Anhang I: Tabelle der Zwecke

Rechtsgrundlage für die Verarbeitung	Zwecke der Verarbeitung	Angaben zu Identität, Kontakt und Familie	Browsing- und elektronische Kommunikationsdaten (mit Ausnahme von Kommunikationsinhalten)	Daten, die im Rahmen der Videoüberwachung von geschlossenen, der Öffentlichkeit nicht zugänglichen Räumen erhoben werden	Daten im Zusammenhang mit verwaltungs- oder strafrechtlichen Sanktionen
Erfüllung einer rechtlichen Verpflichtung	Gewährleistung der Koordination zwischen den verschiedenen Abteilungen und Behörden, die in Belgien mit Cybersicherheit zu tun haben	✓	×	×	×
	Überwachung, Koordinierung und Gewährleistung der Implementierung der belgischen Cybersicherheitsstrategie	✓	×	×	×
	Beaufsichtigung der Implementierung des NIS2-Gesetzes	✓	✓	✓	✓
	Gewährleistung der Koordinierung zwischen den Behörden und dem Privatsektor oder der Wissenschaft	✓	×	×	×
	Ausarbeitung, Verbreitung und Gewährleistung der Implementierung von Standards, Richtlinien und Normen für die Cybersicherheit der verschiedenen Arten von Informationssystemen unter	✓	×	×	×

	Gewährleistung des Krisenmanagements bei Sicherheitsvorfällen im Internet in Zusammenarbeit mit dem Krisen- und Koordinierungszentrum der Regierung	✓	✓	✓	×
	Koordinierung der belgischen Vertretung in internationalen Foren für Cybersicherheit, Überwachung der internationalen Verpflichtungen und Darstellung des nationalen Standpunkts in diesem Bereich	✓	×	×	×
	Koordinierung der Bewertung und Zertifizierung der Sicherheit von Informations- und Kommunikationssystemen	✓	✓	×	×
	Information und Sensibilisierung der Nutzer von Informations- und Kommunikationssystemen	✓	✓	×	×
	Gewährung von Zuschüssen für Cybersicherheitsprojekte und -aktivitäten	✓	×	×	✓
	Erleichterung und Förderung der Organisation von Schulungskursen zur Cybersicherheit für das Personal der NIS2-Einrichtungen.	✓	×	×	×
	Überwachung und Analyse von Cyberbedrohungen, Schwachstellen und Sicherheitsvorfällen auf nationaler Ebene und, auf Anfrage, Unterstützung der wesentlichen und wichtigen Einrichtungen bei der Überwachung ihrer Netzwerke und Informationssysteme in Echtzeit oder nahezu in Echtzeit.	✓	✓	×	×
	Aktivierung des Frühwarnmechanismus, Verbreitung von Warnmeldungen, Ankündigungen und Weitergabe von Informationen über Cyberbedrohungen, Schwachstellen und Sicherheitsvorfälle an die NIS2-Einrichtungen sowie an die zuständigen Behörden und andere relevante Akteure, möglichst in Echtzeit.	✓	✓	×	×
	Reaktion auf Sicherheitsvorfälle und Unterstützung der NIS2-Einrichtungen	✓	✓	✓	×

	Sammlung und Analyse forensischer Daten, dynamische Analyse von Risiken und Sicherheitsvorfällen sowie Bewertung der Cybersicherheitslage	✓	✓	×	×
	Durchführung einer proaktiven Überprüfung der Netzwerke und Informationssysteme der betreffenden Einrichtung auf Ersuchen einer wesentlichen und wichtigen Einrichtung, um Schwachstellen zu entdecken, die erhebliche Auswirkungen haben können	✓	✓	×	×
	Teilnahme am CSIRT-Netzwerk, wirksame, effiziente und sichere Zusammenarbeit innerhalb dieses Netzwerks und gegenseitige Unterstützung anderer Mitglieder des CSIRT-Netzwerks auf deren Ersuchen nach Maßgabe ihrer Kapazitäten und Fähigkeiten.	✓	✓	×	×
	als Koordinator für die koordinierte Offenlegung von Schwachstellen zu fungieren	✓	✓	×	×
	Beitrag zur Einführung von sicheren Instrumenten für den Informationsaustausch	✓	✓	×	×
	Proaktives, nicht-intrusives Scannen von öffentlich zugänglichen Netzwerken und Informationssystemen mit dem Ziel, verwundbare oder unsicher konfigurierte Netzwerke und Informationssysteme zu erkennen und die betreffenden Einrichtungen zu informieren.	✓	✓	×	×
	Erkennen, Beobachten und Analysieren von Sicherheitsproblemen	✓	✓	×	×

