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: 2

CIRAS - CYBER INCIDENT REPORT AND ANALYSIS SYSTEM

Record 2 of processing operation "CIRAS - Cyber Incident Report and Analysis System"	
Date of last update	13/2/24
Name and contact details of controller	ENISA, Knowledge and Information Team (KIT) incidentreporting [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	Bilbomatica that, under a contract with ENISA, is responsbile for web developement, maintenance and administration of electronic platform used for the Cybersecurity Incident Reporting and Analysis System tool. Contractor is based in Spain (www.bilbomatica.es)
Purpose of the processing	ENISA is mandated to collect security incidents from Member States (NRAs and Supervisory Bodies - SBs), based accordingly on Article 13(a) of the Framework Directive 2009/140and Article19 of eIDAS Regulation (EU) N°910/2014. Art 13(a) of the Framework Directive has been repealed and since 2019 relevant incident reporting for telecom authorities takes place under Art 40 of the EECC (European Electronic Communication Code), 2018/1972. Moreover, under NIS2 Directive, Art 23(9) anonymised and aggregated summary reports are submitted by MS to ENISA. Under NIS1 (and until the end of 2024) relevant provisions were defined in Articles 14 and 16. To this end, a platform for submission of such indicents has been created by ENISA (CIRAs), which also includes the contact points (representatives) of NRAs/SBs. The processing of personal data of contact points is part of the platform.
Description of data subjects	Nominated contact persons (representatives) of NRAs/SBs concerned.
Description of data categories	Name, address, phone, e-mail of NRAs/SBs representatives (contact persons). Incident reports submitted by NRAs/SBs in CIRAs are generally not considered to include personal data (only information on specific security indicents). Incident reports are considered to be classified and only accessible to the corresponding MS.
Time limits (for the erasure of data)	Personal data of platform users will be kept until their nomination as contact persons is revoked or they request to be removed.
Data recipients	Designated ENISA staff that is managing CIRAs platform, designated staff of the processor, NRAs/SBs respresentatives who are appointed members in the specific group, European Commission representatives who are appointed members in the specific group.The data may also be available to EU bodies charged with monitoring or inspection tasks in application of EU law (e.g. internal audits, European Anti-fraud Office – OLAF).

Transfers to third countries	No transfers outside EU/EEA are foreseen.
Security measures - General description	1. Restricted access - permission based and cascading (belonging to specific country). i.e. art 13a / art 19 + belonging to specific MS 2. Technical security measures are in place (security tests such as pentests and source code reviews are carried out regularly by contractor). 3.General security policy and technical/organisational measures for ENISA's internal IT systems and ENISA's website.
Privacy statement	Available on ENISA's intranet and to members of CIRAS platform.