Annex I : table of purposes

Legal basis of processing	Purposes of processing	Identification, contact and family details	Browsing and electronic communications data (other than communications content)	Data collected as part of video surveillance of enclosed premises not accessible to the public	Data relating to administrative or criminal penalties
Compliance with a legal obligation	Ensure coordination between the various departments and authorities involved in cyber security in Belgium	✓	×	×	×
	Supervise, coordinate and ensure the implementation of the Belgian cybersecurity strategy	✓	×	×	×
	Oversee the implementation of the NIS2 law	✓	✓	✓	✓
	Ensure coordination between the public authorities and the private sector or the scientific world	✓	×	×	×
	Draw up, disseminate and ensure the implementation of standards, guidelines and norms for the cybersecurity of the various types of information systems	✓	×	×	×
	Ensure crisis management in the event of cyber incidents, in cooperation with the government's Crisis and Coordination Centre	✓	✓	✓	×
	Coordinate Belgian representation at international cybersecurity forums, monitor international obligations and present the national viewpoint in this area	✓	×	×	×
	Coordinate the assessment and certification of the security of information and communication systems	✓	✓	×	×

	Inform and raise awareness among users of information and communication systems	✓	✓	×	×
	Award grants for cyber security projects and activities	✓	×	×	✓
	Facilitate and encourage the organisation of cybersecurity training courses for the staff of NIS2 entities	✓	×	×	×
	Monitor and analyse cyber threats, vulnerabilities and incidents at national level and, on request, provide assistance to the essential and important entities concerned to monitor their networks and information systems in real or near-real time	✓	✓	×	×
	Activate the early warning mechanism, dissemination of alert messages, announcements and dissemination of information on cyber threats, vulnerabilities and incidents to NIS2 entities as well as to competent authorities and other relevant stakeholders, if possible in near real time	✓	✓	×	×
	Respond to incidents and provide assistance to NIS2 entities	✓	✓	✓	×
	Gather and analyse forensic data, and provide a dynamic analysis of risks and incidents and an assessment of the cybersecurity situation	✓	✓	×	×
	Carry out, at the request of an essential and important entity, a proactive scan of the networks and information systems of the entity concerned in order to detect vulnerabilities likely to have a significant impact	✓	✓	×	×
	Participate in the CSIRT network, cooperate effectively, efficiently and securely within this network and provide mutual assistance in accordance with its capacities and skills to other members of the CSIRT network at their request	✓	✓	×	×
	Act as coordinator for the coordinated vulnerability disclosure process	✓	✓	×	×

	Contribute to the deployment of secure information-sharing tools	✓	✓	×	×
	Carry out proactive, non-intrusive scanning of publicly accessible networks and information systems where this scanning is carried out with the aim of detecting vulnerable or insecurely configured networks and information systems and informing the entities concerned	✓	✓	×	×
	Detect, observe and analyse security problems	✓	✓	×	×
	Establish and facilitate cooperative relations with the stakeholders concerned	✓	×	×	×
	Participate in peer reviews organised under the NIS2 Directive	✓	×	×	×
	Improve cybersecurity through the search of a higher level of networks and information systems protection, the reinforcement of prevention and security policies, the prevention of security incidents and the defence against cyberthreats	✓	✓	×	×
	Ensure cooperation, among others the exchange of information between the CCB and other authorities, including sectoral authorities, the NCCN and competent authorities for the law of July 1st, 2011 related to the safety and protection of critical infrastructures, in the framework of the execution of the NIS2 law and the aforementioned law of July 1st, 2011	✓	×	×	×

	Ensure cooperation between essential and important entities and the competent authorities for the NIS2 law	✓	✓	×	×
	Ensure information sharing between the authorities determined by the NIS2 law	✓	✓	×	×
	Ensure the continuity of services provided by important or essential entities	✓	×	×	×
	Notification of incidents and near misses	✓	✓	×	×
	Control and supervise of essential and important entities, as well as preparation, organisation, management and follow-up of administrative measures and administrative fines	✓	✓	✓	✓
	Prevent, research and detect infringements committed online or through a network or a, electronic communications service, including infringements qualified as serious crimes (without any prosecuting purposes)	✓	✓	×	×
	Prevent serious threats to public security (without any prosecuting purposes)	✓	✓	×	×
	Examine security failures of networks or electronic communications services or information systems	✓	✓	×	×

	Disseminate information on significant incidents to other Member states and, where appropriate, to the general public	✓	✓	×	×
	Issue European cybersecurity certificates and manage claims	✓	✓	×	✓
	Control 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 law	✓	×	×	✓
	Participate in the European Cybersecurity Certification Group	✓	×	×	×
	Cooperate with other authorities	✓	✓	×	✓
	Act as a national coordination centre within the meaning of Article 6 of European Regulation (EU) 2021/887	✓	×	×	×
	Act as the national contact point for Regulation (EU) 2021/887	✓	×	×	×
	Provide expertise and actively contribute to the strategic tasks set out in Regulation (EU) 2021/887	✓	×	×	×
	Promote, encourage and facilitate the participation of civil society, industry, in particular start-ups and SMEs, academic and research communities and	✓	×	×	×

	other stakeholders at national level in cross-border projects and actions in the field of cybersecurity funded by relevant EU programmes				
	Provide technical assistance to stakeholders by helping them in their application phase for projects managed by the Competence Centre in line with its mission and objectives	✓	×	×	×
	Endeavour to create synergies with relevant activities at national, regional and local level, such as national research, development and innovation policies in the field of cybersecurity, in particular the policies set out in national cybersecurity strategies	✓	×	×	×
	Implement specific actions for which grants have been awarded by the Centre of Competence	✓	×	×	×
	Establish a dialogue with national authorities regarding possible contributions to the promotion and dissemination of educational programmes on cyber security	✓	×	×	×
	Promote and disseminate the relevant results of the work of the Network, the Community and the Competence Centre at national, regional or local level	✓	×	×	×
	Assess applications from entities established in Belgium to become part of the community	✓	×	×	×
	Promote and facilitate the participation of relevant entities in the activities resulting from the Competence Centre, the Network and the community, and monitor, where appropriate, the level of participation in cybersecurity research, development and deployment and the amount of public financial support provided for it	✓	×	×	×
Public interest mission	Inform the person concerned and answer their questions	✓	✓	×	×

	Welcome visitors and surveil the buildings of the CCB	✓	✓	✓	×
Performance of a contract or consent	Taking part in an event (on premise or online)	✓	×	×	×
	Invite to events (on premise or online) or newsletter	✓	×	×	×
	Answer your questions, help you or contact you	✓	✓	×	×
	Manage public procurement and contract	✓	✓	×	✓
	Registration on one of the CCB websites or for one of the CCB services	✓	✓	×	×
	Registration to websites of the CCB or to a service of the CCB	✓	✓	×	×
	Personnel administration (statutory, contractual, e-gov, trainee, etc.)	✓	✓	×	✓
	Processing for statistical and qualitative purposes, with a view to improving our services, our websites and the portal (search engine used; keywords used; site from which you arrived; pages consulted; duration of consultation 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	Manage the websites of the CCB	×	✓	×	×
	Processing for the purpose of personalising the user experience (in particular responding in the language of the data subject)	×	✓	×	×
	Analysis of traffic on CCB sites	×	✓ Traffic log files	×	×
	Combat malicious sites/phishing attacks and preserve evidence in the event of legal proceedings	✓	✓	×	×