, à l'exclusion des fournisseurs de réseaux de communications électroniques publics au sens de l'article 2, point 8), de la directive (UE) 2018/1972

Secteurs	Sous-secteurs	Catégories d'entités
11. Production, transformation et distribution de denrées alimentaires		— Entreprises du secteur alimentaire au sens de l'article 3, point 2), du règlement (CE) nº 178/2002 du Parlement européen et du Conseil ([22]) qui exercent exclusivement des activités de logistique et de distribution en gros ainsi que de production et de transformation industrielles à grande échelle

([1]) Directive (UE) 2019/944 du Parlement européen et du Conseil du 5 juin 2019 concernant des règles communes pour le marché intérieur de l'électricité et modifiant la directive 2012/27/UE (JO L 158 du 14.6.2019, p. 125).
([2]) Règlement (UE) 2019/943 du Parlement européen et du Conseil du 5 juin 2019 sur le marché intérieur de l'électricité (JO L 158 du 14.6.2019, p. 54).
([3]) Directive (UE) 2018/2001 du Parlement européen et du Conseil du 11 décembre 2018 relative à la promotion de l'utilisation de l'énergie produite à partir de sources renouvelables (JO L 328 du 21.12.2018, p. 82).
([4]) Directive 2009/119/CE du Conseil du 14 septembre 2009 faisant obligation aux États membres de maintenir un niveau minimal de stocks de pétrole brut et/ou de produits pétroliers (JO L 265 du 9.10.2009, p. 9).
([5]) Directive 2009/73/CE du Parlement européen et du Conseil du 13 juillet 2009 concernant des règles communes pour le marché intérieur du gaz naturel et abrogeant la directive 2003/55/CE (JO L 211 du 14.8.2009, p. 94).
([6]) Directive 2009/12/CE du Parlement européen et du Conseil du 11 mars 2009 sur les redevances aéroportuaires (JO L 70 du 14.3.2009, p. 11).
([7]) Règlement (UE) nº 1315/2013 du Parlement européen et du Conseil du 11 décembre 2013 sur les orientations de l'Union pour le développement du réseau transeuropéen de transport et abrogeant la décision nº 661/2010/UE (JO L 348 du 20.12.2013, p. 1).
([8]) Règlement (CE) nº 549/2004 du Parlement européen et du Conseil du 10 mars 2004 fixant le cadre pour la réalisation du ciel unique européen («règlement-cadre») (JO L 96 du 31.3.2004, p. 1).
([9]) Directive 2012/34/UE du Parlement européen et du Conseil du 21 novembre 2012 établissant un espace ferroviaire unique européen (JO L 343 du 14.12.2012, p. 32).
([10]) Directive 2002/59/CE du Parlement européen et du Conseil du 27 juin 2002 relative à la mise en place d'un système communautaire de suivi du trafic des navires et d'information, et abrogeant la directive 93/75/CEE du Conseil (JO L 208 du 5.8.2002, p. 10).
([11]) Règlement délégué (UE) 2015/962 de la Commission du 18 décembre 2014 complétant la directive 2010/40/UE du Parlement européen et du Conseil en ce qui concerne la mise à disposition, dans l'ensemble de l'Union, de services d'informations en temps réel sur la circulation (JO L 157 du 23.6.2015, p. 21).
([12]) Directive 2010/40/UE du Parlement européen et du Conseil du 7 juillet 2010 concernant le cadre pour le déploiement de systèmes de transport intelligents dans le domaine du transport routier et d'interfaces avec d'autres modes de transport (JO L 207 du 6.8.2010, p. 1).
([13]) Règlement (CE) nº 1370/2007 du Parlement européen et du Conseil du 23 octobre 2007 relatif aux services publics de transport de voyageurs par chemin de fer et par route, et abrogeant les règlements (CEE) nº 1191/69 et (CEE) nº 1107/70 du Conseil (JO L 315 du 3.12.2007, p. 1).
([14]) Directive 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers (JO L 88 du 4.4.2011, p. 45).
([15]) Règlement (UE) 2022/2371 du Parlement européen et du Conseil du 23 novembre 2022 concernant les menaces transfrontières graves pour la santé et abrogeant la décision nº 1082/2013/UE (JO L 314 du 6.12.2022, p. 26).
([16]) Directive 2001/83/CE du Parlement européen et du Conseil du 6 novembre 2001 instituant un code communautaire relatif aux médicaments à usage humain (JO L 311 du 28.11.2001, p. 67).
([17]) Règlement (UE) 2022/123 du Parlement européen et du Conseil du 25 janvier 2022 relatif à un rôle renforcé de l'Agence européenne des médicaments dans la préparation aux crises et la gestion de celles-ci en ce qui concerne les médicaments et les dispositifs médicaux (JO L 20 du 31.1.2022, p. 1).
([18]) Directive (UE) 2020/2184 du Parlement européen et du Conseil du 16 décembre 2020 relative à la qualité des eaux destinées à la consommation humaine (JO L 435 du 23.12.2020, p. 1).
([19]) Directive 91/271/CEE du Conseil du 21 mai 1991 relative au traitement des eaux urbaines résiduaires (JO L 135 du 30.5.1991, p. 40).
([20]) Règlement (UE) nº 910/2014 du Parlement européen et 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 (JO L 257 du 28.8.2014, p. 73).
([21]) Directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen (JO L 321 du 17.12.2018, p. 36).
([22]) Règlement (CE) nº 178/2002 du Parlement européen et du Conseil du 28 janvier 2002 établissant les principes généraux et les prescriptions générales de la législation alimentaire, instituant l'Autorité européenne de sécurité des aliments et fixant des procédures relatives à la sécurité des denrées alimentaires (JO L 31 du 1.2.2002, p. 1).