	Aufbau und Erleichterung kooperativer Beziehungen zu den betroffenen Akteuren	✓	×	×	×
	Teilnahme an Peer Reviews, die im Rahmen der NIS2-Richtlinie durchgeführt werden	✓	×	×	×
	Verbesserung der Cybersicherheit durch die Suche nach einem erhöhten Schutzniveau für Netzwerk- und Informationssysteme, die Stärkung von Präventions- und Sicherheitsmaßnahmen, die Prävention von Sicherheitsvorfällen und die Abwehr von Cyberbedrohungen	✓	✓	×	×
	Sicherstellung des Krisenmanagements im Falle von Cybervorfällen in Zusammenarbeit mit dem Koordinierungs- und Krisenzentrum der Regierung	✓	×	×	×
	Zusammenarbeit, insbesondere Informationsaustausch zwischen dem ZCB und anderen Behörden, insbesondere den sektoralen Behörden, dem NCCN und den zuständigen Behörden im Rahmen des Gesetzes vom 1. Juli 2011 über die Sicherheit und den Schutz kritischer Infrastrukturen, im Rahmen der Umsetzung des NIS2-Gesetzes und des oben genannten Gesetzes vom 1. Juli 2011	✓	×	×	×
	Zusammenarbeit zwischen wesentlichen und wichtigen Einrichtungen und den zuständigen Behörden im Rahmen des NIS2-Gesetzes	✓	✓	×	×
	Informationsaustausch zwischen den im NIS2-Gesetz genannten Behörden	✓	✓	×	×

	Gewährleistung der Kontinuität der von wichtigen oder wesentlichen Einrichtungen erbrachten Dienstleistungen	✓	×	×	×
	Meldung von Sicherheitsvorfällen und verhinderten Sicherheitsvorfällen	✓	✓	×	×
	Kontrolle und Überwachung wesentlicher und wichtiger Einrichtungen sowie Vorbereitung, Organisation, Verwaltung und Überwachung von Maßnahmen und Verwaltungsstrafen	✓	✓	✓	✓
	Kontrolle und Aufsicht über wesentliche und wichtige Einrichtungen sowie Vorbereitung, Organisation, Verwaltung und Überwachung von Maßnahmen und Verwaltungsstrafen	✓	✓	×	×
	ohne Strafzweck, Prävention, Ermittlung und Aufdeckung von Straftaten, die online oder über ein elektronisches Kommunikationsnetz oder einen elektronischen Kommunikationsdienst begangen werden, einschließlich Straftaten, die unter die schwere Kriminalität fallen	✓	✓	×	×
	Prävention schwerwiegender Bedrohungen der öffentlichen Sicherheit	✓	✓	×	×
	Untersuchung von Sicherheitsmängeln in Netzwerken oder elektronischen Kommunikationsdiensten oder Informationssystemen	✓	✓	×	×
	Verbreitung von Informationen über einen erheblichen Sicherheitsvorfall an andere Mitgliedstaaten und gegebenenfalls an die Öffentlichkeit	✓	✓	×	×

	Ausstellung europäischer Cybersicherheits-Zertifikate und Verwaltung von Ansprüchen	✓	✓	×	✓
	Kontrolle der Inhaber von europäischen Cybersicherheitszertifikaten, der Aussteller von EU-Konformitätserklärungen und der Konformitätsbewertungsstellen	✓	✓	×	✓
	Verhängung von Sanktionen gemäß der Verordnung (EU) 2019/881 und dem CSA-Gesetz	✓	×	×	✓
	Teilnahme an der Europäischen Zertifizierungsgruppe für Cybersicherheit	✓	×	×	×
	Zusammenarbeit mit anderen Behörden	✓	✓	×	✓
	als nationale Koordinierungsstelle im Sinne von Artikel 6 der europäischen Verordnung (EU) 2021/887 fungieren	✓	×	×	×
	fungiert als nationale Kontaktstelle für die Verordnung (EU) 2021/887	✓	×	×	×
	Bereitstellung von Fachwissen und aktiver Beitrag zu den strategischen Aufgaben, die in der Verordnung (EU) 2021/887 festgelegt sind	✓	×	×	×
	Förderung, Ermutigung und Erleichterung der Beteiligung der Zivilgesellschaft , der Industrie, insbesondere von Start-ups und KMU, der Hochschul- und Forschungsgemeinschaften und anderer Interessengruppen auf nationaler Ebene an grenzüberschreitenden Projekten und Maßnahmen im Bereich der Cybersicherheit, die aus einschlägigen EU-Programmen finanziert werden.	✓	×	×	×

