<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong></td>
<td>Title of the processing activity</td>
<td>Processing personal data via The Rapid Alert System (RAS) and The communicators Portal (CP) related to information exchange on disinformation and proactive communication of EU topics</td>
</tr>
<tr>
<td><strong>2</strong></td>
<td>Update of the record (last modification date)</td>
<td>15/12/2020</td>
</tr>
<tr>
<td><strong>3</strong></td>
<td>Register reference number</td>
<td>2381</td>
</tr>
</tbody>
</table>
| **4** | Identity and contact details of the Data Controller  
Joint Controller (if applicable)  
Data Processor (if applicable) | Controller:  
European External Action Service  
Rond Point Schuman 9A, 1046 Brussels, Belgium  
Data Controller contact entity:  
EEAS Division ’ Strategic Communications 2: Task Forces and Information Analysis Division - EEAS.SG.AFFGEN.7  
Functional mailbox: EEAS SG AFFGEN 7 SG-AFFGEN-7@eeas.europa.eu  
Rapid-Alert-System@eeas.europa.eu  
Concerning the personal data appearing in the content of the Communicators Portal, the data controller determining the purpose and the means of the processing activity under the supervision of the Director General is the following entity:  
Communications Directorate General of the General Secretariat of the Council (GSC) of the European Union  
Processor:  
Aurea, Inc. Aurea Messaging Solutions (AMS)  
https://www.aurea.com  
Data Protection Officer: |
| **5** | Identity and contact details of the Data Protection Officer | EEAS Data Protection Officer (DPO):  
Emese Savoia-Keleti  
SG.AFFGEN.DPO  
Functional Mailbox of the DPO:  
DATA-PROTECTION@eeas.europa.eu |
## Purpose of the processing activity

**Purpose**

The purpose of the processing activity in the context of the Rapid Alert System (RAS) is to enable the exchange of information as well as alerts on disinformation campaigns and foreign interference through a dedicated technological infrastructure, which facilitates sharing of assessments and enables common situational awareness between EU Member States and EU Institutions, coordinated activity as well as attribution and common response. The Rapid Alert System is an important component of the European Union's overall approach to tackling disinformation, as set out in the Action Plan against Disinformation, which was endorsed by the European Council in December 2018.

The Communicators Portal allows uploading and exchanging communication products (such as videos, texts, images, infographics, animations, etc.) among EU Institutions and EU Member States. This aims at intensifying the cooperation between the EU Institutions and the EU Member States when it comes to proactive communication about topics related to the European Union and make EU communication more effective.

**Description**

The Rapid Alert System is an important component of the European Union's overall approach to tackling disinformation, as set out in the Action Plan against Disinformation, which was endorsed by the European Council in December 2018.

The Communicators Portal allows uploading and exchanging communication products (such as videos, texts, images, infographics, animations, etc.) among EU Institutions and EU Member States. This aims at intensifying the cooperation between the EU Institutions and the EU Member States when it comes to proactive communication about topics related to the European Union and make EU communication more effective.

## Legal basis and lawfulness

Processing of personal data is necessary in the public interest (Paragraph 1.a of Art. 5 of Regulation (EU) 2018/1725.

**Legal basis:**

Processing of personal data is necessary in the public interest (Paragraph 1.a of Art. 5 of Regulation (EU) 2018/1725.

**Legal reference:**

- Action Plan against Disinformation JOIN(2018) 36 final Brussels, adopted on December 5, 2018

Concerning the third parties involved, i.e. G7 and NATO: "The Rapid Alert System should be closely linked to existing 24/7 capabilities such as the Emergency Response Coordination Centre and the Situation Room of the European External Action Service. The EU Hybrid Fusion Cell of the Intelligence and Situation Centre as well as the relevant Council Working Parties could also be used as channels for sharing information. The Commission and the High Representative will ensure regular exchange of information and best practices with key partners, including within the G7 and the North Atlantic Treaty Organisation." Further legal reference: Council Decision of 26 July 2010 establishing the organisation and functioning of the EEAS (2010/427/EU) – OJ L 201, 3/8/2010, p. 30.