FICHE D'ÉVALUATION D'IMPACT
MESURES LÉGISLATIVES, RÉGLEMENTAIRES ET AUTRES

Coordonnées du projet

Intitulé du projet :	Avant-projet de loi portant transposition de la directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, et abrogeant la directive 2008/114/CE du Conseil, et modifiant : 1. la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État ; 2. la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale
Ministère initiateur :	Ministère d'État
Auteur(s) :	Elisabeth Wirion / Carina Malheiro
Téléphone :	247-88912 / 247-88913
Courriel :	elisabeth.wirion@hcpn.etat.lu / carina.malheiro@hcpn.etat.lu
Objectif(s) du projet :	Le projet de loi vise à transposer la directive (UE) 2022/2557.
Autre(s) Ministère(s) / Organisme(s) / Commune(s) impliqué(e)(s)	L'élaboration du projet de loi a fait l'objet d'une collaboration étroite entre le Haut-Commissariat à la Protection nationale (HCPN), l'Institut luxembourgeois de régulation, la Commission de surveillance du secteur financier et la Police grand-ducale.
Date :	17/07/2023

Mieux légiférer

1 Partie(s) prenante(s) (organismes divers, citoyens,...) consultée(s) : ☐ Oui ☒ Non

Si oui, laquelle / lesquelles :

Remarques / Observations :

2 Destinataires du projet :

- Entreprises / Professions libérales : ☒ Oui ☐ Non
- Citoyens : ☐ Oui ☒ Non
- Administrations : ☒ Oui ☐ Non

3 Le principe « Think small first » est-il respecté ? ☐ Oui ☐ Non ☒ N.a. [1]
(c.-à-d. des exemptions ou dérogations sont-elles prévues suivant la taille de l'entreprise et/ou son secteur d'activité ?)

Remarques / Observations :

[1] N.a. : non applicable.

4 Le projet est-il lisible et compréhensible pour le destinataire ? ☒ Oui ☐ Non

Existe-t-il un texte coordonné ou un guide pratique, mis à jour et publié d'une façon régulière ? ☐ Oui ☒ Non

Remarques / Observations :

5 Le projet a-t-il saisi l'opportunité pour supprimer ou simplifier des régimes d'autorisation et de déclaration existants, ou pour améliorer la qualité des procédures ? ☐ Oui ☒ Non

Remarques / Observations :

6 Le projet contient-il une charge administrative[2] pour le(s) destinataire(s) ? (un coût imposé pour satisfaire à une obligation d'information émanant du projet ?) ☒ Oui ☐ Non

Si oui, quel est le coût administratif[3] approximatif total ? (nombre de destinataires x coût administratif par destinataire)

Divers coûts sont à supporter par les entités critiques afin de répondre aux exigences posées par le projet (évaluation des risques, élaboration d'un plan de résilience, notification des incidents).

