RECORD OF PERSONAL DATA PROCESSING

*Art. 31 of the REGULATION (EU) 2018/1725 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (*henceforth the "Data protection regulation"*)*

Record nº DPO 54 -2021

In accordance with Article 31 of the data protection regulation, individuals whose personal data are processed by the Executive Agency in any context whatsoever are to be protected with regard to the processing of personal data and the Executive Agency has to keep records of their processing operations.

This record covers two aspects:
1. Mandatory records under Art 31 of the data protection regulation (recommendation: make the header and part 1 publicly available)
2. Compliance check and risk screening (initial; part 2 is internal only to the Agency, not published)

The ground for the record is (tick the relevant one):

☐ *Regularization of a data processing operation already carried out*
☐ *Record of a new data processing operation prior to its implementation*
☐ *Change of a data processing operation.*
☒ *Migration from notification to record.*

Unified Communication and Collaboration (UCC)

1	**Last update of this record if applicable**	**DPO 72-2018**
2	**Short description of the processing**	**The ERCEA relies on the Unified Communication and Collaboration (UCC) solution provided by DG DIGIT in order to ensure its mission. UCC is an integrated set of communication and collaboration tools to all Commission and Executive Agency staff. It comprises telephone facilities, video conferencing, instant messaging and document sharing facilities in a single tool. This service uses the Microsoft LYNC/SKYPE for Business (SfB) software.** **In order to provide the UCC service some handling of personal data is required. The data concerned are the minimum needed to provide and manage the service.** **The processing operations of personal data in the context of the UCC service are necessary to ensure**

		the access, the proper use and management of Commission and ERCEA resources in carrying out efficiently its duties. In this instance it is necessary for ensuring that the Agency's staff has access to the effective communication and collaborative working facilities.
(This part may be public) **Part 1 - Article 31 Record**		
3	**Function and contact details of the controller**	Function: **Head of Unit** Unit : **ERCEA D1** e-mail address: **ERC-IRM@ec.europa.eu**
4	**Contact details of the Data Protection Officer (DPO)**	Functional e-mail address **ERC-DPO@ec.europa.eu**
5	**Name and contact details of joint controller (where applicable)**	**N/A**
6	**Name and contact details of processor (where applicable)**	**DIGIT C5** **DIGIT-C5@ec.europa.eu**
7	**Purpose of the processing**	**UCC provides an integrated set of communication and collaboration tools to all Commission and Executive Agencies staff. It comprises telephone facilities, video conferencing, instant messaging and document sharing facilities in a single tool, based on the Microsoft LYNC/SKYPE for Business (SfB) software.** **The ERCEA's previous communications infrastructure (based essentially on wired telephony) had to be upgraded due to gradual obsolescence, increasing support costs and inability to support modern working methods and service needs. All major organisations have been moving from traditional dedicated cable-based telephony to UCC type facilities based on computer networks for many years already. At the Commission and Executive Agencies apart from the need to be able to support in a cost efficient way new services such as instant messaging, personal videoconferencing, etc., there is also a very significant cost advantage in not having a separate cabling infrastructure for telephony: which is one of the reasons why OIB/OIL now provide new buildings with the requisite UCC infrastructure rather than the old telephony cabling and older buildings, if any, will be progressively adapted.** **In order to provide the UCC service some handling of personal data is required. The data concerned are the minimum needed to provide and manage the service.** **The processing operations on personal data in the context of the UCC service are necessary to ensure the proper use and management of Commission and ERCEA resources in carrying out efficiently its duties.**

		In this instance it is necessary for ensuring that the Agency's staff has effective communication and collaborative working facilities. **For this reason, a set of personal data of each staff member is processed in order to configure and operate the UCC solution. The configuration is done automatically by DIGIT services whenever a staff member joins the ERCEA. The newcomer username is given access to the UCC software and the information from Outlook are synchronized whenever the newcomer perform the first logon on the corporate laptop.** **The personal data that may be handled in UCC consists of:** • **Login/userID** • **Name & Surname** • **Email address (office)** • **Contact details – office telephone number, office address** • **Location - a free text field that by default is empty but a user may choose to enter a value. If a value is entered it is stored with user details and the user can choose to have it visible (or not) to other users. It is not used for any other purpose.** • **Calendar information (from Outlook) – meeting details , availability** • **Usage details of Communications (video/audio/messaging) e.g. start time of call, end time of call** • **External call details for billing purposes (number called, duration)** • **Call details: each communication generates automatically the following data fields which are stored temporarily.** o **User SIP URI (identifies the From & To users)** o **Communication type i.e. IM, voice, video, telephone** o **Communication start & end date & time** o **Technical details relating to technical quality of the communication** o **Telephone numbers – the From and To numbers are stored.** • **Recordings (optional for meeting/conference organisers). Audio/Video meetings may be recorded if the organiser chooses (in this case the participants are automatically informed that recording will take place). The actual recordings are stored on the PC of the organiser and are under his/her exclusive control.** • **IM Conversation details (i.e. content of the messages exchanged) in instant messaging**

