

RECORDING OF PROCESSING ACTIVITY

NOTIFICATION TO THE DATA PROTECTION OFFICER (ARTICLE 31 REGULATION 2018/1725)

NAME OF PROCESSING ACTIVITY¹:

Usage of Microsoft cloud-based collaborative tools: Skype for Business and Teams

1) Controller(s) ² of data processing operation (Article 31.1(a))	
Controller: European Maritime Safety Agency (EMSA) Organisational unit responsible ³ for the processing activity: Unit 3.2 'Digital Infrastructure' Contact person: Ivo Kupsky, Head of Unit 3.2 Data Protection Officer (DPO): Radostina Nedeva-Maegerlein: dpo@emsa.europa.eu	
2) Who is actually conducting the processing? (Article 31.1(a)) ⁴	
The data is processed by EMSA itself	<input type="checkbox"/>
The organisational unit conducting the processing activity is:	

¹ **Personal** data is any information relating to an identified or identifiable natural person, i.e. someone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity. This information may, for example, be the name, date of birth, a telephone number, biometric data, medical data, a picture, professional details, etc.

Processing means any operation or set of operations which is performed on personal data, whether or not by automatic means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

² In case of more than one controller (e.g. joint operations), all controllers need to be listed here

³ This is the unit that decides that the processing takes place and why.

⁴ Is EMSA itself conducting the processing? Or has a provider been contracted?

The data is processed by a third party (contractor) or the processing operation is conducted together with an external third party [Microsoft] x

Contact point at external third party (e.g. Privacy/Data Protection Officer):

Microsoft EU Data Protection Officer

Dedicated mailbox to data subjects: <https://www.microsoft.com/en-GB/concern/privacy>

Tel: +353 (0) 1 295-3826

Attn: Data Protection

One Microsoft Place

Microsoft. South County Business Park, Leopardstown

Dublin 18, D18 P521, Ireland

3) Purpose of the processing (Article 31.1(b))

Why are the personal data being processed? Specify the rationale and underlying reason for the processing and describe the individual steps used for the processing.

There is a need identified in the Agency to facilitate virtual connectivity for collaborative work (e.g. meetings and training) among EMSA staff and with external users. This could easily be done via Skype for Business and Teams. To share information remotely and work collaboratively between users is amongst the common features of Teams and Skype for Business platforms due to their smooth integration with Office suite documents and the capacity to organize large meetings (up to 250 participants). With MS Teams and Skype for Business one can organise and record meetings combining video, audio, sharing features and special functions for the host. Participants can join via: PC, tablet, phone, or video conferencing system H.323.

Processing by EMSA

Providing authentication and authorization using EMSA Active Directory

Both tools are integrated with EMSA AD (Active Directory) and the authentication and authorization for using the tools is performed through it. This means the users need to be already registered at EMSA with name, last name and email address to enter EMSA environment/workspaces.

For external users that are not registered in EMSA AD joining meetings following links, not personal data processing is performed by EMSA.

Accessing the contents of the sessions during a limited period of time if the session is recorded.

Processing by provider (Processor):

a) Providing Customer the Online Services:

Delivering functional capabilities as licensed, configured, and used by Customer and its users, including providing personalized user experiences;

Troubleshooting (preventing, detecting, and repairing problems); and

Ongoing improvement (installing the latest updates and making improvements to user productivity, reliability, efficacy, and security).

When providing Online Services, Microsoft will not use or otherwise process Customer Data or Personal Data for: (a) user profiling, (b) advertising or similar commercial purposes, or (c) market research aimed at creating new functionalities, services, or products or any other purpose, unless such use or processing is in accordance with Customer's documented instructions.

b) Processing for Microsoft's Legitimate Business Operations:

"Microsoft's legitimate business operations" consist of the following, each as incident to delivery of the Online Services to Customer: (1) billing and account management; (2) compensation (e.g., calculating employee commissions and partner incentives); (3) internal reporting and modelling (e.g., forecasting, revenue, capacity planning, product strategy); (4) combatting fraud, cybercrime, or cyber-attacks that may affect Microsoft or Microsoft Products; (5) improving the core functionality of accessibility, privacy or energy-efficiency; and (6) financial reporting and compliance with legal obligations (subject to the limitations on disclosure outlined below).

When processing for Microsoft's legitimate business operations, Microsoft will not use or otherwise process Customer Data (i.e. EMSA) or Personal Data for: (a) user profiling, or (b) advertising or similar commercial purposes or any other purposes incompatible with the purposes of the processing by EMSA. In addition, where Microsoft is processing this data for legitimate business operations, Microsoft will process it only for the purposes set out in this section.