[2] Il s'agit d'obligations et de formalités administratives imposées aux entreprises et aux citoyens, liées à l'exécution, l'application ou la mise en œuvre d'une loi, d'un règlement grand-ducal, d'une application administrative, d'un règlement ministériel, d'une circulaire, d'une directive, d'un règlement UE ou d'un accord international prévoyant un droit, une interdiction ou une obligation.

[3] Coût auquel un destinataire est confronté lorsqu'il répond à une obligation d'information inscrite dans une loi ou un texte d'application de celle-ci (exemple : taxe, coût de salaire, perte de temps ou de congé, coût de déplacement physique, achat de matériel, etc.).

7 a) Le projet prend-il recours à un échange de données inter-administratif (national ou international) plutôt que de demander l'information au destinataire ? ☐ Oui ☐ Non ☒ N.a.

Si oui, de quelle(s) donnée(s) et/ou administration(s) s'agit-il ?

b) Le projet en question contient-il des dispositions spécifiques concernant la protection des personnes à l'égard du traitement des données à caractère personnel[4] ? ☐ Oui ☐ Non ☒ N.a.

Si oui, de quelle(s) donnée(s) et/ou administration(s) s'agit-il ?

[4] Loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (www.cnpd.lu)

8 Le projet prévoit-il :

- une autorisation tacite en cas de non réponse de l'administration ? ☐ Oui ☒ Non ☐ N.a.
- des délais de réponse à respecter par l'administration ? ☐ Oui ☒ Non ☐ N.a.
- le principe que l'administration ne pourra demander des informations supplémentaires qu'une seule fois ? ☐ Oui ☒ Non ☐ N.a.

9 Y a-t-il une possibilité de regroupement de formalités et/ou de procédures (p.ex. prévues le cas échéant par un autre texte) ? ☒ Oui ☐ Non ☐ N.a.

Si oui, laquelle : Notification d'incidents prévue dans le projet de loi portant transposition de la directive 2022/2555

10 En cas de transposition de directives communautaires, le principe « la directive, rien que la directive » est-il respecté ? ☒ Oui ☐ Non ☐ N.a.

Sinon, pourquoi ?

11 Le projet contribue-t-il en général à une :

a) simplification administrative, et/ou à une ☐ Oui ☒ Non

b) amélioration de la qualité réglementaire ? ☐ Oui ☒ Non

Remarques / Observations :

12 Des heures d'ouverture de guichet, favorables et adaptées aux besoins du/des destinataire(s), seront-elles introduites ? ☐ Oui ☒ Non ☐ N.a.

13 Y a-t-il une nécessité d'adapter un système informatique auprès de l'Etat (e-Government ou application back-office) ☒ Oui ☐ Non

Si oui, quel est le délai pour disposer du nouveau système ?

14 Y a-t-il un besoin en formation du personnel de l'administration concernée ? ☐ Oui ☐ Non ☒ N.a.

Si oui, lequel ?

Remarques / Observations :

Egalité des chances

15 Le projet est-il :

- principalement centré sur l'égalité des femmes et des hommes ? ☐ Oui ☒ Non
- positif en matière d'égalité des femmes et des hommes ? ☐ Oui ☒ Non

Si oui, expliquez de quelle manière :

- neutre en matière d'égalité des femmes et des hommes ? ☒ Oui ☐ Non

Si oui, expliquez pourquoi :

- négatif en matière d'égalité des femmes et des hommes ? ☐ Oui ☒ Non

Si oui, expliquez de quelle manière :

16 Y a-t-il un impact financier différent sur les femmes et les hommes ? ☐ Oui ☒ Non ☐ N.a.

Si oui, expliquez de quelle manière :

Directive « services »

17 Le projet introduit-il une exigence relative à la liberté d'établissement soumise à évaluation[5] ? ☐ Oui ☐ Non ☒ N.a.

Si oui, veuillez annexer le formulaire A, disponible au site Internet du Ministère de l'Economie et du Commerce extérieur :

www.eco.public.lu/attributions/dg2/d_consommation/d_march___int__rieur/Services/index.html

[5] Article 15 paragraphe 2 de la directive « services » (cf. Note explicative, p.10-11)

18 Le projet introduit-il une exigence relative à la libre prestation de services transfrontaliers[6] ? ☐ Oui ☐ Non ☒ N.a.