Access given to non-EEA (G7 and NATO) members is based on the public interest enshrined in the Action plan and the Charleroi commitments: the need for G7 members to tackle disinformation.

## Categories of individuals whose data is processed

**Users of the system:**

- Assigned National contact points
- Assigned additional national members nominated by EU Member States
- Assigned RAS / CA participants nominated by the EU institutions
- Assigned Representatives of the G7 member states
- Assigned NATO staff (subsequent to registration)
### Categories of data - Data processed

Concerning the RAS, the data, including personal data, which may be processed for that purpose are the following:

I. Personal data of National contact points as well as additional national members nominated by the EU Member States as well as RAS participants nominated by the EU institutions, from representatives of the G7 member states (for the G7 Rapid Response Mechanism) and subsequent to registration assigned NATO staff, include:

- a) name
- b) mobile telephone number (optional, are used to send sms alerts, in its absence only e-mail alerts are sent),
- c) e-mail addresses,
- d) Member State
- e) information on the professional occupation and work place,
- f) photo (optional).
- g) additional information voluntarily provided by the individual member, such as a short CV (optional).

II. Content-type data linked to the open source materials that will be uploaded to the system by its participants, including names, e-mail addresses and behaviour. Only personal data which appear in open sources are processed, they are not intended to be specifically collected, neither to be further processed in any way.

Concerning the Communicators Portal, the data (including personal data) processed are the following:

I. Personal data of National contact points as well as additional national members nominated by the EU Member States as well as RAS participants nominated by the EU institutions, from G7 member states and subsequent to registration assigned NATO staff, include

- a) name
- b) e-mail address
- c) Member State
- d) information on the professional occupation and work place
- e) photo (optional)
- f) additional information voluntarily provided by individual members, e.g. short CV or phone number (optional).

II. Content-type data linked to the open source materials that will be uploaded to the system by its participants, including names, e-mail addresses and behaviour. Only personal data which appear in open sources are processed, they are not intended to be specifically collected, neither to be further processed in any way.

Users access the Rapid Alert System and the Communicators Portal through EULogin. Data Controllers only receive information from EULogin about your identity that is necessary to confirm user access to the portal.

More information on:
https://webgate.ec.europa.eu/cas/privacyStatement.html
### Recipients of data – Access to data

Concerning the Rapid Alert System, the recipients of data are as follows:
- EEAS Strategic Communications Division staff members assigned to manage and moderate the work of the Rapid Alert System.
- Staff of the EEAS IT department responsible for development and technical supervision of the IT systems (see note below)*.
- Staff of the European Commission’s IT department responsible for ensuring the functioning of 2-factor-authentication through the EU Login application, through which users access the Rapid Alert System.
- National contact points as well as additional members from EU Members and EU institutions, who have been registered to the system (both RAS and CP) as its users with viewer or contributor rights.
- Representatives of the G7 Rapid Response Mechanism, in the framework of the G7 Information Sharing Group on the Rapid Alert System, and subsequent to registration, NATO Headquarters assigned staff. These representatives of the G7 RRM and NATO will have access to the information you provide on your profile.

Concerning the Communicators Portal, the recipients of data are as follows:
- Staff of the COMM directorate-general of the Council of the European Union assigned to manage and moderate the work of the Communicators Portal.
- EEAS Strategic Communications Division staff members assigned to assist COMM directorate-general of the Council of the European Union in managing the work of the Communicators Portal.
- Staff of the EEAS IT department responsible for development and technical supervision of the IT systems*.
- Staff of the European Commission’s IT department responsible for ensuring the functioning of 2-factor-authentication through the EU Login application, through which users access the Communicators Portal.
- National contact points as well as additional national members from EU Members and EU institutions, who have been registered to the system (both RAS and CP) as its users with viewer or contributor rights.
- Representatives of the G7 Rapid Response Mechanism, in the framework of the G7 Information Sharing Group on the Rapid Alert System, and subsequent to registration, NATO Headquarters assigned staff. These representatives of the G7 RRM and NATO will have access to the information you provide on your profile.

