

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

NAME OF PROCESSING ACTIVITY:

Usage of ZOOM tool for virtual meetings/trainings/interviews

1) Controller(s)¹ of data processing operation (Article 31.1(a))
<p>Controller: European Maritime Safety Agency (EMSA)</p> <p>Organisational unit responsible for the processing activity: 4.2 Events</p> <p>Contact person: Sharif Abu-Ghazaleh, Events Assistant, events_bookings@emsa.europa.eu</p> <p>Data Protection Officer (DPO): Radostina Nedeva-Maegerlein: dpo@emsa.europa.eu</p>
2) Who is actually conducting the processing? (Article 31.1(a))²
<p>The data is processed by EMSA itself <input checked="" type="checkbox"/></p> <p>The organisational unit conducting the processing activity is: 4.2 Events</p> <hr/> <p>The data is processed by a third party (contractor) or the processing operation is conducted together with an external third party <input checked="" type="checkbox"/></p> <p>Gonzalo Gutierrez Espinosa</p> <p>Account Executive Zoom Video Communications Call 888-799-9666 Zoom 628-802-59000</p> <p>Zoom is contracted via Insight: Karyna Ponomarova Inside Account Manager Insight t. +32 2 263 60 38 karyna.ponomarova@insight.com</p>

¹ In case of more than one controller (e.g. joint operations), all controllers need to be listed here

² Is EMSA itself conducting the processing? Or has a provider been contracted?

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 to hold and record virtual meetings/trainings/interviews with external and internal participants via Zoom tool which is the most suitable for larger number of participants. With the Zoom tool, one can organise meetings with up to 100 participants, combining video, audio, recording, sharing features and special functions for the host. Participants can join via: PC, tablet, phone, or video conferencing system H.323. For larger virtual meetings/trainings/interviews the ZOOM tool offer additional functions which cannot be provided by other similar tools for a comparable price and accessibility.

Due to COVID- 19 pandemic, the use of ICT tools to support remote work is in high demand to ensure business continuity. Some of those tools may pose risks to the processing of personal data due to their technical immaturity and different purposes of usage. To evaluate and attempt to mitigate those risks, EMSA carried out a DPIA on the ZOOM tool. As such a description of the procedure to use Zoom is explained below:

The process of booking a Zoom meeting shall be as follows:

1. Once the meeting/training/interview date is decided a booking request is sent to Events Cell via the dedicated email address, the events assistant will schedule the meeting in Zoom. An Outlook calendar booking including all connection details meeting ID and meeting Password will be sent to the person organising the meeting/training/interview, who will forward to all the participants. The participants can connection to the meeting via: PC, tablet, mobile device, phone or via H.323 video conferencing system. The invitation for the meeting/training/interview to the participants may be sent via the ARES or email accompanied with the Privacy Statement of the Zoom tool together with the connection guide.

Connection procedure for participants:

a. If joining from a computer, they enter by clicking the Zoom meeting link or by entering the meeting ID and password in Zoom tool <https://zoom.us/join>. When entering a Zoom meeting for the first time from a computer they will need to download a small application file. (it is also possible to attend by web-based option without the need to download the application file but with limited control options). The recommended browsers are updated versions of Mozilla, Chrome and Edge

b. If they are joining from a mobile device (Android smartphone/tablet, Apple iPhone/iPad) then it will simply prompt them to download the Zoom Cloud Meetings app from the App/Play Store.

c. By phone: If they would like to attend a Zoom meeting via telephone, they call the number for their country (up to date numbers <https://zoom.us/join>). Then enter the Meeting ID and PIN when prompted.

2. Just before entering the meeting they will be prompted to enter a display name. This name is simply to identify the participant in the meeting.

3. The participants will enter a waiting room first and then the host or co-host will accept the participants to enter. This has become a mandatory/standard as of 06/04/2020 and avoids unwanted participants joining the meeting. It is also possible to lock the meeting so no additional participants can join even if they have the meeting ID and password.

- The meeting organiser (EMSA staff) can record and download the video and the attendees list from Zoom. The record function is deactivated in the administrator settings for attendees. The host shall announce that no recordings of any kind shall be made by the attendees. If participants do not wish their image to be recorded, they shall to turn-off their camera.

The only legitimate recording shall be made by the host for the purposes of recording content of the meeting/training/interview.