Si oui, veuillez annexer le formulaire B, disponible au site Internet du Ministère de l'Economie et du Commerce extérieur :

www.eco.public.lu/attributions/dg2/d_consommation/d_march___int__rieur/Services/index.html

[6] Article 16, paragraphe 1, troisième alinéa et paragraphe 3, première phrase de la directive « services » (cf. Note explicative, p.10-11)

CHECK DE DURABILITÉ - NOHALTEGKEETSCHECK

⚠ La présente page interactive nécessite au minimum la version 8.1.3 d'Adobe Acrobat® Reader®. La dernière version d'Adobe Acrobat Reader pour tous systèmes (Windows®, Mac, etc.) est téléchargeable gratuitement sur le site de Adobe Systems Incorporated.

Ministre responsable :	Le Premier Ministre, Ministre d'État
Projet de loi ou amendement :	Avant-projet de loi portant transposition de la directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, et abrogeant la directive 2008/114/CE du Conseil, et modifiant 1° la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État ; 2° la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale

Le check de durabilité est un outil d'évaluation des actes législatifs par rapport à leur impact sur le developpement durable. Son objectif est de donner l'occasion d'introduire des aspects relatifs au développement durable à un stade préparatoire des projets de loi. Tout en faisant avancer ce thème transversal qu'est le developpement durable, il permet aussi d'assurer une plus grande cohérence politique et une meilleure qualité des textes législatifs.

1. Est-ce que le projet de loi sous rubrique a un impact sur le champ d'action (1-10) du 3ième Plan national pour un développement durable (PNDD) ?
   En cas de réponse négative, expliquez-en succinctement les raisons.
   En cas de réponse positive sous 1., quels seront les effets positifs et/ou négatifs éventuels de cet impact ?

2. Quelles catégories de personnes seront touchées par cet impact ?

3. Quelles mesures sont envisagées afin de pouvoir atténuer les effets négatifs et comment pourront être renforcés les aspects positifs de cet impact ?

Afin de faciliter cet exercice, l'instrument du contrôle de la durabilité est accompagné par des points d'orientation – **auxquels il n'est pas besoin de réagir ou répondre mais qui servent uniquement d'orientation**, ainsi que par une documentation sur les dix champs d'actions précités.

1. Assurer une inclusion sociale et une éducation pour tous.

Points d'orientation Documentation ☐Oui ☒Non

Cet avant-projet de loi ne s'applique pas à toute la population. Il s'applique aux entités critiques et ne contribue donc pas à favoriser une inclusion sociale et une éducation pour tous.

2. Assurer les conditions d'une population en bonne santé.

Points d'orientation Documentation ☐Oui ☒Non

Cet avant-projet de loi ne s'applique pas à toute la population. Il s'applique aux entités critiques et n'a donc pas de lien avec la santé de la population.

3. Promouvoir une consommation et une production durables.

Points d'orientation Documentation ☐Oui ☒Non

Cet avant-projet de loi concerne la résilience des entités critiques et n'a pas d'impact sur la consommation ou la production durables.

4. Diversifier et assurer une économie inclusive et porteuse d'avenir. Points d'orientation Documentation ☐Oui ☒Non

Cet avant-projet de loi concerne la résilience des entités critiques et n'a pas d'influence sur la diversification d'une économie inclusive et porteuse d'avenir.

5. Planifier et coordonner l'utilisation du territoire. Points d'orientation Documentation ☐Oui ☒Non

Cet avant-projet de loi, relatif à la résilience des entités critiques, n'a pas d'impact sur la coordination et la planification de l'utilisation du territoire luxembourgeois.

6. Assurer une mobilité durable. Points d'orientation Documentation ☐Oui ☒Non

Cet avant-projet de loi n'a pas d'impact sur la mobilité durable.

7. Arrêter la dégradation de notre environnement et respecter les capacités des ressources naturelles. Points d'orientation Documentation ☐Oui ☒Non

Cet avant-projet de loi n'a pas d'effet sur l'environnement ou les ressources naturelles.

