European Research Council
Executive Agency

Established by the European Commission

# 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 52-2021

*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.*

| **Name of the processing operation**<br>**Telephony and PDA service of the ERCEA** | | |
|---|---|---|
| **1** | **Last update of this record if applicable** | DPO 29-2012 [Ares(2012)877105] |
| **2** | **Short description of the processing** | Since the introduction in ERCEA of the Unified Communication & Collaboration (UCC) solution, which is covered by DPO 54-2020, the traditional phones on users desks have been replaced with a software solution.<br><br>The remaining services that are linked to the telephone network are: conference call hardware equipment installed in meeting rooms, corporate smartphones (PDAs) allocated to staff members for fully justified reasons, emergency phones in strategic locations like elevators or stairs. |

| (This part may be public)<br>**Part 1 - Article 31 Record** | | |
|---|---|---|
| **3** | **Function and contact details of the controller** | Function: **Head of Unit**<br>Unit : **ERCEA D1**<br>e-mail address: erc-irm@ec.europa.eu |
| **4** | **Contact details of the Data Protection Officer (DPO)** | Functional e-mail address<br>**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)** | **DG DIGIT**<br>**DIGIT-DPC@ec.europa.eu (Data Protection Coordinator)** |
| **7** | **Purpose of the processing** | Since the introduction in ERCEA of the Unified Communication & Collaboration (UCC) solution, which is covered by DPO 54-2021, the traditional phones on users desks have been replaced with a software solution.<br><br>The remaining services that are linked to the telephone network are: conference call hardware equipment installed in meeting rooms, corporate smartphones (PDAs) allocated to staff members for fully justified reasons, emergency phones in strategic locations like elevators or stairs.<br><br>Minimal personal data are processed only to provide Telephone equipment to the Data Subjects and allow the management of the Telephone infrastructure, network and system to provide the necessary service.<br><br>Corporate smartphones are assigned to:<br>• Management (Heads of Unit, Heads of Department, Director, Chief Accounting officer).<br>• Key users who, because of their functions are in the obligation to liaise rapidly or frequently with their working environment.<br><br>DIGIT is responsible for the physical allocation and the configuration of ERCEA smartphones after approval of the ERCEA IRM (Information Resource Manager).<br><br>For the fixed telephony service (including audio conferencing), the processing operation is, basically, to format the data in a way that service usage could be easily evaluated.<br><br>ERCEA is using DG DIGIT solutions for all services linked to the telephone network. ERCEA staff members are the customers of the services, whereas DG DIGIT is the service provider.<br><br>It is not a purpose of the processing to evaluate personal aspects of the Data Subjects and/or their conduct but only of technical aspects. Personal data will not be used for an |

| | | |
|---|---|---|
| | | automated decision-making including profiling. |
| **8** | **Description of the categories of data subjects** | Whose personal data are being processed?<br>In case data categories differ between different categories of persons, please explain as well (e.g. suspects vs. witnesses in administrative inquiries)<br><br>☒ EA staff (Contractual and temporary staff in active position<br><br>☐ Visitors to the EA<br><br>☐ Contractors providing goods or services<br><br>☐ Applicants<br><br>☐ Relatives of the data subject<br><br>☐ Complainants, correspondents and enquirers<br><br>☐ Witnesses<br><br>☐ Beneficiaries<br><br>☐ External experts<br><br>☐ On Site Contractors<br><br>☒ Other, please specify: any participant in a conference call that is being recorded_____ |
| **9** | **Description of personal data categories**<br><br>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:*<br><br>☒ in the form of personal identification numbers<br><br>Usernames<br><br>☒ concerning the physical characteristics of persons as well as the image, voice or fingerprints<br><br>Voice in case of videoconference recorded<br><br>☐ concerning the data subject's private sphere<br><br>☐ concerning pay, allowances and bank accounts<br><br>☐ concerning recruitment and contracts<br><br>☐ concerning the data subject's family<br><br>☐ concerning the data subject's career<br><br>☐ concerning leave and absences<br><br>☐ concerning missions and journeys<br><br>☐ concerning social security and pensions<br><br>☐ concerning expenses and medical benefits |