4) Lawfulness of the processing (Article 5(a)–(d)): Processing necessary for:

Mention the legal basis which justifies the processing

- (a) a task carried out in the public interest or in the exercise of official authority vested in EMSA (including management and functioning of the institution) ☒ (e.g. Article 2 'Core tasks of the Agency', par.4 b) EMSA founding regulation)
- (b) compliance with a legal obligation to which EMSA is subject ☐
- (c) necessary for the performance of a contract with the data subject or for the preparation of such a contract ☐

Important Note

Consent may not be the most appropriate legal basis, in particular in the employment context. However, if you wish to use consent as legal basis, ensure that it complies with the following: it must be freely given, specific, informed and unambiguous consent. Contact the DPO if you need further clarifications.

- (d) Data subject has given consent (*ex ante*, explicit, informed) ☐
Describe how consent will be collected and where the relevant proof of consent will be stored

5) Description of the categories of data subjects (Article 31.1(c))

Whose personal data are being processed?

EMSA staff	<input checked="" type="checkbox"/>
Non-EMSA staff (contractors staff, external experts, trainees)	<input checked="" type="checkbox"/>
Visitors to EMSA building	<input type="checkbox"/>
Relatives of the data subject	<input type="checkbox"/>
Other (please specify):	

6) Categories of personal data processed (Article 31.1(c))

Please tick all that apply and give details where appropriate

(a) General personal data:

The personal data contains:

- | | |
|--|--------------------------|
| Personal details (name, address etc) | x |
| Education & Training details | <input type="checkbox"/> |
| Employment details | x |
| Financial details | <input type="checkbox"/> |
| Family, lifestyle and social circumstances | <input type="checkbox"/> |
| Goods or services provided | <input type="checkbox"/> |

Other (please give details): recordings could include video images and voice.

(b) Sensitive personal data (Article 10)

The personal data reveals:

- | | |
|--|-------------------------------------|
| Racial or ethnic origin | <input checked="" type="checkbox"/> |
| Political opinions | <input type="checkbox"/> |
| Religious or philosophical beliefs | <input type="checkbox"/> |
| Trade union membership | <input type="checkbox"/> |
| Genetic, biometric or data concerning health | <input type="checkbox"/> |
| Information regarding an individual's sex life or sexual orientation | <input type="checkbox"/> |

Important Note

If you have ticked any of the sensitive data boxes, please contact the DPO before processing the data further.

7) Recipient(s) of the data (Article 31.1 (d)) <i>Recipients are all parties who have access to the personal data</i>	
Data subjects themselves	X
Managers of data subjects	<input type="checkbox"/>
Designated EMSA staff members	X
Designated Contractors' staff members	<input checked="" type="checkbox"/>
Other (please specify):	
8) Transfers to third countries or recipients outside the EEA (Article 31.1 (e)) <i>If the personal data are transferred outside the European Economic Area, this needs to be specifically mentioned, since it increases the risks of the processing operation.</i>	
Data are transferred to third country recipients:	
Yes	X
No	<input type="checkbox"/>
If yes, specify to which country: United States of America.	
If yes, specify under which safeguards:	
Adequacy Decision of the European Commission	<input type="checkbox"/>
Standard Contractual Clauses	X

Binding Corporate Rules

☐

Memorandum of Understanding between public authorities

☐

Important Note

If no safeguards are applicable, please contact the DPO before processing the data further.

9) Technical and organisational security measures (Article 31.1(g))

Please specify where the data are stored during and after the processing

How is the data stored?

EMSA network shared drive

☐

Outlook Folder(s)

☐

Hardcopy file

☐

Cloud (give details, e.g. public cloud)

X

Stored in EMSA Azure Active Directory (AAD) in Microsoft Datacentre

Servers of external provider

☐

Other (please specify):

- EMSA private infrastructure (on-premises) where the local AD is running.

10) Retention time (Article 4(e))

How long will the data be retained and what is the justification for the retention period? Keep in mind that there are pre-determined retention periods for most types of files. Those are explained in the Records Management Policy and Procedure of the Agency. You can check EMSA Records Management Policy and Procedure at the Intranet of the Agency.

Personal data is stored by EMSA only to provide authentication and authorization to access the tools.

- EMSA staff (including trainees and Seconded National Experts) will have access to the tools during the service period or until the tools are decommissioned from EMSA. When EMSA staff is leaving the organization, his/her associated user in AD is removed.
- Non-EMSA staff personal data included in AD is removed when the access to the workspaces are no longer needed (project termination includes decommission of the workspace including external users).
- Microsoft will delete or return all copies of Professional Services Data after the business purposes for which the Professional Services Data was collected or transferred have been fulfilled or earlier upon Customer's request, unless Microsoft is permitted or required by applicable law, or authorized under DPA, to retain such data.

Thank you for completing the form.
Now please send it to the DPO using the ARES workflow