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: 89

BUSINESS PROCESS MANAGEMENT TOOL

Record 89 of processing operation "Business Process Management Tool"	
Date of last update	19/01/26
Name and contact details of controller	ENISA, Corporate Support Services (CSS) – Governance, CSS-services [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	**BOC Information Technologies Consulting GmbH,** established in Vienna, Austria, **a** SaaS provider offering the ADONIS BPM tool, under EC Framework Contract DI/08030 – SIDE III to which ENISA is also a party.
Purpose of the processing	ADONIS is a BPM tool to support ENISA in: • Management and documentation of business processes; • Workflow visualisation, optimisation, and compliance management • Supporting internal audits and organisational governance; • Provision of user accounts and access control for BPM environment; • Maintenance, incident management, and technical support by BOC.
Description of data subjects	Appointed staff members and contractors of ENISA as well as designated contact persons or external collaborators that participate at process models definition.
Description of data categories	• Identification/contact data: name, email, department/unit/team • Organisational information: role, responsibilities, position in org. structure • Usage/activity data: login details, timestamps, actions in ADONIS, audit logs
Time limits (for the erasure of data)	• User accounts (such as first and last name, email, role) and process-related data: Retained for the duration of employment or project; deleted or anonymised within 6 months after account deactivation • Support and diagnostic data: Kept only as long as necessary to resolve the case (≤ 6 months) • System logs: Retained ≥ 60 days (BOC TOMs) and back ups: Typically retained between 30 – 90 days
Data recipients	Designated ENISA staff that are either authorised business process owners or business asministrators and ENISA contractors supporting the tool maintenance. 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	Security policy and technical/organisational measures that include • ISO 27001 / 27018 certified data centres; • Physical and logical access control (2-factor VPN, role-based authorisation); • Encryption in transit and at rest; • Central logging and alerting (≥ 60 days retention); • Daily backups + bi-annual restore tests; • Confidentiality agreements for all personnel; • Secure disposal of media and automated deletion of temporary support data.
Data Protection Notice	Available to all users of the tool.