Bijlage I: tabel met de doeleinden

Juridische basis van de verwerking	Doeleinden van de verwerkingen	Identificatie-gegevens, contactgege-vens en gegevens over de gezinssituatie	Navigatie-gegevens en elektronische -communicatie gegevens (die geen betrekking hebben op de inhoud van de communicatie)	Gegevens verzameld in het kader van videobewaking van besloten, niet voor het publiek toegankelijke plaatsen	Gegevens betreffende administra-tieve of strafrechte-lijke sancties
Naleven van een wettelijke verplichting	Zorgen voor coördinatie tussen de verschillende diensten en autoriteiten die betrokken zijn bij cyberbeveiliging in België;	✓	×	×	×
	Opvolgen en coördineren van en toezien op de uitvoering van de Belgische strategie inzake cyberbeveiliging	✓	×	×	×
	Toezien op de uitvoering van de NIS2-wet	✓	✓	✓	✓
	Zorgen voor coördinatie tussen de overheden en de private sector of de wetenschappelijke wereld	✓	×	×	×
	Het opstellen, verspreiden en toezien op de uitvoering van standaarden, richtlijnen en normen voor cyberbeveiliging van de verschillende soorten informatiesystemen	✓	×	×	×
	In samenwerking met het Coördinatie- en Crisiscentrum van de regering, het crisisbeheer bij cyberincidenten verzekeren	✓	✓	✓	×

	Het coördineren van de Belgische vertegenwoordiging in internationale fora voor cyberbeveiliging, van opvolging van internationale verplichtingen en van voorstellen van het nationale standpunt op dit vlak	✓	×	×	×
	Coördineren van de evaluatie en certificering van de beveiliging van informatie- en communicatiesystemen	✓	✓	×	×
	Informeren en sensibiliseren van gebruikers van informatie- en communicatiesystemen	✓	✓	×	×
	Het toekennen van subsidies voor projecten en activiteiten rond cyberbeveiliging	✓	×	×	✓
	Het faciliteren en aanmoedigen van de organisatie van opleidingen rond cyberbeveiliging voor personeelsleden van NIS2-entiteiten	✓	×	×	×
	Monitoren en analyseren van cyberdreigingen, kwetsbaarheden en incidenten op nationaal niveau en, op verzoek, het verlenen van bijstand aan de betrokken essentiële en belangrijke entiteiten met betrekking tot het realtime of bijna-realtime monitoren van hun netwerk- en informatiesystemen	✓	✓	×	×
	Verstrekken van vroegtijdige waarschuwingen, meldingen en aankondigingen en het verspreiden van informatie onder de NIS2-entiteiten en aan de bevoegde autoriteiten en andere relevante belanghebbenden over cyberdreigingen, kwetsbaarheden en incidenten, in bijna-realtime indien mogelijk	✓	✓	×	×
	Reageren op incidenten en verlenen van bijstand aan de NIS2- entiteiten	✓	✓	✓	×
	Verzamelen en analyseren van forensische gegevens en het zorgen voor dynamische risico- en incidentenanalyse en situationeel bewustzijn met betrekking tot cyberbeveiliging;	✓	✓	×	×

	Op verzoek van een essentiële of belangrijke entiteit: het proactief scannen van de netwerk- en informatiesystemen van de betrokken entiteit om kwetsbaarheden met mogelijk significante gevolgen op te sporen	✓	✓	×	×
	Het deelnemen aan het CSIRT-netwerk, het doeltreffend, efficiënt en veilig samenwerken in dit netwerk en, in overeenstemming met zijn capaciteiten en bevoegdheden, het verlenen van wederzijdse bijstand aan andere leden van dit netwerk op hun verzoek;	✓	✓	×	×
	Optreden als coördinator ten behoeve van het proces van gecoördineerde bekendmaking van kwetsbaarheden;	✓	✓	×	×
	Bijdragen aan de uitrol van veilige instrumenten voor het delen van informatie	✓	✓	×	×
	Het proactief en niet-intrusief scannen van openbaar toegankelijke netwerk- en informatiesystemen als deze scan wordt uitgevoerd om kwetsbare of onveilig geconfigureerde netwerk- en informatiesystemen op te sporen en de betrokken entiteiten te informeren	✓	✓	×	×
	Opsporen, observeren en analyseren van computerbeveiligingsproblemen	✓	✓	×	×
	Het tot stand brengen van samenwerkingsrelaties met relevante belanghebbenden;	✓	×	×	×
	Deelnemen aan collegiale toetsingen georganiseerd in het kader van de NIS2-richtlijn	✓	×	×	×

	Het verbeteren van de cyberbeveiliging dankzij een betere bescherming van de netwerk- en informatiesystemen, een krachtiger preventie- en veiligheidsbeleid, de preventie van beveiligingsincidenten en de bescherming tegen cyberdreigingen;	✓	✓	×	×
	De samenwerking, met name de informatie-uitwisseling tussen het CCB en andere autoriteiten, met name de sectorale overheden, het NCCN en de autoriteiten die bevoegd zijn in het kader van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van kritieke infrastructuren, in het kader van de uitvoering van de NIS2-wet en voornoemde wet van 1 juli 2011	✓	×	×	×
	De samenwerking tussen essentiële en belangrijke entiteiten en de bevoegde autoriteiten in het kader van de NIS2-wet	✓	✓	×	×
	De informatie-uitwisseling tussen de autoriteiten die onder de NIS2-wet vallen	✓	✓	×	×
	Het verzekeren van de continuïteit van de dienstverlening door belangrijke of essentiële entiteiten	✓	×	×	×
	Het melden van incidenten en bijna-incidenten	✓	✓	×	×
	De controle van en het toezicht op essentiële en belangrijke entiteiten, alsook de voorbereiding, de organisatie, het beheer en de opvolging van administratieve maatregelen en geldboetes	✓	✓	✓	✓

