JUSTEL - Législation consolidée

http://www.ejustice.just.fgov.be/eli/loi/2022/07/20/2022204364/justel

Dossier numéro : 2022-07-20/11

Titre

20 JUILLET 2022. - Loi relative à la certification de cybersécurité des technologies de l'information et des communications et portant désignation d'une autorité nationale de certification de cybersécurité

Source : CHANCELLERIE DU PREMIER MINISTRE

Publication : Moniteur belge du 05-08-2022 page : 60924

Entrée en vigueur : 05-08-2022

Table des matières

Texte

CHAPITRE 1er. - Définitions et dispositions générales

Section 1re. - Objet et champ d'application

Sous-section 1re. - Objet

Article 1er. La présente loi règle une matière visée à l'article 74 de la Constitution.

Art. 2. La présente loi met en oeuvre partiellement le règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013, ci-après : le " Règlement sur la cybersécurité ".

Sous-section 2. - Champ d'application

Art. 3. § 1er. La présente loi s'applique à la certification européenne volontaire de cybersécurité des produits TIC, services TIC et processus TIC visée par le Règlement sur la cybersécurité.
§ 2. Les chapitres 1er à 4, 7 et 8, ainsi que les articles 21 et 22, s'appliquent également à une certification européenne de cybersécurité rendue obligatoire.
Lors de la mise en oeuvre des articles 21 et 22 dans le cadre de la certification visée à l'alinéa 1er, les articles 19 et 26 sont applicables.
Le Roi peut, par arrêté délibéré en Conseil des ministres, rendre applicables, en tout ou en partie, les chapitres 5 et 6 dans le cadre de la certification visée à l'alinéa 1er.
§ 3. La présente loi est sans préjudice des compétences de rendre obligatoire une certification de cybersécurité et d'en assurer le contrôle dont disposent les autorités publiques, notamment les autorités de surveillance de marché ou les autorités sectorielles visées à l'article 6, 2°, de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, de l'article 3, 3°, de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques et de l'article 2, alinéa 1er, 1°, de l'arrêté royal du 2 décembre 2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien.
Dans le respect du paragraphe 2, les autorités visées à l'alinéa 1er et les services d'inspection compétents assurent le contrôle et les sanctions des certifications européennes de cybersécurité rendues obligatoires.
§ 4. L'article 5, § § 2 à 4, n'est applicable ni à la Banque nationale de Belgique visée à la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique ni à la FSMA visée à la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers ni au SPF Economie visé au Code de droit économique.
§ 5. La présente loi ne porte pas préjudice à l'application de l'arrêté royal du 31 janvier 2006 portant création du système BELAC d'accréditation des organismes d'évaluation de la conformité.

Section 2. - Définitions

Art. 4. Pour l'application de la présente loi, on entend par:
1° " autorité nationale de certification de cybersécurité " : l'autorité visée à l'article 58 du Règlement sur la cybersécurité et désignée par le Roi conformément à l'article 5, § 1er;
2° " GECC " : le Groupe européen de certification de cybersécurité visé à l'article 62 du Règlement sur la cybersécurité;
3° " autorité nationale d'accréditation " : l'organisme national d'accréditation unique créé par le Roi en exécution de l'article VIII.30 du Code de droit économique et visé à l'article 2, 16), du Règlement sur la cybersécurité;
4° " autorité publique " : l'autorité publique au sens de l'article 5 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel;
5° " service d'inspection " : le service d'inspection visé à l'article 13, § 1er.

CHAPITRE 2. - Autorités compétentes et coopération au niveau national

Section 1re. - Autorités compétentes

Art. 5. § 1er. Le Roi désigne l'autorité qui est chargée, en tant qu'autorité nationale de certification de cybersécurité, des tâches et missions visées par le Règlement sur la cybersécurité et par la présente loi.

§ 2. En fonction de l'objet du schéma de certification concerné et à la demande de l'autorité publique concernée, le Roi peut, par dérogation, confier, par arrêté délibéré en Conseil des ministres, en tout ou en partie, les missions visées aux chapitres 5 et 6 de l'autorité visée au paragraphe 1er à une autre autorité publique, à l'exception des missions visées aux articles 21 et 22.

Le Roi veille à tenir compte de l'expertise de l'autorité publique concernée lors de l'attribution éventuelle de tâches de contrôle.

§ 3. Dans l'hypothèse visée au paragraphe 2, le Roi sollicite l'avis et se concerte au préalable avec l'autorité visée au paragraphe 1er et l'autorité publique concernée.