		(stored like emails in the individual users Outlook) • **Current availability for communication purposes status information (e.g. busy/away/in a call/offline since etc). This status is available only in real-time and intended to show colleagues if a user is available to communicate directly with at this moment. Only the last known status is stored. E.g. the system can indicate that a user is on-line and free to communicate now, or that they are busy or have been offline for three days for example. Availability statuses include Available, Busy, Away, Do Not Disturb and Offline. Status is based on information in Microsoft Outlook Calendar or UCC activities and it can also be set manually by the user.** • **Technical logging of system information for technical support purposes takes place. These logs do not contain the content of messages or communications.**
8	**Description of the categories of data subjects**	☒ EA staff (Contractual and temporary staff in active position ☐ Visitors to the EA ☒ Contractors providing goods or services ☐ Applicants ☐ Relatives of the data subject ☐ Complainants, correspondents and enquirers ☐ Witnesses ☐ Beneficiaries ☐ External experts ☒ On Site Contractors ☐ Other, please specify _____

9	**Description of personal data categories** Indicate **all** the categories of personal data processed and specify which personal data are being processed for each category (between brackets under/next to each category):	*Categories of personal data:* ☒ in the form of personal identification numbers Staff usernames ☒ concerning the physical characteristics of persons as well as the image, voice or fingerprints User picture and recorded voicemails saved in user mailbox ☐ concerning the data subject's private sphere ☐ concerning pay, allowances and bank accounts ☐ concerning recruitment and contracts ☐ concerning the data subject's family ☐ concerning the data subject's career ☐ concerning leave and absences ☐ concerning missions and journeys ☐ concerning social security and pensions ☐ concerning expenses and medical benefits ☒ concerning telephone numbers and communications ☒ concerning names and addresses (including email addresses) ☐ Other :please specify :_____ *Categories of personal data processing likely to present <u>specific risks:</u>* ☐ data relating to suspected offences, offences, criminal convictions or security measures ☐ data being used to evaluate personal aspects of the data subject (ability, efficiency, conduct) *Categories of personal data whose processing is <u>prohibited</u>, with exceptions (art. 10 new Regulation):* ☐ revealing racial or ethnic origin ☐ revealing political opinions ☐ revealing religious or philosophical beliefs ☐ revealing trade-union membership ☐ concerning health ☐ genetic data, biometric data for the purpose of uniquely identifying a natural person ☐ concerning sex life or sexual orientation *Specify any additional data or explanatory information on the data being processed, if any:*
10	**Retention time (time limit for keeping the**	**Data are retained for a period of 6 months. Traffic data**

	personal data)	**concerning external telephone calls (for billing purposes) are transferred to GESTEL where the period foreseen by that processing operation applies (see EC DPO-832). Audio/video recordings made by meeting organisers are stored by each organiser and are under their exclusive control.** In case you intend to FURTHER process the personal data for a compatible purpose with the 'initial' one, please also indicate this retention period if different Is any further processing for archiving purposes in the public interest, historical, statistical or scientific purposes envisaged? ☐ yes ☒ no If yes, indicate the further retention time: … If the answer is yes, please go to Part 2 Compliance check, Storage and Security for technical safeguards.
11	**Recipients of the data**	**Technical engineers at DIGIT C5 who will need to troubleshoot any communication issue via UCC. The access will be on the metadata of the communication, not on the content of the latter.** **GESTEL for external traffic data analysis (billing purposes). The access will be granted for metadata of calls and not the content of call.** **<u>Comments/additional information on data recipients:</u>** **Availability for communication status:** **All users of the UCC system can see current/last status (i.e. available/not available/offline since etc.) of other connected users (internal to the Commission and Executive Agencies only but teleworkers included when connected from outside on Commission provided PCs).** **Traffic data concerning external telephone calls (for billing purposes) are transferred to GESTEL (see EC DPO-832).** **For purposes of system support, service administration, incident management and user assistance the relevant technical teams within DIGIT Directorate C and their possible subcontractors have controlled access to all system data stored. They can access log files, usage reports and investigate issues for a specific user. These recipients however have no access to the contents of message or communications or to recordings made and stored by the users themselves.**
12	**Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?**	**NO** **<u>Comments:</u>** **Under very rare circumstances extracts of technical logs for specific debugging purposes may be provided to external companies under contract to the Commission. It cannot be guaranteed that some of this debugging work will not involve transfers outside of the UE/EEA. In such cases all possible care is taken to ensure anonymization of any personal data that may be contained therein. Technical logs contain essentially technical information linked to the**

		establishment of communication calls (IM, Audio, Video), quality indicators, and error messages which help in the identification and resolution of problems on the UCC service. The external companies are contractual suppliers of the Commission that deliver specific support services (e.g. Microsoft) and are bound by the specific provisions included in the contract.
13	**<u>General</u> description of the technical and organisational security measures**	**Access Control System implemented to avoid errors in mistakenly disclosing of personal data to unauthorized people.** **The members of authorized people are reviewed on a frequent basis (due to possible turnover and change of roles), ensuring only current people with a need to know basis have the access rights.** **Lync/Skype for Business communication use TLS for client -server communication (voice call), instant messaging, web conferencing and desktop sharing.** **Server-to-Server is protected by MTLS.** **Audio, video and desktop sharing of media is protected by SRTP.** **Meeting content download is protected by HTTPS.**
14	**Information to data subjects/Specific Privacy Statement (SPS)**	**The data protection notice (DPN) is made available on the ERCEA Intranet.**