Deviating from the above, personal data appearing in the content of the portals is visible only to the users of that portal.

### Transfer to Third Countries or International Organizations (IOs) and suitable safeguards (if applicable)

Personal data is not intended to be transferred to a Third Country, nor to an International Organisation with the exception of the G7 Rapid Response Mechanism and of potentially NATO Headquarters assigned staff as well as the service provider (processor).

Staff of the service provider for the platform supporting the RAS and CP assist EEAS IT experts in resolving technical issues and have access to the platform and the data of users contained therein only when finding solution to technical problems and questions. The service provider is a U.S.-based enterprise (https://www.aurea.com) that will process data merely occasionally, as far as necessary for technical assistance, and on documented instructions provided by EEAS IT experts, solely on behalf of the EEAS pursuant to Article 29 of Regulation (EU) 2018/1725. In cases where the Aurea Messaging Solutions (AMS) "AlertFind" is used, staff of the service provider may have access to personal data.

### Time limit for keeping the data - Retention period

Personal data is kept for a maximum period of one year after the termination of the operations of the Rapid Alert System and of the Communicators Portal. Regular update of the data is guaranteed by provision of information from the national contact points and by the users themselves. Upon 4 months of inactivity the profile will be disabled and not visible to other users, which can be reactivated upon the request of the user. Rectification or deletion of data can be requested as indicated under point 6; however deletion of the account may result in losing contact with the EU Member State national authorities, organisations and EU institutions designating the platform user. Deletion of the account may also result in losing any content that the member of the RAS or of the Communicators Portal has posted on the platform during his activity.
<table>
<thead>
<tr>
<th>13</th>
<th>Data Storage</th>
<th>Files storing personal data are kept on the secure servers of the EEAS.</th>
</tr>
</thead>
</table>
| 14 | General description of security measures | Appropriate organisational and technical measures are ensured according to Article 33 of Reg. (EU) 2018/1725. Data is processed by assigned staff members. Individual files storing personal data of users are protected by a password only known to those who need it. They are kept on the secure servers of the EEAS. Measures are provided to prevent unauthorised entities from access, alteration, deletion, disclosure of data. General access to personal data is only possible to recipients with a UserID/Password. Access to the Rapid Alert System and the Communications Portal is ensured by the two-factor authentication system of EULogin. Physical copies of personal data are stored in a properly secured manner.
Participants from outside the EEA member states have to sign a confidentiality declaration. |
| 15 | Rights of individuals | Individuals have the right of access to their personal data and the right to correct any inaccurate or incomplete personal data. The right of rectification can only apply to factual data processed. Under certain conditions, individuals have the right to ask the deletion of their personal data or restrict their use as well as to object at any time to the processing of their personal data on grounds relating to their particular situation. The EEAS will consider the request, take a decision and communicate it to the individuals without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary. For more detailed legal references, information can be found in Articles 14 to 21, 23 and 24 of Regulation (EU) 2018/1725. In specific cases, restrictions under Article 25 of the Regulation may apply.
If individuals have questions concerning the processing of their personal data, they may address them to the Data Controller via the following functional mailboxes.  
Concerning the Rapid Alert System: Rapid-Alert-System@eeas.europa.eu  
Concerning the Communicators Portal: information.wp@consilium.europa.eu |
| 16 | Information to data subjects | Information is provided to the Data Subjects related to this Record in the Privacy Statement. The Privacy Statement or Data Protection Notice is accessible on the intranet / internet of the EEAS / on the IT tool. Data Subjects may also request further information by contacting the controller via Rapid-Alert-System@eeas.europa.eu. |