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	Superviser, coordonner et veiller à la mise en œuvre de la stratégie belge en matière de cybersécurité	✓	×	×	×
	Gérer par une approche intégrée et centralisée les différents projets relatifs à la cybersécurité	✓	×	×	×
	Assurer la coordination entre les services et autorités concernés mais aussi entre autorités publiques et le secteur privé ou le monde scientifique	✓	×	×	×
	Formuler des propositions pour l'adaptation du cadre légal et réglementaire en matière de cybersécurité	✓	×	×	×
	Assurer la gestion de crise en cas de cyberincidents, en	✓	✓	✓	×

	coopération avec le Centre de coordination et de crise du gouvernement				
	Elaborer, diffuser et veiller à la mise en œuvre des standards, directives et normes de sécurité pour les différents types de système informatique des administrations et organismes publics	✓	×	×	×
	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	✓	×	×	×
	Assurer le rôle de centre de coordination national au sens de l'article 6 du règlement européen (UE) 2021/887	✓	×	×	×
	Suivre les incidents au niveau national et international, en ce compris le traitement de données à caractère personnel	✓	✓	×	×

	lié au suivi de ces incidents				
	Activer le mécanisme d'alerte précoce, la diffusion de messages d'alerte, les annonces et la diffusion d'informations sur les risques et incidents auprès des parties intéressées	✓	✓	×	×
	Intervenir en cas d'incident	✓	✓	×	×
	Effectuer une analyse dynamique des risques et incidents et conscience situationnelle	✓	✓	×	×
	Détecter, observer et analyser des problèmes de sécurité informatique	✓	✓	×	×
	Promouvoir l'adoption et l'utilisation de pratiques communes ou normalisées pour les procédures de gestion des risques et incidents, ainsi que des systèmes de classification des incidents, risques et informations	✓	×	×	×
	Etablir des relations de coopération avec le secteur privé, d'autres services administratifs ou autorités publiques	✓	×	×	×
	Participer au réseau des CSIRT visé à l'article 12 de la directive NIS	✓	×	×	×

	Signaler une infraction pénale et communiquer au ministère public toute information y afférente	✓	✓	✓	✓
	Signaler une vulnérabilité de réseaux et systèmes d'information	✓	✓	×	×
	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	✓	✓	×	×
	Faire office de point de contact au niveau national dans le cadre du règlement précité	✓	×	×	×
	Fournir une expertise et contribuer activement aux tâches stratégiques énoncées par le règlement précité	✓	×	×	×

	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	✓	✓	×	×
Exécution d'un contrat ou consentement	Participation à un événement	✓	×	×	×
	Accueil des visiteurs	✓	×	×	×
	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.)	✓	✓	×	×
	Formulaire électronique	✓	✓	×	×
	Informer la personne concernée et répondre à ses questions	✓	✓	×	×
	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	✓	✓	✓	✓