8. Protéger le climat, s'adapter au changement climatique et assurer une énergie durable. Points d'orientation Documentation ☐Oui ☒Non

A travers cet avant-projet de loi, les entités critiques devront s'adapter aux risques résultants du changement climatique et être capables d'en faire face, mais cela n'a pas d'impact direct sur le climat, le changement climatique ou l'énergie durable.

9. Contribuer, sur le plan global, à l'éradication de la pauvreté et à la cohérence des politiques pour le développement durable. Points d'orientation Documentation ☐Oui ☒Non

Cet avant-projet de loi n'a pas d'impact sur la pauvreté ou sur la cohérence des politiques pour le développement durable.

10. Garantir des finances durables. Points d'orientation Documentation ☐Oui ☒Non

Cet avant-projet de loi ne contribuera pas financièrement à l'action climatique, ni au développement durable.

Cette partie du formulaire est facultative - Veuillez cocher la case correspondante

En outre, et dans une optique d'enrichir davantage l'analyse apportée par le contrôle de la durabilité, il est proposé de recourir, de manière facultative, à une évaluation de l'impact des mesures sur base d'indicateurs retenus dans le PNDD. Ces indicateurs sont suivis par le STATEC.

Continuer avec l'évaluation ? ☒Oui ☐Non

(1) Dans le tableau, choisissez l'évaluation : **non applicable**, ou de 1 = **pas du tout probable** à 5 = **très possible**

Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
1	non app	Contribue à la réduction du taux de risque de pauvreté ou d'exclusion sociale	Taux de risque de pauvreté ou d'exclusion sociale	% de la population
1	non app	Contribue à la réduction du nombre de personnes vivant dans des ménages à très faible intensité de travail	Personnes vivant dans des ménages à très faible intensité de travail	milliers
1	non app	Contribue à la réduction de la différence entre taux de risque de pauvreté avant et après transferts sociaux	Différence entre taux de risque de pauvreté avant et après transferts sociaux	pp
1	non app	Contribue à l'augmentation du taux de certification nationale	Taux de certification nationale	%
1	non app	Contribue à l'apprentissage tout au long de la vie en % de la population de 25 à 64 ans	Apprentissage tout au long de la vie en % de la population de 25 à 64 ans	%
1	non app	Contribue à l'augmentation de la représentation du sexe sous-représenté dans les organes de prises de décision	Représentation du sexe sous-représenté dans les organes de prises de décision	%
1	non app	Contribue à l'augmentation de la proportion des sièges détenus par les femmes au sein du parlement national	Proportion des sièges détenus par les femmes au sein du parlement national	%
1	non app	Contribue à l'amélioration de la répartition des charges de travail domestique dans le sens d'une égalité des genres	Temps consacré au travail domestique non payé et activités bénévoles	hh:mm
1	non app	Contribue à suivre l'impact du coût du logement afin de circonscrire le risque d'exclusion sociale	Indice des prix réels du logement	Indice 2015=100
2	non app	Contribue à la réduction du taux de personnes en surpoids ou obèses	Taux de personnes en surpoids ou obèses	% de la population
2	non app	Contribue à la réduction du nombre de nouveaux cas d'infection au VIH	Nombre de nouveaux cas d'infection au VIH	Nb de personnes
2	non app	Contribue à la réduction de l'incidence de l'hépatite B pour 100 000 habitants	Incidence de l'hépatite B pour 100 000 habitants	Nb de cas pour 100 000 habitants
2	non app	Contribue à la réduction du nombre de décès prématurés liés aux maladies chroniques pour 100 000 habitants	Nombre de décès prématurés liés aux maladies chroniques pour 100 000 habitants	Nb de décès pour 100 000 habitants
2	non app	Contribue à la réduction du nombre de suicides pour 100 000 habitants	Nombre de suicides pour 100 000 habitants	Nb de suicides pour 100 000 habitants
2	non app	Contribue à la réduction du nombre de décès liés à la consommation de psychotropes	Nombre de décès liés à la consommation de psychotropes	Nb de décès

Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
2	non app	Contribue à la réduction du taux de mortalité lié aux accidents de la route pour 100 000 habitants	Taux de mortalité lié aux accidents de la route pour 100 000 habitants	Nb de décès pour 100 000 habitants
2	non app	Contribue à la réduction de la proportion de fumeurs	Proportion de fumeurs	% de la population
2	non app	Contribue à la réduction du taux de natalité chez les adolescentes pour 1 000 adolescentes	Taux de natalité chez les adolescentes pour 1 000 adolescentes	Nb de naissance pour 1 000 adolescentes
2	non app	Contribue à la réduction du nombre d'accidents du travail	Nombre d'accidents du travail (non mortel + mortel)	Nb d'accidents
3	non app	Contribue à l'augmentation de la part de la surface agricole utile (SAU) en agriculture biologique	Part de la surface agricole utile (SAU) en agriculture biologique	% de la surface agricole utile (SAU)
3	non app	Contribue à l'augmentation de la productivité de l'agriculture par heure travaillée	Productivité de l'agriculture par heure travaillée	Indice 2010=100
3	non app	Contribue à la réduction d'exposition de la population urbaine à la pollution de l'air par les particules fines	Exposition de la population urbaine à la pollution de l'air par les particules fines	Microgrammes par m^3
3	non app	Contribue à la réduction de production de déchets par habitant	Production de déchets par habitant	kg/hab
3	non app	Contribue à l'augmentation du taux de recyclage des déchets municipaux	Taux de recyclage des déchets municipaux	%
3	non app	Contribue à l'augmentation du taux de recyclage des déchets d'équipements électriques et électroniques	Taux de recyclage des déchets d'équipements électriques et électroniques	%
3	non app	Contribue à la réduction de la production de déchets dangereux	Production de déchets dangereux	tonnes
3	non app	Contribue à l'augmentation de la production de biens et services environnementaux	Production de biens et services environnementaux	millions EUR
3	non app	Contribue à l'augmentation de l'intensité de la consommation intérieure de matière	Intensité de la consommation intérieure de matière	tonnes / millions EUR
4	non app	Contribue à la réduction des jeunes sans emploi et ne participant ni à l'éducation ni à la formation (NEET)	Jeunes sans emploi et ne participant ni à l'éducation ni à la formation (NEET)	% de jeunes
4	non app	Contribue à l'augmentation du pourcentage des intentions entreprenariales	Pourcentage des intentions entreprenariales	%
4	non app	Contribue à la réduction des écarts de salaires hommes-femmes	Ecarts de salaires hommes-femmes	%
4	non app	Contribue à l'augmentation du taux d'emploi	Taux d'emploi	% de la population

Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
4	non app	Contribue à la création d'emplois stables	Proportion de salariés ayant des contrats temporaires	% de l'emploi total
4	non app	Contribue à la réduction de l'emploi à temps partiel involontaire	Emploi à temps partiel involontaire	% de l'emploi total
4	non app	Contribue à la réduction des salariés ayant de longues heures involontaires	Salariés ayant de longues heures involontaires	% de l'emploi total
4	non app	Contribue à la réduction du taux de chômage	Taux de chômage	% de la population active
4	non app	Contribue à la réduction du taux de chômage longue durée	Taux de chômage longue durée	% de la population active
4	non app	Contribue à l'augmentation du taux de croissance du PIB réel (moyenne sur 3 ans)	Taux de croissance du PIB réel (moyenne sur 3 ans)	%
4	non app	Contribue à l'augmentation de la productivité globale des facteurs	Productivité globale des facteurs	Indice 2010=100
4	non app	Contribue à l'augmentation de la productivité réelle du travail par heures travaillées (taux de croissance moyen sur 3 ans)	Productivité réelle du travail par heures travaillées (taux de croissance moyen sur 3 ans)	%
4	non app	Contribue à l'augmentation de la productivité des ressources	Productivité des ressources	Indice 2000=100
4	non app	Contribue à l'augmentation de la valeur ajoutée dans l'industrie manufacturière	Valeur ajoutée dans l'industrie manufacturière, en proportion de la valeur ajoutée totale des branches	% de la VA totale
4	non app	Contribue à l'augmentation de l'emploi dans l'industrie manufacturière	Emploi dans l'industrie manufacturière, en proportion de l'emploi total	% de l'emploi
4	non app	Contribue à la réduction des émissions de CO_2 de l'industrie manufacturière	Émissions de CO_2 de l'industrie manufacturière par unité de valeur ajoutée	% de la VA totale
4	non app	Contribue à l'augmentation des dépenses intérieures brutes de "Research & Development"	Niveau des dépenses intérieures brute de "Research & Development"	% du PIB
4	non app	Contribue à l'augmentation du nombre de chercheurs	Nombre de chercheurs pour 1 000 actifs	nb pour 1 000 actifs
5	non app	Contribue à la réduction du nombre de personnes confrontées à la délinquance, à la violence ou au vandalisme dans leur quartier, en proportion de la population totale	Nombre de personnes confrontées à la délinquance, à la violence ou au vandalisme dans leur quartier, en proportion de la population totale	%
5	non app	Contribue à la réduction du pourcentage du territoire transformé en zones artificialisées	Zones artificialisées	% du territoire

Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
5	non app	Contribue à l'augmentation des dépenses totales de protection environnementale	Dépenses totales de protection environnementale	millions EUR
6	non app	Contribue à l'augmentation de l'utilisation des transports publics	Utilisation des transports publics	% des voyageurs
7	non app	Contribue à la fertilité des sols sans nuire à la qualité des eaux de surface et/ou les eaux souterraines, de provoquer l'eutrophisation des eaux et de dégrader les écosystèmes terrestres et/ou aquatiques (unité : kg d'azote par ha surface agricole utile surface agricole utile SAU)?	Bilan des substances nutritives d'azote	kg d'azote par ha surface agricole utile (SAU)
7	non app	Contribue à la fertilité des sols sans nuire à la qualité des eaux de surface et/ou les eaux souterraines, de provoquer l'eutrophisation des eaux et de dégrader les écosystèmes terrestres et/ou aquatiques (unité : kg de phosphore par ha surface agricole utile SAU)	Bilan des substances nutritives phosphorées	kg de phosphore par ha surface agricole utile (SAU)
7	non app	Contribue à une consommation durable d'une eau de robinet de qualité potable	Part des dépenses en eau dans le total des dépenses des ménages	%
7	non app	Contribue à l'augmentation du pourcentage des masses d'eau de surface naturelles ayant atteint un état écologique "satisfaisant" et des masses d'eau souterraine ayant atteint un bon état chimique	Pourcentage des masses d'eau de surface naturelles ayant atteint un état écologique "satisfaisant" et des masses d'eau souterraine ayant atteint un bon état chimique	%
7	non app	Contribue à l'augmentation de l'efficacité de l'usage de l'eau	Efficacité de l'usage de l'eau	m^3/millions EUR
7	non app	Contribuer à une protection des masses d'eau de surfaces et les masses d'eau souterraine par des prélèvements durables et une utilisation plus efficiente de l'eau	Indice de stress hydriques	%
7	non app	Contribue à la préservation et/ou l'augmentation de la part de zones agricoles et forestières	Part des zones agricoles et forestières	% du territoire
7	non app	Contribue à l'augmentation de la part du territoire designée comme zone protégée pour la biodiversité	Part du territoire désignée comme zone protégée pour la biodiversité	% du territoire
7	non app	Contribue à la protection des oiseaux inscrits sur la liste rouge des espèces menacées	Nombre d'espèces sur la liste rouge des oiseaux	Nb d'espèces
7	non app	Contribue à la lutte contre les espèces exotiques invasives inscrites sur la liste noire	Nombre de taxons sur la liste noire des plantes vasculaires	Nb de taxons
7	non app	Contribue à la favorabilité de l'état de conservation des habitats	État de conservation des habitats	% favorables
8	non app	Contribue à la réduction de l'intensité énergétique	Intensité énergétique	Térajoules/millions EUR
8	non app	Contribue à la réduction de la consommation finale d'énergie	Consommation finale d'énergie	GWh

Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
8	non app	Contribue à l'augmentation de la part des énergies renouvelables dans la consommation finale d'énergie	Part des énergies renouvelables dans la consommation finale d'énergie	%
8	non app	Contribue à la réduction de la part des dépenses énergétiques dans le total des dépenses des ménages	Part des dépenses énergétiques dans le total des dépenses des ménages	%
8	non app	Contribue à la réduction du total des émissions de gaz à effet de serre	Total des émissions de gaz à effet de serre	millions tonnes CO_2
8	non app	Contribue à la réduction des émissions de gaz à effet de serre hors système d'échanges de quotas d'émission (SEQE)	Émissions de gaz à effet de serre hors système d'échanges de quotas d'émission (SEQE)	millions tonnes CO_2
8	non app	Contribue à la réduction de l'intensité des émissions de gaz à effet de serre	Intensité des émissions de gaz à effet de serre	kg CO_2 / EUR
9	non app	Contribue à l'augmentation de l'aide au développement - Éducation	Aide au développement - Éducation	millions EUR
9	non app	Contribue à l'augmentation de l'aide au développement - Agriculture	Aide au développement - Agriculture	millions EUR (prix constant 2016)
9	non app	Contribue à l'augmentation de l'aide au développement - Santé de base	Aide au développement - Santé de base	millions EUR (prix constant 2016)
9	non app	Contribue à l'augmentation de la part des étudiants des pays en développement qui étudient au Luxembourg	Part des étudiants des pays en développement qui étudient au Luxembourg	%
9	non app	Contribue à l'augmentation du montant des bourses d'étude	Montant des bourses d'étude	millions EUR
9	non app	Contribue à l'augmentation de l'aide au développement - Eau et assainissement	Aide au développement - Eau et assainissement	millions EUR (prix constant 2016)
9	non app	Contribue à l'augmentation de l'aide au développement - Énergie	Aide au développement - Énergie	millions EUR (prix constant 2016)
9	non app	Contribue à l'augmentation de l'aide au développement - Lois et règlements commerciaux	Aide au développement - Lois et règlements commerciaux	millions EUR (prix constant 2016)
9	non app	Contribue à l'augmentation du montant des dépenses sociales expimé en ratio du PIB	Montant des dépenses sociales exprimé en ratio du PIB	% du PIB
9	non app	Contribue à l'augmentation de l'aide publique nette au développement, montant alloué aux pays les moins avancés (absolu)	Aide publique nette au développement, montant alloué aux pays les moins avancés	millions EUR (prix constant 2016)
9	non app	Contribue à l'augmentation de l'aide publique nette au développement, montant alloué aux pays les moins avancés (en proportion du montant total d'aide au développement)	Aide publique nette au développement, montant alloué aux pays les moins avancés, en proportion du montant total d'aide au développement	%
9	non app	Contribue à l'augmentation de l'aide au développement - Prévention et préparation aux catastrophes	Aide au développement - Prévention et préparation aux catastrophes	millions EUR (prix constant 2016)

Champ d'action	Évaluation[1]	Indicateur évaluation	Indicateur national	Unité
9	non app	Contribue à l'engagement international de 100 milliards USD pour dépenses reliées au climat	Contribution à l'engagement international de 100 milliards USD pour dépenses reliées au climat	millions EUR
9	non app	Contribue à l'augmentation de l'aide au développement avec marqueur biodiversité	Aide au développement avec marqueur biodiversité	millions EUR (prix constant 2016)
9	non app	Contribue à l'augmentation de l'aide publique nette au développement, montant total, en proportion du revenu national brut	Aide publique nette au développement, montant total, en proportion du revenu national brut	% du RNB
9	non app	Contribue à l'augmentation de l'aide au développement - Coopération technique	Aide au développement – Coopération technique	millions EUR (prix constant 2016)
9	non app	Contribue à la réduction de la dette publique en proportion du produit intérieur brut	Dette publique en proportion du produit intérieur brut	% du PIB
9	non app	Contribue à l'augmentation du montant investi dans des projets de soutien à l'enseignement supérieur	Montant investi dans des projets de soutien à l'enseignement supérieur	millions EUR (prix constant 2016)
9	non app	Contribue à l'augmentation de l'aide publique au développement - Renforcement de la société civile dans les pays partenaires	Aide publique au développement - Renforcement de la société civile dans les pays partenaires	millions EUR (prix constant 2016)
10	non app	Contribue à l'action climatique dans les pays en développement et à la protection du climat au niveau global	Contributions déterminées au niveau national (CDN) à la réduction des émissions de gaz à effet de serre	millions EUR
10	non app	Contribue à l'augmentation de l'alimentation du fonds climat énergie	Fonds climat et énergie	millions EUR
10	non app	Contribue à l'augmentation de la part des taxes environnementales dans le total des taxes nationales	Part des taxes environnementales dans le total des taxes nationales	% du revenu fiscal

Impression: CTIE – Division Imprimés et Fournitures de bureau