- For larger meetings or trainings, the EMSA online registration tool (Joomla) may be used for participants to register their attendance, which will include their name, family name, organisation, country and email address. The outlook invitation for the Zoom meeting (with connection details) will be sent to participants via the email address provided during the online registration.
- Monitor the announced risks as well as the reactions of the specialists in cyber security.
- The supporting infrastructures needed for usage of ZOOM is: MS Edge (or Chrome or Mozilla).

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)



The European Maritime Safety Agency (EMSA) was established under Regulation 1406/2002/EC, as amended, for the purpose of ensuring a high, uniform and effective level of maritime safety. More information is available at: <http://www.emsa.europa.eu>.

(b)	compliance with a legal obligation to which EMSA is subject	<input type="checkbox"/>
(c)	necessary for the performance of a contract with the data subject or for the preparation of such a contract	<input type="checkbox"/>
(d)	Data subject has given consent (<i>ex ante</i> , explicit, informed)	<input type="checkbox"/>
5) Description of the categories of data subjects (Article 31.1(c)) <i>Whose personal data are being processed?</i>		
	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)) <i>Please tick all that apply and give details where appropriate</i>		
(a) General personal data: The personal data contains:		
	Personal details:	<input checked="" type="checkbox"/>
	Account data includes name, email address, phone, language preference, user Ids and password (if single sign on is not used), and profile picture.	
	Image/voice of the participants in case of recordings.	
	Education & Training details	<input type="checkbox"/>

Employment details	<input type="checkbox"/>
Financial details	<input type="checkbox"/>
Family, lifestyle and social circumstances	<input type="checkbox"/>
Goods or services provided	<input type="checkbox"/>
Other (please give details):	
(b) Sensitive personal data (Article 10)	
The personal data reveals:	
Racial or ethnic origin	<input 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"/>
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	<input checked="" type="checkbox"/>
External and Internal Participants of meetings/trainings/interviews	

Managers of data subjects	<input type="checkbox"/>
Designated EMSA staff members	<input checked="" type="checkbox"/>
EMSA Events and Training Teams	
Designated Contractors' staff members	<input checked="" type="checkbox"/>
Zoom staff	
Other (please specify): Any participants of meetings/trainings/interviews	

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 ☒

If yes, specify to which country:

Zoom divide data into three categories:

Account Data. This is the information a user gives to create a Zoom account. It includes name, email address, phone, language preference, user Ids and password (if single sign on is not used), and profile picture.

Operation Data. This is all information that is generated automatically through use of the Zoom service.

Communications Content. This is the data the user chooses to record or share during a meeting or call including cloud recordings, meeting transcripts, files that are exchanged during a meeting and voicemails. It includes configuration data, metadata, feature usage data and performance data.

The renewal of the Zoom subscriptions was done through the existing framework contract with INSIGHT and they have a specific setup in Zoom as a EU Cluster customer, meaning that they have a special setup with Zoom where their communications content is stored only in **EU or Canadian** data centres.

From the application side, account data and operation data is also be stored in the **US**, not exclusively in the EU.

If yes, specify under which safeguards:

Adequacy Decision of the European Commission with Canada	<input checked="" type="checkbox"/>
Standard Contractual Clauses within the framework contract of Insight	<input checked="" type="checkbox"/>
Binding Corporate Rules	<input type="checkbox"/>
Memorandum of Understanding between public authorities	<input type="checkbox"/>
9) Technical and organisational security measures (Article 31.1(g)) <i>Please specify where the data are stored during and after the processing</i>	
<p>How is the data stored?</p> <p>EMSA network shared drive <input checked="" type="checkbox"/></p> <p>For video recording of the meeting</p> <p>Outlook Folder(s) <input checked="" type="checkbox"/></p> <p>For video recording of the meeting</p> <p>Hardcopy file <input type="checkbox"/></p> <p>Cloud (Zoom cloud meeting space) <input checked="" type="checkbox"/></p> <p>Servers of external provider <input checked="" type="checkbox"/></p> <p>See point 8 above.</p> <p>Other (please specify):</p>	
10) Retention time (Article 4(e)) <i>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.</i>	

The Retention period of the Zoom tool is defined in their privacy statement published here: [ZOOM PRIVACY STATEMENT - Zoom](#)

If there is a recording of the meeting where EMSA download the video file, the video file is retained for 5 years in line with the EMSA 6.3.1 Organisation of Events Retention List.