Annex I: table of purposes

Legal basis of processing	Purposes of processing	Identification information, contact information and family status information	Navigation data and electronic communication data (not related to the content of the communication)	Data collected in the context of video surveillance of private places not accessible to the public	Data relating to administrative or criminal sanctions
Compliance with a legal obligation	Monitor, coordinate and oversee the implementation of Belgium's cybersecurity strategy	✓	×	×	×
	From an integrated and centralized approach, manage the various cybersecurity projects	✓	×	×	×
	Ensure coordination between relevant departments and governments, and governments and the private or scientific sector	✓	×	×	×
	Formulate proposals to adapt the cybersecurity regulatory framework	✓	×	×	×
	In cooperation with the Government Coordination and	✓	✓	✓	×

	Crisis Center, ensure crisis management in cyber incidents				
	Establish, disseminate and oversee the implementation of standards, guidelines and security standards for the various information systems of administrations and public institutions	✓	×	×	×
	Coordinate Belgian representation in international cybersecurity forums, follow-up of international commitments and proposals of the national position in this area	✓	×	×	×
	Coordinate evaluation and certification of information and communications systems security	✓	✓	×	×
	Inform and sensitize users of information and communication systems	✓	×	×	×
	Act as a national coordination center within the meaning of Article 6 of European Regulation (EU) 2021/887	✓	×	×	×

	Monitoring incidents at the national and international level, including the processing of personal data related to the monitoring of these incidents	✓	✓	×	×
	To the benefit of relevant stakeholders, provide early warnings, alerts, announcements and dissemination of information on risks and incidents	✓	✓	×	×
	Responding to incidents	✓	✓	×	×
	Provide dynamic risk and incident analysis and situational awareness	✓	✓	×	×
	Detect, observe and analyze computer security problems	✓	✓	×	×
	Encourage the adoption and use of common or standardized practices in incident and risk handling procedures, and incident, risk and information classification systems	✓	×	×	×
	Ensure cooperative contacts with the private sector and with other administrative	✓	×	×	×

	departments or authorities				
	Participate in the CSIRT network referred to in Article 12 of the NIS Directive	✓	×	×	×
	Report a criminal violation and provide all information about it to the prosecutor's office	✓	✓	✓	✓
	Report a vulnerability in network and information systems	✓	✓	×	×
	Issue European cybersecurity certificates and manage complaints	✓	✓	×	×
	Supervise holders of European cybersecurity certificates, issuers of EU declarations of conformity and conformity assessment bodies	✓	✓	×	×
	Impose penalties under Regulation (EU) 2019/881 and the CSA Act	✓	×	×	✓
	Participating in the European Cybersecurity Certification Group	✓	×	×	×
	Working with other governments	✓	✓	×	×
	Act as point of contact at the national level under	✓	×	×	×

	the aforementioned regulation				
	Provide expert advice and actively contribute to the strategic tasks referred to in the aforementioned regulation	✓	×	×	×
	Promote, encourage and facilitate at the national level the participation of civil society, industry, especially start-ups and SMEs, the academic and research community and other stakeholders in cross-border projects and in cybersecurity actions funded from the relevant Union programs	✓	×	×	×
	Provide technical assistance to stakeholders by supporting them at the application stage for projects managed by the knowledge center related to its mission and objectives	✓	×	×	×
	Pursue synergies with relevant activities at national, regional and local levels, such as national cybersecurity research, development and innovation policies, especially those	✓	×	×	×

	outlined in national cybersecurity strategies				
	Implementation of specific actions to which the knowledge center has awarded grants	✓	×	×	×
	Consult with national authorities on possible contributions to the promotion and dissemination of cybersecurity education programs	✓	×	×	×
	Promote and disseminate the relevant results of the work of the network, the knowledge community and the knowledge center at the national, regional or local level	✓	×	×	×
	Assessing requests from entities based in Belgium to be part of the knowledge community	✓	×	×	×
	Advocate for and promote the involvement of relevant entities in the activities of the knowledge center, network and knowledge community and, where appropriate, monitor the level of involvement in and amount of public	✓	×	×	×

	financial support for cybersecurity research, development and deployment				
Public interest duties	Informing the data subject and answering his/her questions	✓	✓	×	×
Performance of a contract or consent	Participation in an event	✓	×	×	×
	Welcoming visitors	✓	×	×	×
	To answer your questions, help you or contact you	✓	×	×	×
	Public procurement management, contracts	✓	×	×	×
	Registering on one of the websites or signing up for one of the CCB's services	✓	✓	×	×
	Personnel administration (statutory, contract, e-gov, trainee, etc.)	✓	✓	×	×
	Electronic form	✓	✓	×	×
	Informing the data subject and answering his/her questions	✓	✓	×	×
	Processing for statistical and qualitative purposes, to improve our	✓	✓ search engine used; keywords used; the	×	×

	services, our websites and the portal site		website through which you came; pages accessed; consultation time per page; list of files downloaded; date and time of access; browser used; platform and/or operating system installed on your computer		
Legitimate interest of the CCB	Managing the websites of the CCB	×	✓	×	×
	Processing to personalize the user experience (especially responses in the language of the data subject)	×	✓	×	×
	Analysis of traffic on CCB websites	×	✓ Log files regarding web traffic	×	×
	Combat *rogue/phishing* websites and preserve evidence in case of legal proceedings	✓	✓	✓	✓