§ 4. Dans l'exercice de ces missions confiées par le Roi et sans préjudice de ses compétences légales en matière de contrôle et de sanctions, l'autorité publique concernée dispose des mêmes droits et obligations que ceux visés aux chapitres 5 et 6.

Section 2. - Coopération au niveau national

Art. 6. § 1er. L'autorité visée à l'article 5, § 1er, et l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6 accomplissent leurs tâches en concertation avec les autorités publiques, notamment avec l'autorité nationale d'accréditation. En fonction de l'objet précis du schéma de certification, l'autorité visée à l'article 5, § 1er, et l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6 peuvent également consulter les acteurs privés concernés par la certification en matière de cybersécurité.

§ 2. Conformément à l'article 58, paragraphe 7, h), du Règlement sur la cybersécurité, l'autorité visée à l'article 5, § 1er, et l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6, d'une part, les autorités sectorielles et les services d'inspection, visés respectivement aux articles 3, 3°, et 24, § 2, de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques ou à l'article 7, § § 3 et 5, de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, l'Institut belge des services postaux et des télécommunications et l'autorité nationale d'accréditation, d'autre part, s'échangent les informations nécessaires à l'application du Règlement sur la cybersécurité, de la présente loi ou des articles 107/2 à 107/5 de la loi du 13 juin 2005 relative aux communications électroniques, notamment en matière de délivrance de certificats, de contrôle, de sanctions et de réclamations. Lorsqu'un échange d'informations porte sur des données à caractère personnel, cet échange est effectué conformément aux dispositions du chapitre 8. Les modalités d'échange d'informations préservent la confidentialité des informations concernées.

§ 3. L'autorité visée à l'article 5, § 1er, et l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6 communiquent aux destinataires, à savoir une autorité sectorielle, un service d'inspection, l'inspection aéroportuaire, l'inspection aéronautique ou la Belgian Supervising Authority for Air Navigation Services visés respectivement aux articles 3, 3°, et 24, § 2, de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, à l'article 7, § § 3 et 5, de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique ou aux articles 2, alinéa 1er, 1° et 9°, et 15, §§ 1er à 3, de l'arrêté royal du 2 décembre 2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien, toute information obtenue dans le cadre de l'exécution du Règlement sur la cybersécurité, de la présente loi ou d'un schéma européen de certification de cybersécurité lorsque cette information porte sur un manquement à l'article 13 de la loi précitée du 1er juillet 2011, aux articles 20, 21, § 1er, et 33, de la loi précitée du 7 avril 2019, à l'article 11 de l'arrêté royal précité du 2 décembre 2011 ou aux sections 1.7 et 11.2.8 du règlement d'exécution (UE) 2015/1998 de la Commission du 5 novembre 2015 fixant des mesures détaillées pour la mise en oeuvre des normes de base communes dans le domaine de la sûreté de l'aviation civile, et que l'entité concernée par l'information se trouve sous la surveillance desdits destinataires.

§ 4. Dans le cadre de la coopération prévue aux paragraphes 2 et 3, les autorités publiques dépositaires, par état, des secrets ou informations confidentielles qu'on leur confie sont autorisées à faire connaître ces secrets ou ces informations confidentielles à l'autorité visée à l'article 5, § 1er, ou à l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6 lorsque cela est nécessaire à l'application du Règlement sur la cybersécurité ou de la présente loi.

Seules les informations nécessaires en matière de contrôle, de sanctions et de réclamations peuvent être communiquées. Lorsque ces informations portent sur des données à caractère personnel, le chapitre 8 est d'application. Les modalités d'échange d'informations préservent la confidentialité des informations concernées.

Art. 7. Dans le cadre des missions et pouvoirs qui leur sont attribués par la loi, les autorités publiques peuvent assister l'autorité visée à l'article 5, § 1er, ou l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6, dans ses missions de contrôle visées par la présente loi.

CHAPITRE 3. - Autorité nationale de certification de cybersécurité

Section 1re. - Représentation au Groupe européen de certification de cybersécurité

Art. 8. § 1er. L'autorité visée à l'article 5, § 1er, représente la Belgique au sein du GECC.
§ 2. Dans le cadre de sa mission de représentation de la Belgique au sein du GECC, l'autorité visée à l'article 5, § 1er, se concerte avec les autres autorités publiques désignées par le Roi, en particulier en ce qui concerne la préparation et l'adoption d'un avis sur un schéma de certification candidat au sens de l'article 49 du Règlement sur la cybersécurité.
§ 3. D'autres autorités publiques peuvent assister avec l'autorité visée à l'article 5, § 1er, aux travaux et réunions du GECC.