| | | |
|---|---|---|
| | | ☒ concerning telephone numbers and communications<br><br>Office phone number or corporate mobile phone number<br><br>☒ concerning names and addresses (including email addresses)<br><br>Office email address<br><br>☒ Other :please specify : Call date and time, call duration, communication cost, voice-mail messages<br><br>All personal data parameters come from the technical function of the service , which allows the establishment of the connection or the duration of the call decided by the user. In case of Mobile phone calls, the personal data (Calling number, Called number, Call date and time and Call duration) come from the contractor via electronic files.<br><br>*Categories of personal data processing likely to present <u>specific risks:</u>*<br><br>☐ data relating to suspected offences, offences, criminal convictions or security measures<br><br>☐ data being used to evaluate personal aspects of the data subject (ability, efficiency, conduct)<br><br>*Categories of personal data whose processing is <u>prohibited</u>, with exceptions (art. 10 new Regulation):*<br><br>☐ revealing racial or ethnic origin ☐<br>revealing political opinions ☐<br>revealing religious or philosophical beliefs ☐<br>revealing trade-union membership ☐<br>concerning health ☐<br>genetic data, biometric data for the purpose of uniquely identifying a natural person ☐<br>concerning sex life or sexual orientation<br><br>*Specify any additional data or explanatory information on the data being processed, if any:* |
| **10** | **Retention time (time limit for keeping the personal data)** | - Data (name, surname, phone n°, office address) that are necessary for the operation of the telephone system are kept and used as long as the data subject is the "owner" of the phone number and uses the ERCEA phone services.<br><br>- Data concerning calls of the current month + the 6 previous months are stored in the Database and are visible to the Data Subject via the eGestel application.<br><br>- For the MDM service, the information is collected at enrolment and only kept for as long as the device is active/ registered.<br><br>- The log files are kept for 90 days that is a balance between being able to analyse incidents and not keeping logs files too long.<br><br>Is any further processing for archiving purposes in the public interest, historical, statistical or scientific purposes |

| | | |
|---|---|---|
| | | envisaged?<br>☐ yes ☒ no<br><br>If yes, indicate the further retention time: …<br><br>If the answer is yes, please go to Part 2 Compliance check, Storage and Security for technical safeguards. |
| **11** | **Recipients of the data** | Data Subjects have access to all their information via eGestel. The eGestel application is an EU Login protected application and can only be accessed by the Data Subject after entering his/her EU Login password.<br><br>Officials and external engineers working in unit DIGIT C3 - CUPS, in the telephony service, on a need-to-know basis.<br><br>Access to personal data is provided to the Commission staff responsible for carrying out this processing operation and to authorised staff according to the "need to know" principle. Such staff abide by statutory, and when required, additional confidentiality agreements.<br><br>The external contractor is PROXIMUS SA, PLC under Belgian Public Law, Boulevard du Roi Albert II, 27B – 1030 Brussels. The information originating from the external contractor, is disclosed to EC Staff on a need to know basis, exclusively for the purposes of the performance, management and monitoring of the Contract.<br><br>The final recipient is the Agency; however, for the processing operation on mobile devices only, the contractor would be the initial recipient of some personal information (Calling number, Called number, Call date and time, Call duration, calling number list and Voice mail list) which are not user-identifiable. Fixed telephony is not treated by the contractor. |
| **12** | **Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?** | **NO** |
| **13** | **General description of the technical and organisational security measures** | All personal data in electronic format are stored either on the servers of the European Commission and its Contractor based on its service. The contractor stores only the data needed for the mobile telephony service invoicing (Mobile Calling number, Called number, Call date and time, Call duration, calling number list and Voice mail list). All processing operations are carried out pursuant to the Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission, and its subsequent update.<br><br>The Commission's contractors are bound by a specific contractual clause for any processing operations of the data on behalf of the Commission, and by the confidentiality obligations deriving from the transposition of the General Data Protection Regulation in the EU Member States ('GDPR' Regulation (EU) 2016/679)<br><br>In order to protect the personal data, the Commission has |

| | | |
|---|---|---|
| | | put in place a number of technical and organisational measures in place. Technical measures include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised access, taking into consideration the risk presented by the processing and the nature of the personal data being processed. Organisational measures include restricting access to the personal data solely to authorised persons with a legitimate need to know for the purposes of this processing operation.<br><br>**Physical security**<br><br>Email and telephony servers are managed by DIGIT.C and are kept in their data centres. Access to these rooms is controlled and reserved to the members of the DIGIT LSA team, who must use their badge in combination with a personal PIN code.<br><br>**Logical security**<br><br>Data Subjects have access to all their information via eGestel, which is EU Login protected. PDAs are password secured, if the code is wrongly introduced more than six times the device resets erasing all data contained in it. Administrators can also remotely wipe a lost or stolen mobile device. |
| **14** | **Information to data subjects/Data Protection Notice** | The SPS for eGestel can be found on the home page of eGestel (not public).<br><br>The SPS for the MDM system can be found at point 7 of the following DPO Record https://ec.europa.eu/dpo-register/detail/DPR-EC-03608#rights |