From: EDPS-REG-TECH-PRIVACY <edps-reg-tech-privacy@edps.europa.eu>

To: [redacted]

CC:

Sent at: 14/03/22 13:02:01

Subject: C 2020-0336 - D(2022) 0673

Dear [redacted]

Please find attached, for your attention, a letter signed by [redacted] Acting Head of Unit Technology and Privacy - concerning the case in reference: Conclusions on Personal Data Breach Notification of 18 March 2020.

This letter is encrypted. The password will be provided to you either in a separate mail or by phone.

Kind regards,

EDPS Technology and Privacy Secretariat

| Tel. (+32) 228 31900 | Fax +32(0)22831950 | › Email edps-reg-tech-privacy@edps.europa.eu
European Data Protection Supervisor
Postal address: Rue Wiertz 60, B-1047 Brussels
Office address: Rue Montoyer 30, B-1000 Brussels
@EU_EDPS www.edps.europa.eu

ZIP Archive with 1 entry

D(2022)+0673+C+2020-0336_Closure+Letter+Ms+Mapelle.pdf

EUROPEAN DATA PROTECTION SUPERVISOR

TECHNOLOGY AND PRIVACY UNIT
Acting Head of Unit

[redacted]
European Court of Auditors
12, rue Alcide de Gasperi
L - 1615 Luxembourg

By encrypted email only
[redacted]

Brussels, 14 March 2020
[redacted] D(2022) 0673 **C 2020-0336**
Please use edps-reg-tech-privacy@edps.europa.eu for all correspondence

Subject: Conclusions on Personal Data Breach Notification of 18 March 2020

Dear [redacted],

We are writing in response to the personal data breach notification you have submitted to the European Data Protection Supervisor (EDPS) on 18 March 2020 (Case-File 2020-0336). As the notification was done in phases according to Article 34(4) of the Regulation (EU) 2018/1725, you submitted additional information on 22 October 2020 and 09 September 2021. We would like to thank you for the above notification and provide you with our feedback. Please accept our apologies for the delay in replying to you.

The personal data breach you notified us concerned a case where the Office for Administration and Payment of Individual Entitlements (PMO), acting as European Court of Auditor (ECA)'s processor erroneously communicated an ECA staff member's salary details to her ex-spouse. This led to a court dispute between her and her ex-spouse, who, allegedly, used the disclosed personal data causing financial loss. The personal data breach was caused by human error, due to a misinterpretation of the Staff Regulations[1].

[1] Regulation No 31 (EEC), 11 (EAEC), laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Economic Community and the European Atomic Energy Community

The personal data breach notification you submitted contains all the necessary information required by Article 34(3) of Regulation (EU) 2018/1725.

Under Article 34(1) of Regulation (EU) 2018/1725, the controller must notify the EDPS "without undue delay" and "no later than 72 hours after becoming aware of the personal data breach". The EDPS did not receive the notification within the above deadline. We would like to point your attention to the fact that we received the notification approximately 8 days after the detection date of the incident, due to delays in receiving additional information from the processor and DPO's absence. Data breach notifications are a responsibility of the controller, who must ensure the existence of an effective internal data breach notification process, accounting, among others, for immediate collaboration with any processors and for ensuring the assessment of the breach and notification does not rely on a single person. If not all relevant information is available to you within 72 hours you should provide us with a notification in phases as laid down in Article 34(4) of Regulation (EU) 2018/1725 to ensure a quick response to such incidents, to mitigate any risks and fulfil the controller's obligation for timely notification to the EDPS.

We take note of the fact that the data protection officer (DPO) notified the incident and, therefore, was informed. We also acknowledge that you documented the personal data breach, including its facts and its effects to the data subjects concerned and you took immediate measures, by contacting your processor.

You have assessed that the personal data breach resulted in a high risk to the rights and freedom of the data subject taking into account the nature of the personal data breach, the nature and amount of data. In this specific case, you did not inform the data subject as she was already aware of the incident and informed the controller. Moreover, the risk had materialised as the personal data was used in a court dispute. **The EDPS agrees with your risk assessment.**

To avoid similar incidents in the future, the EDPS proposes the below additional measures (if not yet implemented):

1. Revisit the service level agreement with PMO as to the requirements/instructions on the processing of personal data by the PMO on ECA's behalf. Personal data protection and data minimization should be provisioned in the SLA.
2. Seek (regular) feedback about the implementation of these instructions, including asking PMO to review the respective processes and provide staff with examples of common mistakes resulting in personal data breaches, such as providing information to wrong recipients.

In general, we also propose to establish a program of regular awareness raising to involved staff members, with a goal to explain the sensitivity of the involved personal data categories and to avoid common mistakes in the process especially with the use of communication technologies (such as email, SMS etc).

To conclude, the EDPS considers that, apart from not respecting the deadline of the notification to the EDPS, you have taken adequate measures in the context of this personal data breach.

Consequently, there appears no need for further intervention from our side. We will therefore close the case. This is without prejudice of possible future supervisory actions the EDPS might wish to undertake.

Should you require additional information, please do not hesitate to contact [redacted]

Yours sincerely,

[e-signed]

[redacted]