	Zonder strafrechtelijke finaliteit, het voorkomen, onderzoeken en opsporen van inbreuken die online of via een elektronische-communicatienetwerk of -dienst worden gepleegd, met inbegrip van zware criminele feiten (niet voor strafrechtelijke doeleinden)	✓	✓	×	×
	Het voorkomen van ernstige bedreigingen voor de openbare veiligheid (niet voor strafrechtelijke doeleinden)	✓	✓	×	×
	Het onderzoeken van beveiligingsproblemen bij elektronische-communicatienetwerken of -diensten of informatiesystemen	✓	✓	×	×
	Het verspreiden van informatie over een significant incident onder andere lidstaten en, waar nodig, het brede publiek.	✓	✓	×	×
	Europese cyberbeveiligings-certificaten afgeven en klachten beheren	✓	✓	×	✓
	Toezicht uitoefenen op houders van Europese cyberbeveiligings-certificaten, afgevers van EU-conformiteitsver-klaringen en conformiteitsbe-oordelingsinstan¬ties	✓	✓	×	✓
	Sancties opleggen in het kader van verordening (EU) 2019/881 en de CSA-wet	✓	×	×	✓
	Deelnemen aan de Europese Groep voor cyberbeveiligings-certificering	✓	×	×	×

	Samenwerken met andere overheden	✓	✓	×	✓
	Optreden als nationaal coördinatiecentrum in de zin van artikel 6 van verordening (EU) 2021/887	✓	×	×	×
	Optreden als contactpunt op nationaal niveau in het kader van verordening (EU) 2021/887	✓	×	×	×
	Verstrekken van deskundig advies en actief bijdragen aan de strategische taken als bedoeld in verordening (EU) 2021/887	✓	×	×	×
	Bevorderen, stimuleren en vergemakkelijken op nationaal niveau van de deelname van het maatschappelijk middenveld, de industrie, met name starters en kmo's, de academische en onderzoeksgemeenschap en andere stakeholders aan grensoverschrijdende projecten en aan acties op het gebied van cyberbeveiliging die uit de betreffende Unieprogramma's gefinancierd worden	✓	×	×	×
	Verlenen van technische bijstand aan stakeholders door hen te ondersteunen in de aanvraagfase voor door het kenniscentrum beheerde projecten met betrekking tot zijn opdracht en doelstellingen	✓	×	×	×
	Streven naar synergieën met relevante activiteiten op nationaal, regionaal en lokaal niveau, zoals nationaal beleid inzake onderzoek, ontwikkeling en innovatie op het gebied van cyberbeveiliging, met name het beleid dat in de nationale cyberbeveiligingsstrategieën is uiteengezet	✓	×	×	×
	Uitvoeren van specifieke acties waaraan het kenniscentrum subsidies heeft toegekend	✓	×	×	×
	Overleggen met de nationale autoriteiten over mogelijke bijdragen aan de bevordering en verspreiding van onderwijsprogramma's op het gebied van cyberbeveiliging	✓	×	×	×
	Bevorderen en verspreiden van de betreffende resultaten van de werkzaamheden van het netwerk, de kennisgemeenschap en het kenniscentrum op nationaal, regionaal of lokaal niveau	✓	×	×	×

	Beoordelen van verzoeken van in België gevestigde entiteiten om deel uit te maken van de kennisgemeenschap	✓	×	×	×
	Pleiten voor en bevorderen van de betrokkenheid van relevante entiteiten bij de activiteiten van het kenniscentrum, het netwerk en de kennisgemeenschap en, indien nodig, toezicht houden op de mate van betrokkenheid bij en het bedrag aan publieke financiële steun voor onderzoek, ontwikkeling en uitrol op het gebied van cyberbeveiliging	✓	×	×	×
Taak van openbaar belang	De betrokkene informeren en antwoorden op zijn/haar vragen	✓	✓	×	×
	Ontvangst van bezoekers en toezicht op de gebouwen van het CCB	✓	✓	✓	×
Uitvoering van een overeenkomst of toestemming	Deelname aan een evenement (fysiek of online)	✓	×	×	×
	Uitnodigingen voor evenementen (fysiek of online) of nieuwsbrieven	✓	×	×	×
	Om op uw vragen te antwoorden, u te helpen of u te contacteren	✓	✓	×	×
	Beheer van overheidsopdrachten, van overeenkomsten	✓	✓	×	✓
	Registratie op een van de websites of inschrijving voor een van de diensten van het CCB	✓	✓	×	×
	Personeelsadministratie (statutair, contractueel, e-gov, stagiair, enz.)	✓	✓	×	✓

	Verwerking voor statistische en kwalitatieve doeleinden, om onze diensten, onze websites en de portaalsite te verbeteren (gebruikte zoekmachine; gebruikte trefwoorden; de website waarlangs u gekomen bent; geraadpleegde pagina's; raadplegingsduur per pagina; lijst van gedownloade bestanden; datum en tijdstip van toegang; gebruikte browser; platform en/of besturingssysteem dat op uw computer is geïnstalleerd)	✓	✓	×	×
Legitiem belang van het CCB	De websites van het CCB beheren	×	✓	×	×
	Verwerking om de gebruikerservaring te personaliseren (met name antwoorden in de taal van de betrokkene)	×	✓	×	×
	Analyse van het verkeer op de websites van het CCB	×	✓ Logbestanden betreffende het webverkeer	×	×
	Malafide/*phishing* websites bestrijden en bewijzen bewaren in geval van gerechtelijke procedures	✓	✓	×	×