Annexe I : tableau des finalités

Bases juridiques du traitement	Finalités des traitements	Données d'identification, de contact et relatives à la situation familiale	Données de navigation et de communication électroniques (autres que le contenu des communications)	Données recueillies dans le cadre de la vidéosurveillance de lieux fermés non accessibles au public	Données relatives aux sanctions administratives ou pénales
Respect d'une obligation légale	Assurer la coordination entre les différents services et autorités concernés par la cybersécurité en Belgique	✓	×	×	×
	Superviser, coordonner et veiller à la mise en œuvre de la stratégie belge en matière de cybersécurité	✓	×	×	×
	Superviser la mise en œuvre de la loi NIS2	✓	✓	✓	✓
	Assurer la coordination entre les autorités publiques et le secteur privé ou le monde scientifique	✓	×	×	×
	Elaborer, diffuser et veiller à la mise en œuvre des standards, directives et normes pour la cybersécurité des différents types de systèmes d'information	✓	×	×	×
	Assurer la gestion de crise en cas de cyberincidents, en coopération avec le Centre de coordination et de crise du gouvernement	✓	✓	✓	×
	Coordonner la représentation belge aux forums internationaux sur la cybersécurité, le suivi des obligations internationales et la présentation du point de vue national en la matière	✓	×	×	×

	Coordonner l'évaluation et la certification de la sécurité des systèmes d'information et de communication	✓	✓	×	×
	Informer et sensibiliser les utilisateurs des systèmes d'information et de communication	✓	✓	×	×
	Accorder des subventions pour des projets et activités relatifs à la cybersécurité	✓	×	×	✓*
	Faciliter et encourager l'organisation de formations en matière de cybersécurité pour les membres du personnel des entités NIS2	✓	×	×	×
	Surveiller et analyser les cybermenaces, les vulnérabilités et les incidents au niveau national et, sur demande, apporter une assistance aux entités essentielles et importantes concernées pour surveiller en temps réel ou quasi réel leurs réseaux et systèmes d'information	✓	✓	×	×
	Activer le mécanisme d'alerte précoce, la diffusion de messages d'alerte, les annonces et la diffusion d'informations sur les cybermenaces, les vulnérabilités et les incidents auprès des entités NIS2 ainsi qu'auprès des autorités compétentes et des autres parties prenantes concernées, si possible en temps quasi réel	✓	✓	×	×
	Réagir aux incidents et apporter une assistance aux entités NIS2	✓	✓	✓*	×
	Rassembler et analyser des données forensiques, et assurer une analyse dynamique des risques et incidents et une appréciation de la situation en matière de cybersécurité	✓	✓	×	×
	Réaliser, à la demande d'une entité essentielle ou importante, un scan proactif des réseaux et des systèmes d'information de l'entité concernée afin de détecter les vulnérabilités susceptibles d'avoir un impact important	✓	✓	×	×
	Participer au réseau des CSIRT, coopérer de manière effective, efficace et sécurisée au sein de ce réseau et apporter une assistance mutuelle en fonction de ses capacités et de ses compétences aux autres membres du réseau des CSIRT à leur demande	✓	✓	×	×

	Agir en qualité de coordinateur aux fins du processus de divulgation coordonnée des vulnérabilités	✓	✓	×	×
	Contribuer au déploiement d'outils sécurisés de partage d'informations	✓	✓	×	×
	Procéder à un scan proactif et non intrusif des réseaux et systèmes d'information accessibles au public lorsque ce scan est effectué dans le but de détecter les réseaux et systèmes d'information vulnérables ou configurés de façon peu sûre et d'informer les entités concernées	✓	✓	×	×
	Détecter, observer et analyser des problèmes de sécurité informatique	✓	✓	×	×
	Etablir et faciliter des relations de coopération avec les acteurs concernés	✓	×	×	×
	Participer aux évaluations par les pairs organisées dans le cadre de la directive NIS2	✓	×	×	×
	Amélioration de la cybersécurité à travers la recherche d'un niveau accru de protection des réseaux et systèmes d'information, le renforcement des politiques de prévention et de sécurité, la prévention des incidents de sécurité et la défense contre les cybermenaces;	✓	✓	×	×
	Coopération, notamment l'échange d'informations entre le CCB et d'autres autorités, notamment les autorités sectorielles, le NCCN et les autorités compétentes dans le cadre de la loi du 1er juillet 2011 relative à la sécurité	✓	×	×	×

	et la protection des infrastructures critiques, dans le cadre de l'exécution de la loi NIS2 et la loi du 1er juillet 2011 précitée				
	Coopération entre les entités essentielles et importantes et les autorités compétentes dans le cadre de la loi NIS2	✓	✓*	×	×
	Partage d'informations entre les autorités visées par la loi NIS2	✓	✓*	×	×
	Assurer la continuité des services prestés par les entités importantes ou essentielles	✓	×	×	×
	Notification d'incidents et d'incidents évités	✓	✓	×	×
	Contrôle et la supervision des entités essentielles et importantes, ainsi que la préparation, l'organisation, la gestion et le suivi de mesures et d'amendes administratives	✓	✓	✓	✓
	Prévention, recherche et détection des infractions commises en ligne ou par le biais d'un réseau ou service de communications électroniques, en ce compris des faits qui relèvent de la criminalité grave (sans finalité à caractère pénal)	✓	✓	×	×
	Prévention de menaces graves contre la sécurité publique (sans finalité à caractère pénal)	✓	✓	×	×

