EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

RECORD OF PROCESSING ACTIVITY ACCORDING TO ARTICLE 31 REGULATION 2018/1725[1] NOTIFICATION TO THE DATA PROTECTION OFFICER

NAME OF PROCESSING OPERATION[2]: Handling of contact data stored in the Agency's contacts database (CRM)

Reference number: DPR-2018-052
Creation date of this record: 21/12/2018
Last update of this record: 15/07/2022
Version: 3

Part 1 (Publicly available)

1) Controller(s)[3] of data processing operation (Article 31.1(a))
Controller: European Union Agency for Fundamental Rights (FRA) Schwarzenbergplatz 11, A-1040 Vienna, Austria Telephone: +43 1 580 30 – 0 Organisational unit **responsible**[4] for the processing activity: Communications and Events Unit Contact details: information@fra.europa.eu Data Protection Officer (DPO): dpo@fra.europa.eu

2) Who is actually conducting the processing? (Article 31.1(a))[5]	
The data is processed by the FRA itself	☒
The data is processed also by a third party (contractor)	☒

1 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1725

2 **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.

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

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

5 Is the FRA itself conducting the processing? Or has a provider been contracted?

-Managing Innovation Strategies, SLL (MainStrat) in consortium with SARENET, S.A.U., FRA's Web hosting contractor, where the CRM system is hosted.

-EWORX S.A., the Agency's web development contractor providing the Customer Relationship Management system (CRM)
This particular processor is specifically involved in the setting up of the CRM system and providing technical support. Beyond this concrete task, it is not envisaged that it will process data on the controller's behalf on a regular basis.

-Flowmailer SMTP relay service – Flowmailer is FRA's contractor for email relays. They receive the email that needs to be delivered and then relays it to the final recipient. All data processed by Flowmailer is safely stored in independently functioning Dutch data centers (Amsterdam region). Customer data therefore never leaves the European Union. For further information, please refer to the website of Flowmailer (https://flowmailer.com/en/why/compliance-security)

The processors/contractors were selected by FRA following a public procurement procedure

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

Why are the personal data being processed? Please provide a very concise description of what you intend to achieve with the processing operation. Specify the rationale and underlying reason for the processing and describe the individual steps used for the processing. If you do this on a specific legal basis, mention it as well (e.g. staff regulations for selection procedures).

The purpose of the processing of the personal data is to inform interested parties, whose details are stored in the Agency's contacts database (CRM or Customer Relationship Management system), on the upcoming and recent activities of the Agency.

With regard to the FRA's stakeholder groups and FRA internal bodies like Data Protection Authorities, Equality Bodies, FRANET, Fundamental Rights Platform, National Human Rights Institutes, National Liaison Officers, National Parliamentary Focal Points, FRA Management Board, and Scientific Committee, etc, such data (name, organisation, job title, email address) may be used for the purpose of FRA's stakeholder cooperation activities as defined in FRA's communication and cooperation framework, notably to include these personal data in a 'country overview of national stakeholders'. These data will only be shared with FRA networks and FRA internal bodies and not further processed in a way incompatible with those purposes.

More concretely, the CRM system handles contact data as follows. There are two workflows depending on whether there is a pre-existing consent to receive information about the Agency's activities from the stakeholder or not.

i) No pre-existing consent: In this case, an opt-in procedure is used. The data subject's data is stored in the CRM but cannot be used for mailings until they grant consent. An e-mail is sent to the subject requesting their consent, indicated by a ticked checkbox in the CRM. Reminder e-mails may also be sent. If consent is granted, this is recorded with a second ticked checkbox. If the subject does not respond by granting consent within a set period, their details will be automatically deleted from the system.

ii) Pre-existing consent: If the subject has already granted consent, this is recorded in the system in the same way (double tick), together with details of how the consent was granted.

Once granted, the consent remains valid until it expires, or until withdrawn by the subject. Data subjects are sent automatic reminders to renew their consent before it expires. The consent will then either be renewed or the subject's data deleted, depending on the response.

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

Whose personal data are being processed?

FRA staff ☐

Non-FRA staff (persons whose data is stored in the FRA CRM: FRA's stakeholder groups and FRA internal bodies like Data Protection Authorities, Equality Bodies, FRANET, Fundamental Rights Platform, National Human Rights Institutes, National Liaison Officers, National Parliamentary Focal Points, FRA Management Board, and Scientific Committee, media, academics, students, and any other category of person wishing to receive information about the Agency's activities, etc,) ☒

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

Please tick all that apply and give details where appropriate

(a) **General personal data (add or delete as appropriate – the data in the brackets are only examples)**

Personal details (name, surname, salutation) ☒

Contact details (postal address, email address, telephone number, social media contact information) ☒

Education & Training details ☐

Employment details (job title, organisation) ☒

Financial details (e.g. financial identification form, bank account information) ☐

Family, lifestyle and social circumstances ☐

Goods or services provided ☐

Other (please give details): Preferences regarding the thematic areas of the Agency's work about which the data subject wishes to receive information, e.g. Roma, data protection, LGBTI, migration, etc. ☒

Emails are sent via Flowmailer, an SMTP relay service to which emails are directed before they can be sent on to the final recipient. In the process recipient email addresses are stored in Flowmailer to ensure that emails are sent correctly and are not marked as spam. Flowmailer stores the date and time the email was sent, the email from and to address, the delivery status as well as the subject and text of the email.