Section 2. - Indépendance

Art. 9. § 1er. L'autorité visée à l'article 5, § 1er, prend les mesures nécessaires afin d'assurer l'indépendance des membres de son personnel, de prévenir, d'identifier et de résoudre efficacement les conflits d'intérêts lors de l'exécution de ses tâches de contrôle ou de certification en matière de cybersécurité, afin d'éviter des distorsions de concurrence et de garantir l'égalité de traitement de tous.
La notion de conflit d'intérêts vise au moins les situations dans lesquelles un membre du personnel de l'autorité visée à l'article 5, § 1er, chargé de la certification ou du contrôle a, directement ou indirectement, un intérêt financier, économique ou un autre intérêt personnel qui pourrait être perçu comme compromettant son impartialité et son indépendance dans le cadre de sa mission ou de ses fonctions.
§ 2. Les membres du personnel de l'autorité visée à l'article 5, § 1er, ne reçoivent ni ne cherchent dans les limites de leurs attributions, de façon directe ou indirecte, d'instructions de personne.
Il leur est interdit d'être présents lors d'une délibération ou décision sur les dossiers pour lesquels ils ont un intérêt personnel ou direct ou pour lesquels leurs parents ou alliés jusqu'au troisième degré ont un intérêt personnel ou direct.
Le Roi peut également désigner d'autres situations comme étant des conflits d'intérêts.

CHAPITRE 4. - Délivrance des certificats européens

Section 1re. - Certificats de cybersécurité européens attestant d'un niveau d'assurance " élémentaire " ou " substantiel "

Art. 10. § 1er. Conformément à l'article 56, paragraphe 4, du Règlement sur la cybersécurité, les organismes d'évaluation de la conformité accrédités par l'autorité nationale d'accréditation délivrent les certificats de cybersécurité européens attestant d'un niveau d'assurance dit " élémentaire " ou " substantiel ".
§ 2. Conformément à l'article 56, paragraphe 5, a), du Règlement sur la cybersécurité, lorsque le schéma européen de certification de cybersécurité l'impose, la délivrance des certificats visés au paragraphe 1er est réservée à l'autorité visée à l'article 5, § 1er.
§ 3. Conformément à l'article 56, paragraphe 5, b), du Règlement sur la cybersécurité, en fonction des exigences techniques du schéma de certification et moyennant une délégation préalable, l'autorité visée à l'article 5, § 1er, peut déléguer en tout ou en partie la délivrance d'un certificat visé au paragraphe 2 à un organisme public accrédité par l'autorité nationale d'accréditation en tant qu'organisme d'évaluation de la conformité.

Section 2. - Certificats de cybersécurité européens attestant d'un niveau d'assurance " élevé "

Art. 11. § 1er. Conformément à l'article 56, paragraphe 6, du Règlement sur la cybersécurité, l'autorité visée à l'article 5, § 1er, délivre les certificats de cybersécurité européens attestant d'un niveau d'assurance dit " élevé ".
§ 2. Conformément à l'article 56, paragraphe 6, b), du Règlement sur la cybersécurité, en fonction des exigences techniques du schéma de certification et moyennant une délégation préalable, l'autorité visée à l'article 5, § 1er, peut toutefois déléguer en tout ou en partie cette tâche à un organisme d'évaluation de la conformité accrédité par l'autorité nationale d'accréditation.

Section 3. - Réclamation en cas de refus de délivrance

Art. 12. Conformément à l'article 63, paragraphe 1er, du Règlement sur la cybersécurité, en cas de refus de délivrance d'un certificat de cybersécurité européen par l'autorité visée à l'article 5, § 1er, ou par un organisme d'évaluation de la conformité dans le cadre de la délégation prévue à l'article 10, § 3, ou à l'article 11, § 2, le demandeur peut introduire une réclamation devant l'autorité visée à l'article 5, § 1er, selon les modalités prévues au chapitre 7.

CHAPITRE 5. - Contrôle

Art. 13. § 1er. Conformément à l'article 58, paragraphes 7 et 8, du Règlement sur la cybersécurité, l'autorité visée à l'article 5, § 1er, et l'autorité publique désignée par le Roi pour accomplir certaines missions visées aux chapitres 5 et 6 disposent chacune d'un service d'inspection qui peut à tout moment réaliser des contrôles du respect par les organismes d'évaluation de la conformité, les titulaires de certificats de cybersécurité européens volontaires et les émetteurs de déclarations de conformité de l'Union européenne des règles imposées par le règlement sur la cybersécurité, les schémas européens de certification de cybersécurité, la présente loi ou ses