	Examen de défaillances de la sécurité des réseaux ou de services de communications électroniques ou des systèmes d'information	✓	✓	×	×
	Dissémination d'informations relatives à un incident significatif à d'autres Etats Membres et, le cas échéant, au public en général	✓	✓	×	×
	Délivrer des certificats de cybersécurité européens et gérer des réclamations	✓	✓	×	✓*
	Contrôler les titulaires de certificats de cybersécurité européens, les émetteurs de déclarations de conformité de l'Union européenne et les organismes d'évaluation de la conformité	✓	✓	×	✓
	Imposer des sanctions dans le cadre du règlement (UE) 2019/881 et de la loi CSA	✓	×	×	✓
	Participer au Groupe européen de certification de cybersécurité	✓	×	×	×
	Coopérer avec d'autres autorités	✓	✓	×	✓
	Assurer le rôle de centre de coordination national au sens de l'article 6 du règlement européen (UE) 2021/887	✓	×	×	×
	Faire office de point de contact au niveau national dans le cadre du règlement (UE) 2021/887	✓	×	×	×

	Fournir une expertise et contribuer activement aux tâches stratégiques énoncées par le règlement (UE) 2021/887	✓	×	×	×
	Promouvoir, encourager et favoriser la participation de la société civile, de l'industrie, en particulier des start-up et des PME, des milieux académiques et de la recherche ainsi que d'autres parties prenantes au niveau national à des projets transfrontières et à des actions en matière de cybersécurité financés par des programmes de l'Union pertinents	✓	×	×	×
	Fournir une assistance technique aux parties prenantes en les aidant dans leur phase de candidature pour les projets gérés par le Centre de compétences en rapport avec sa mission et ses objectifs	✓	×	×	×
	S'efforcer de créer des synergies avec les activités pertinentes au niveau national, régional et local, telles que les politiques nationales en matière de recherche, de développement et d'innovation dans le domaine de la cybersécurité, en particulier les politiques énoncées dans les stratégies nationales de cybersécurité	✓	×	×	×
	Mettre en œuvre des actions spécifiques pour lesquelles des subventions ont été accordées par le Centre de compétences	✓	×	×	×
	Nouer un dialogue avec les autorités nationales en ce qui concerne d'éventuelles contributions à la promotion et à la diffusion de programmes éducatifs en matière de cybersécurité	✓	×	×	×
	Promouvoir et diffuser les résultats pertinents des travaux du Réseau, de la communauté et du Centre de compétences au niveau national, régional ou local	✓	×	×	×
	Evaluer les demandes présentées par des entités établies en Belgique en vue de faire partie de la communauté	✓	×	×	×
	Prôner et faciliter la participation des entités concernées aux activités résultant du Centre de compétences, du Réseau et de la communauté, et assurer un suivi, le cas échéant, du niveau de participation à la recherche, au développement et au déploiement en matière de cybersécurité et du montant du soutien financier public qui y est accordé	✓	×	×	×

Mission d'intérêt public	Informer la personne concernée et répondre à ses questions	✓	✓	×	×
	Accueil des visiteurs et surveillance des bâtiments du CCB	✓	✓	✓	×
Exécution d'un contrat ou consentement	Participation à un événement (physique ou en ligne)	✓	×	×	×
	~~Accueil des visiteurs~~ Invitation à des événements (physique ou en ligne) ou newsletters	✓	×	×	×
	Pour répondre à vos questions, vous assister ou vous contacter	✓	✓~~*~~	×	×
	Gestion des marchés publics, des contrats	✓	✓~~*~~	×	✓~~*~~
	Inscription sur un des sites internet du CCB ou à un des services du CCB	✓	✓	×	×
	Administration du personnel (statutaire, contractuel, e-gov, stagiaire, etc.)	✓	✓	×	✓~~*~~
	Traitement à des fins statistiques et qualitatives, en vue d'améliorer nos services, nos sites internet et le portail (moteur de recherche utilisé ; mots-clés utilisés ; site par lequel vous êtes arrivé ; pages consultées; durée de consultation par page ; liste des fichiers téléchargés ; date et heure d'accès; navigateur utilisé ; plate-forme et/ou système d'exploitation installés sur votre ordinateur)	✓~~✓~~	✓	×	×

Intérêt légitime du CCB	Gérer les sites internet du CCB	×	✓	×	×
	Traitement en vue de personnaliser l'expérience utilisateur (notamment répondre dans la langue de la personne concernée)	×	✓	×	×
	Analyse du trafic sur les sites du CCB	×	✓ Fichiers logs relatifs au trafic	×	×
	Lutter contre les sites malveillants/ d'hameçonnage (*phishing*) et conserver des preuves en cas de procédures judiciaires	✓	✓	×✓	×✓