European Union Agency
for Cybersecurity

Agamemnonos 14
Chalandri 15231 | Attiki | Greece
Tel: +30 28 14 40 9711
E-mail: info@enisa.europa.eu
www.enisa.europa.eu

RECORD NO: 65

ENISA CYBER PARTNERSHIP PROGRAMME

Record 65 of processing operation “ENISA Cyber Partnership Programme”	
Date of last update	02/04/2025
Name and contact details of controller	ENISA, Operational Cooperation Unit (OCU), partnership_programme [at] enisa.europa.eu
Name and contact details of DPO	dataprotection [at] enisa.europa.eu
Name and contact details of Joint Controller	N/A
Name and contact details of processor	Microsoft Azure providing cloud hosting services under a framework contract with the European Commission (Cloud II) to which ENISA is party, hosting Mattermost collaboration platform.
Purpose of the processing	The processing of the data exchanged and shared within the trusted partnership programme with vendors, suppliers and similar initiatives (refered to as Trusted Network of partners) helps ENISA assist the Member States as well as EU Institutions in addressing large scale cross-border cybersecurity incidents and crises. The trusted network of partners should support ENISA and the Member States in reaching a common high level of cybersecurity through the access and exchange of information on threat and situational awareness and cyber events. This information should support ENISA to detect, protect, respond and recover from large-scale cybersecurity incidents and crisis within the EU. For the context there are three use cases in scope, namely: • Threat and situational awareness and information sharing on cyber events (first use case) • Request for information response (initiated by ENISA or by the other party) (second use case) • Collaboration on cyber information exchange projects (third use case) In the context of this exchange ENISA might receive information about cyber security incidents, which potentially may include personal data such as IP address. This however shall only be in limited ad-hoc cases and does not constitute the main purpose of the processing.
Description of data subjects	Appointed contact points from the partners. It is an unlikely case, but the data subject could be potentially any individual whose personal data are processed in the context of an information exchange/sharing within the Trusted Network of partners.
Description of data categories	For appointed contact points: First, Last, email, position Any information that could be Ad hoc personal data that might be included in the context of information sharing on threats or incidents through the relevant communication means (e.g., email). Depending on the type of event this information might include: any file transmitted to ENISA, technical protocol data (IP address, MAC address).

Time limits (for the erasure of data)	For appointed contact points, personal data are deleted upon request or upon withdrawal from the programme. Operational data, that might include some personal data (e.g. IP addresses), will be kept for as long as the information sharing on a particular event is required, in accordance with rules and procedures of ENISA. Data related to events that are older than 3 years will be kept for operation needs but irrelevant personal information will be removed, and the remaining data will be stored on ENISA's internal systems in a folder that is encrypted. Log data and similar data will be stored for a maximum period of three years. Data that needs to be kept longer to allow investigating breaches that took place in the past will be stored according to the highest security standards.
Data recipients	Dedicated ENISA staff members and appoint persons from programme partners. In justified cases data might be shared with MSs, CSIRTs Network, Cyclone Network and EUIBAs.
Transfers to third countries	No transfers outside EU/EEA are foreseen.
Security measures - General description	General security policy and technical/organisational measures applicable to ENISA's IT systems.
Privacy statement	Available at Mattermost platform.