EUROPEAN DATA PROTECTION SUPERVISOR

8 April 2020

*** This is an extract from the EDPS' personal data breach register**			
EUI	**Date of notification**	**Type of incident**	**Description**
European Medicines Agency (EMA)	20/12/2018	Confidentiality	The hard copy of a contract amendment was sent by postal mail to the incorrect recipient. It was sent to another Contractor within a separate framework contract which was concluded in the context of the same tender. The document sent erroneously included personal data related to contractor's staff members. The breach was caused due to mistakenly using an incorrect letter template, triggered by an error in the choice of contract number. The data breach was detected when the Contractor, which received the contract amendment erroneously, informed EMA of the matter.
EMA	24/01/2019	Confidentiality	Folder with HR data was duplicated without proper access restriction rights.
Innovation and Networks Executive Agency (INEA)	28/02/2019	Confidentiality	A project officer sent wrong email containing personal data of experts to a limited number of experts. Immediately recall and ask the recipients to delete it.
Executive Agency for Small and Medium-sized Enterprises (EASME)	22/01/2019	Confidentiality	During the application phase for the EUSEW Awards, due to a technical bug a user could access 7 other applications containing personal data.
EASME	01/03/2019	Confidentiality	Contractor sent wrong email with personal data to 287 project coordinators. The contact details was already information publicly available.
European Commission - DG SANTE	12/07/2019	Confidentiality	Publication on Internet of personal data of employees of ID issues in tobacco by mistake.
European Commission - DG SANTE	08/02/2019	Confidentiality	A service agreement was disclosed to a wrong recipient (3rd party). It was deleted by the recipient.

European Food Safety Authority (EFSA)	28/03/2019	Confidentiality	An EFSA staff member sent an email reminder to complete online application to potential candidates for an EFSA recruitment (using cc instead of bcc) - revealing the email address of all candidates among them.
European Asylum Support Office (EASO)	24/07/2019	Confidentiality	In a recruitment procedure, an email sent to all (100) non-shortlisted candidates with use of cc instead of bcc.
SESAR Joint Undertaking	20/12/2018	Confidentiality	Email unintentionally sent with an email with an attachment containing the evaluation grid (covering a quantitative assessment of knowledge, experience and interpersonal skills, as well as a qualitative assessment of the performance of the candidates) within the frame of a Recruitment/selection procedure involving 14 candidates. The recipient of the email is a lawyer that has been contracted by the SJU in the past, and who still has contacts with the SJU for a different purpose not covered by the scope of the present data breach. The recipient confirmed having deleted the email received as per the request of the SJU.
Education, Audiovisual and Culture Executive Agency (EACEA)	19/12/2018	Confidentiality	An online tool managed by EACEA and used by their beneficiaries, for submitting final reports for their grant agreements had a malfunction. More specifically, due to a technical failure of this tool, reports concerning one beneficiary could be accessed by another beneficiary. This incident that EACEA initially notified in December 2018, was repeated in February 2019 when EACES submitted the follow-up notification. In a conclusive notification in July 2019 EACEA concluded that the incident occurred only exceptionally and under specific technical circumstances and concerned four reports out of approximately 4.700 final Interim reports. The Agency took measures to address this issue including the release of a new version of the tool.
EACEA	21/01/2019	Availability	Legal and other documents of staff related with articles 24 and 90 of the Staff Regulations, available on a shared network drive with restricted permissions were missing (empty folder) for a short period.

EACEA	25/01/2019	Confidentiality	On 24/01/2019 the operational unit EACEA.B2 informed the DPO about the erroneous upload from REA Validation Services since 2014 on the Participants Portal (a EU dedicated website managed by REA) of the wrong documents and the potential disclosure of information. In the conclusive notification and after careful analysis, it has been confirmed by REA that no third party could access the documents.
European GNSS Agency	29/03/2019	Confidentiality	In the context of a mobile app competition, an email notification was sent by a contractor accidentally to all participants making their email visible. This was detected by the officer of the GNSS Agency.
European Chemicals Agency	17/01/2019	Confidentiality	HR officer unintentionally sent an email with an attachment containing performance appraisal documents of two persons to the HoU and put in copy one of the persons . 9 documents of the other person were included in the email.
EUIPO	27/06/2019	Availability	Technical issue where the photos of the staff (10%) were not transferred properly to the directories. The issue was resolved with the manual transfer of photos. No personal data breach final assessment.
EUIPO	31/07/2019	Confidentiality	Web service had a bug that left the selective publication on one database of contact information of their representatives while they have not authorised it.
European Union Agency for Fundamental Rights (FRA)	25/01/2019	Confidentiality	Career development report of one staff member under Career Development Review (CDR) has been accessible to unauthorized users (internal staff) for a few hours.
EUROPOL	11/12/2018	Confidentiality	Accidental sent of email containing logs that were not fully sanitized and contained three names of suspects. The breach was immediately identified (7 minutes after the email has been sent) The email was deleted by the recipient. [redacted]
EUROPOL	26/02/2019	Confidentiality	Medical results of 2 staff members were mistakenly sent (mixed up). Contractor.
The Council	13/12/2018	Confidentiality	A German security company that was not authorized by the GSC, has detected a vulnerability by using the guest account feature of the Council App (an application that can be installed on Android or Apple smartphones and tablets) and reported this

			to CERT-Bund. CERT-Bund notified CERT-EU. CERTEU has forwarded this to the Network Defense Capability (NDC) of the General Secretariat of the Council of the European Union (GSC). As soon as NDC became aware of this vulnerability, it took the necessary steps for containment and minimizing the effects. Based on the examination, there is no evidence of exploitation of the vulnerability to extract personal data from the backend service.
Research Executive Agency (REA)	01/04/2019	Confidentiality	Initially not sure whether this was a data breach. REA candidates reimbursement online procedures. DG DIGIT informed REA on 29 March that some documents containing personal data could be accessed online. Finally it was verified that no breach has taken place.
European Commission - PMO	18/03/2019	Confidentiality	The spouse of a JSIS affiliate received the invitation for an annual medical check intended for another affiliate.
European Commission - PMO	24/05/2019	Confidentiality	On 21.05.2019, a case handler of PMO for pensions, communicated by e-mail to a wrong recipient the decision granting entitlement to a retirement pension as well as the details of the amounts of this pension (specified by the notice of assessment of entitlements to a pension) and the details of the calculations of this pension. The e-mail was sent to a private e-mail address of a pensioner of the Commission, through the ARES Mail Registration system of the Commission. The unintended recipient who received the mail on his "Gmail address", informed the case handler on 16:48 the same day, that these documents concerned another person. It appeared that the data subject and the wrong recipient had the same first name, only the surnames were different.
European Commission - PMO	26/07/2019	Confidentiality	Email including the decision granting entitlement to a family and child allowances was sent to wrong recipient (another pensioner of the Commission).
European Commission - DG DEVCO	11/04/2019	Confidentiality	Following a request for access to documents under regulation 1049/2001 by AskThe EU platform, DG DEVCO replied by sending a document (minutes of a meeting of April 2018) that included more personal data than necessary (sensitive data political

			opinion) and this document was published to the AskThe EU Platform. It was further analysed that no high risk for the data subjects was caused.
European Commission - DG HR - DDG A3	29/04/2019	Confidentiality	HR Reporting services - one EACEA staff member asked for a report of the list of staff of his Agency - the result report included other names. The reporting team fixed the issue.
European Commission - DG JUST	12/07/2019	Confidentiality	Inclusion of personal data in a public consultation file on the Internet. It was later verified that the persons have consented for this publication (not opted out for anonymous).