

RECORDING OF PROCESSING ACTIVITY
NOTIFICATION TO THE DATA PROTECTION OFFICER
(ARTICLE 31 REGULATION 2018/1725)

NAME OF PROCESSING ACTIVITY¹:

Usage of Microsoft Online Services

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

Contact person: Maja Markovčić Kostelac

Data Protection Officer (DPO): Radostina Nedeva-Maegerlein: dpo@emsa.europa.eu

2) Who is actually conducting the processing? (Article 31.1(a))⁴

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.

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

European Maritime Safety Agency (EMSA)

Executive.Secretariat@emsa.europa.eu

Tel +351 21 1209 220

EMSA, Praça Europa 4, 1249-206 Lisbon, Portugal

<https://emsa.europa.eu>

The data is processed by EMSA itself

☐

The organisational unit conducting the processing activity is:

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.

Reason 1:

There could be performance, functional, security and economic reasons to exploit virtual infrastructure and operations from the Cloud (see EMSA Cloud Strategy for further details) both for the maritime and corporate applications provision of services. Microsoft offers on online services that fulfil EMSA needs.

Reason 2:

For large virtual environments the Microsoft online services and tools integrate well

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

between them and offer additional functions. As an example, the Microsoft SharePoint online and Teams ecosystem integrates well with office desktop suite which cannot be provided by other similar tools for a comparable price and accessibility. However, there are specific risks for other tools such as Teams or the email as explained before in this chapter. Those are considered both within the scope of this DPIA and other particular DPIAs dedicated to each tool separately.

Reason 3:

Microsoft is already a trustworthy provider for EMSA and for this particular project, no additional personal data need to be provided to it. The shortfalls in terms of privacy issues were studied and mapped by the EDPS Investigation Ref.C 2018-0319. Considering the outcome of the said investigation, the Agency implemented the measures below as risk mitigation measure. This being said those measures do not preclude the possibility that the Agency implements also additional (supplementary measures) should additional risks be identified in the process of using the said services. From a technical point of view, the services run using the same infrastructure EMSA is using for enjoying other services from the same provider. In addition to that, no additional contracts and investment need to be made since the service is already paid and under the same contract EMSA holds with Microsoft.

Reason 4:

Specific use cases such as training sessions or videoconference with contractors, among others, require recording such sessions to allow participants on the session to access the content asynchronously. This feature is offered natively by both MS Teams and Skype for Business.

Description of the processing

Personal information processed by Microsoft online services can be:

- Usernames, password hashes and emails for log in (authentication and authorization) into the cloud services. The process flow is as follows:

Microsoft Online services are integrated with EMSA AD (active directory), using EMSA Azure AD or using EMSA IDM (as explained in Risks' chapter). The authentication and authorization for using the tools is performed through EMSA AD, EMSA AAD and EMSA IDM. On the other hand, EMSA AAD is not used for direct registration of users and the information contained in EMSA AAD comes from synchronization of the EMSA AD with the EMSA AAD (one direction, from EMSA to Azure, and not the other way around).

This means the users need to be already registered at EMSA with name, surname and email address though this feature could change in the future and direct registration in AAD could be allowed.

For external users that are not registered in EMSA AD, no information is collected by EMSA. This means that this element of the processing relates to an integration of an existing data, rather than collection (i.e. processing) of additional data.

- Personal information contained in customer data and customer content. The process flow is as follows:

Microsoft differentiates between customer data (any file such as text files, images, videos, audio files, spreadsheets, meeting notifications, chat records, etc) and customer content within customer Data (Exchange online email text and attachments, information processed by applications in Azure, information in SharePoint online, site content, instant messaging conversations, Power BI reports, etc).

All this information is originated by the user (e.g. emails, files uploaded to SharePoint online) or could be received by an external source (e.g., received emails; personal data received by a maritime application from a member state as explained before for the case of SafeSeaNet). In any case the information is transferred in and out and stored by the Microsoft Online services as explained in the Scope chapter for Microsoft SaaS services and MS Azure for corporate and maritime applications.

For the specific secure configuration of the different services under scope to minimize the exposure of personal information, check *Annex II - DPIA Service Elements Matrix_Microsoft Online*.

For understanding the specific risks and proper configuration related to Exchange online, and the Microsoft 365 in general, check Annex IV - Security assessment of Microsoft 365_rev1.

For the specific risks and actions related to Teams, an ad-hoc DPIA is performed in the Agency.

Purposes of the processing:

- Providing Online Services includes:
 - Details of the scope of the contracted services are detailed in EMSA contractual data and the applicable standard contractual clauses regarding data protection so all processing shall be aligned to what is described there. Microsoft processes the information to Deliver de services following EMSA licences and configurations. This also affects EMSA users configuration and use of the services in order to create a specific user experience
 - Troubleshooting (preventing, detecting, and repairing problems) following EMSA tickets or automatically; and
 - Ongoing improvement (installing the latest updates and making improvements to user productivity, reliability, efficacy, and security).

When providing Online Services, Microsoft shall 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 EMSA documented instructions.

- Processing for Microsoft's Legitimate Business Operations:

Microsoft could process EMSA's business data for legitimate business operations. Microsoft considers as its legitimate business operations those that provide to them:

1. Billing capacity and account management where
2. Calculating its own employee commissions and partner incentives and other compensations;
3. Security investigations to combatting fraud, cybercrime, or cyber-attacks to their infrastructure;
4. Improving the core functionality of accessibility, privacy or energy-efficiency;
5. Financial reporting and compliance with legal obligations;

In every such case EMSA shall be informed in advance or as soon as possible when such processing takes place and about the scope and the nature of such processing.

Microsoft shall commit to process only for the previously mentioned business operations and not processing EMSA's personal data for profiling EMSA's users or customizing commercial and advertising campaigns.

Description of its interactions with other processes

Microsoft online tools rely on personal data existing in EMSA Active Directory on premises or in Cloud: a username, an email address and a password.

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)	<input checked="" type="checkbox"/>
Education & Training details	<input checked="" type="checkbox"/>
Employment details	<input checked="" type="checkbox"/>
Financial details	<input checked="" type="checkbox"/>
Family, lifestyle and social circumstances	<input checked="" type="checkbox"/>
Goods or services provided	<input checked="" 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 checked="" type="checkbox"/> |
| Religious or philosophical beliefs | <input checked="" type="checkbox"/> |
| Trade union membership | <input checked="" type="checkbox"/> |
| Genetic, biometric or data concerning health | <input checked="" type="checkbox"/> |
| Information regarding an individual's sex life or sexual orientation | <input checked="" 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))

Recipients are all parties who have access to the personal data

- | | |
|---------------------------------------|-------------------------------------|
| Data subjects themselves | <input checked="" type="checkbox"/> |
| Managers of data subjects | <input type="checkbox"/> |
| Designated EMSA staff members | <input checked="" type="checkbox"/> |
| 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))

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.

Data are transferred to third country recipients:

Yes ☒

No ☐

If yes, specify to which country:

United States of America.

If yes, specify under which safeguards:

Adequacy Decision of the European Commission ☐

Standard Contractual Clauses ☒

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 public cloud, EMSA Azure servers datacentres in the EU

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 and IDM is removed.

- Non-EMSA staff personal data included in AD and in IDM is removed when the access is 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