(b) **Special categories of personal data** (Article 10)
The personal data collected reveal:

Racial or ethnic origin ☐

Political opinions ☐

Religious or philosophical beliefs ☐

Trade union membership ☐

Genetic, biometric or data concerning health ☐

Information regarding an individual's sex life or sexual orientation ☐

N/A ☒

(c) **Personal data relating to criminal convictions and offences** (Article 11)

Criminal record (or similar, e.g. declaration of good conduct) ☐

N/A ☒

6) Recipient(s) of the data (Article 31.1 (d))

*Recipients are all parties who have access to the personal data. Who will have access to the data **within** FRA? Who will have access to the data **outside** FRA? No need to mention entities that may have access in the course of a particular investigation (e.g. OLAF, EO, EDPS).*

Designated **FRA** staff members
Data can be accessed by authorized FRA staff, SNEs or trainees handling contact data stored in the CRM. ☒

Recipients **outside** FRA: ☒
Data can be accessed by authorized staff members of the Agency's web development contractor

Flowmailer service provider. All data processed by Flowmailer is safely stored in independently functioning Dutch data centers (Amsterdam region). Customer data therefore never leaves the European Union.

7) Transfers to third countries or international organisations (Article 31.1 (e))[6]

If the personal data are transferred outside the European Economic Area or to international organisations, this needs to be specifically mentioned, since it increases the risks of the processing operation.

Transfer outside of the EU or EEA

Yes ☐

No ☒

If yes, specify to which country:

Transfer to international organisation(s)

Yes ☐

No ☒

If yes specify to which organisation:

Legal base for the data transfer

[6] **Processor** in a third country using standard contractual clauses, a third-country public authority you cooperate with based on a treaty. If needed, consult your DPO for more information on how to ensure safeguards.

☐ Transfer on the basis of the European Commission's adequacy decision (Article 47)

☐ Transfer subject to appropriate safeguards (Article 48.2 and .3), specify:

a) ☐ A legally binding and enforceable instrument between public authorities or bodies.

Standard data protection clauses, adopted by

b) ☐ the Commission, or

c) ☐ the European Data Protection Supervisor and approved by the Commission, pursuant to the examination procedure referred to in Article 96(2) .

d) ☐Binding corporate rules, ☐ Codes of conduct , ☐ Certification mechanism pursuant to points (b), (e) and (f) of Article 46(2) of Regulation (EU) 2016/679, where the processor is not a Union institution or body.

Subject to the authorisation from the European Data Protection Supervisor:
☐ Contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation.

☐ Administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

☐ Transfer based on an international agreement (Article 49), specify:

Derogations for specific situations (Article 50.1 (a) –(g))

☒ N /A
☐ Yes, derogation(s) for specific situations in accordance with article 50.1 (a) –(g) apply
In the absence of an adequacy decision, or of appropriate safeguards, transfer of personal data to a third country or an international organisation is based on the following condition(s):

☐ (a) The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards
☐ (b) The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request
☐ (c) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person
☐ (d) The transfer is necessary for important reasons of public interest
☐ (e) The transfer is necessary for the establishment, exercise or defense of legal claims
☐ (f) The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent
☐ (g) The transfer is made from a register which, according to Union law, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in Union law for consultation are fulfilled in the particular case

8) Retention time (Article 4(e))

How long will the data be retained and what is the justification for the retention period? Please indicate the starting point and differentiate between categories of persons or data where needed (e.g. in selection procedures candidates who made it onto the reserve list vs. those who didn`t). Are the data limited according to the adage "as long as necessary, as short as possible"?

Contact information is stored until the contact requests to unsubscribe from one or more mailing lists, in which case the name is removed from those mailing lists only, or until they request to delete their details entirely, in which case all the details are entirely removed from the system. All e-mails the contact receives from the Agency will have the options to unsubscribe or delete their details.

FlowMailer operational logs of the service (e.g. user access logs) are kept for 30 days after retention time (back up process). Email metadata (such as headers and time stamps) are saved for 3 years and the entire email is saved for 1 year.

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

Please specify where/how the data are stored during and after the processing; please describe the security measures taken by FRA or by the contractor

How is the data stored?

Document Management System (DMS)	☐
FRA network shared drive	☐
Outlook Folder(s)	☐
CRM	☒
Hardcopy file	☐
Cloud (give details, e.g. cloud provider)	☐
Servers of external provider	☒

The data is stored in the CRM hosted on the servers of the FRA web hosting contractor at the latter's data centre. Access to the system is granted only to authorized staff members of the Agency and to authorized staff members of the Agency's web development contractor. All data is stored in the EU and not transferred outside the EU; the system does not track the IP addresses; cookies are enabled just for keeping the session active and deleted after the session expires; all data transmission is encrypted (using https).

The final sending of the e-mails is done by the Agency's e-mail forwarding provider (Flowmailer), an external contractor using European Commission's

SIDE II – Group S contract. The personal data stored in the CRM is not shared with this provider.

Flowmailer service provider's datacenter is located in Amsterdam, Schipol-Rijk and Haarlem. Flowmailer is ISO27001 certified and access to the tool is limited to 2 FRA staff members via using 2-factor authentication. WAN traffic is encrypted by general-purpose hardware, with specialised cryptographic hardware holding and protecting cryptographic keys. All encryption methods used (key exchange/establishment, peer authentication, symmetric encryption, hashing, etc.) provide effective security strength equal to or greater than 128-bit. All encryption methods used are based on identified open industrial standards. All firewalls are stateful and rules can be applied to groups of objects.

10) Exercising the rights of the data subject (Article 14 (2))

How can people contact you if they want to know what you have about them, want to correct or delete the data, have it blocked or oppose to the processing? How will you react?

See further details in the Data Protection notice: e-mail to information@fra.europa.eu

Data subject rights

☒ Right of access

☒ Right to rectification

☒ Right to erasure (right to be forgotten)

☒ Right to restriction of processing

☐ Right to data portability

☒ Right to object

☒ Notification obligation regarding rectification or erasure of personal data or restriction of processing

☒ Right to have recourse

☒ Right to withdraw consent at any time