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

CIRAS - CYBER INCIDENT REPORT AND ANALYSIS SYSTEM

Record of processing activity

Title	CIRAS - Cyber Incident Report and Analysis System
Name and contact details of controller	ENISA, Knowledge &Information Team
Name and contact details of DPO	dataprotection@enisa.europa.eu
Name and contact details of Joint Controller	N/A
Name and contact details of processor	Eau de Web: contactor responsbile for web developement and hosting of electronic platform used for information exchange (Resilience portal) and relevant tool (CIRAs). Contractor is based in Romania (www.eaudeweb.ro).
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. 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	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 as personal data (only information on specific security indicents).
Time limits (for the erasure of data)	As the need for a contact list is permanent, the data are stored in the CIRAs tool, as long as the NRAs or SBs keep this information available.
Data recipients	Designated ENISA staff that is managing CIRAs. 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.
Transfers to third countries	N/A
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 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.