	Bereitstellung von technischer Unterstützung für Interessengruppen, indem sie ihnen in der Antragsphase für Projekte helfen, die vom Kompetenzzentrum im Einklang mit seinem Auftrag und seinen Zielen verwaltet werden.	✓	×	×	×
	Bemühung um die Schaffung von Synergien mit einschlägigen Aktivitäten auf nationaler, regionaler und lokaler Ebene, z. B. mit der nationalen Forschungs-, Entwicklungs- und Innovationspolitik im Bereich der Cybersicherheit, insbesondere mit den in den nationalen Cybersicherheitsstrategien dargelegten Maßnahmen.	✓	×	×	×
	Implementierung spezifischer Maßnahmen, für die das Kompetenzzentrum Zuschüsse gewährt hat	✓	×	×	×
	Aufnahme eines Dialogs mit nationalen Behörden über mögliche Beiträge zur Förderung und Verbreitung von Bildungsprogrammen zur Cybersicherheit.	✓	×	×	×
	Förderung und Verbreitung der einschlägigen Ergebnisse der Arbeit des Netzwerks, der Gemeinschaft und des Kompetenzzentrums auf nationaler, regionaler oder lokaler Ebene	✓	×	×	×
	Bewertung der Anträge von Einrichtungen mit Sitz in Belgien auf Aufnahme in die Gemeinschaft	✓	×	×	×
	Förderung und Erleichterung der Beteiligung der betreffenden Einrichtungen an den Tätigkeiten, die sich aus dem Kompetenzzentrum, dem Netzwerk und der Gemeinschaft ergeben, und Überwachung, soweit angemessen, des Umfangs der Beteiligung an der Forschung, Entwicklung und Einführung von Cybersicherheit sowie des Umfangs der dafür bereitgestellten öffentlichen finanziellen Unterstützung.	✓	×	×	×

Auftrag im öffentlichen Interesse	Unterrichtung der betroffenen Person und Beantwortung ihrer Fragen	✓	✓	×	×
	Besucherempfang und Überwachung der Gebäude des ZCB	✓	✓	✓	×
Erfüllung eines Vertrags oder Zustimmung	Teilnahme an einer Veranstaltung (physisch oder online)	✓	×	×	×
	Einladung zu Veranstaltungen (physisch oder online) oder Newsletter	✓	×	×	×
	Um Ihre Fragen zu beantworten, Ihnen zu helfen oder Sie zu kontaktieren	✓	✓	×	×
	Öffentliches Auftragswesen und Vertragsmanagement	✓	✓	×	✓
	Registrierung auf einer der ZCB Websites oder für eine der ZCB Dienstleistungen	✓	✓	×	×
	Personalverwaltung (Statut, Vertrag, E-Gov, Auszubildende usw.)	✓	✓	×	✓
	Elektronisches Formular	✓	✓	×	×
	Unterrichtung der betroffenen Person und Beantwortung ihrer Fragen	✓	✓	×	×
	Verarbeitung zu statistischen und qualitativen Zwecken mit dem Ziel, unsere Dienstleistungen, unsere Websites und das Portal zu verbessern	✓	✓	×	×

	(verwendete Suchmaschine; verwendete Schlüsselwörter; Website, von der aus Sie gekommen sind; aufgerufene Seiten; Dauer des Aufrufs pro Seite; Liste der heruntergeladenen Dateien; Datum und Uhrzeit des Zugriffs; verwendeter Browser; Plattform und/oder Betriebssystem, das auf Ihrem Computer installiert ist)				
Legitimes Interesse des ZCB	Verwaltung der ZCB Websites	×	✓	×	×
	Verarbeitung zum Zwecke der Personalisierung der Nutzererfahrung (insbesondere Antworten in der Sprache der verpflichtenden Person)	×	✓	×	×
	Analyse des Verkehrs auf den ZCB Websites	×	✓ Verkehrsprotokolldateien	×	×
	Bekämpfung von bösartigen Websites/ Phishing-Angriffe und Beweissicherung im Falle eines Gerichtsverfahrens	✓	✓	×	×