EUROPEAN DATA PROTECTION SUPERVISOR

PERSONAL DATA BREACH NOTIFICATION – ASSESSMENT FORM

EDPS Case number: 2023-1230 EUROPEAN OMBUDSMAN 24-11-2022 COMPREHENSIVE

TP Case officer: [redacted]

TP Backup case officer: [redacted]

S&E case officer:

Assessment starting date: 24/11/2022

☒ The breach has been included in the personal data breach registry.

A complainant received a reply that among the requested documents included by a human error a document of another complainant revealing also sexual orientation. However this information was already made publicly available by the data subject in several public platforms.

D.2 Security criteria affected I. Confidentiality

The referenced document is the EDPS Data breach management Case Manual.

1. Is the breach, as described by the data controller, a personal data breach? (Reg. 2018/1725 Art. 3(16), 34(1), 34(2) and case manual 4.1)

   ☐ Yes ☐ No

2. Date of the acknowledgment of receipt (case manual 4.3): 21/12/2022

3. Did the controller notify the personal data breach within the 72 hours deadline? (Reg. 2018/1725 Art. 34(1), 34(2) and case manual 4.2)

   ☒ Yes ☐ No

   If not, are there reasonable arguments in the notification for the delay?

   ☐ Yes ☐ No

   Controller argument summary:

   Case officer reasoning:

   Does the notification contain the minimum required information? (Reg. 2018/1725 Art. 34(3), 34(4) and case manual 4.4)

   ☒ Yes ☐ No ☐ Phased

   Missing requirements:

   ☐ a description of the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned
   ☐ name and contact details of the DPO
   ☐ a description of the likely consequences of the personal data breach

   ☐ a description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects on individuals.

4. Did the data controller inform the Data Protection Officer? (Reg. 2018/1725 Art. 34(5))

   ☒ Yes, according to the D.7 field of the notification form.

   ☐ Yes, the DPO was in copy of the emails the EDPS received regarding the data breach.

   ☐ Yes. Other evidence:

☐ No

5. Is the information provided in the notification sufficient to assess the risk level of the data breach? (case manual 4.5)

   ☒ Yes ☐ No

   If no, which information is missing?

   The further information request was sent on:

6. The severity assessment of the data controller is ☐ high-risk ☒ risk

   The severity assessment of the case officer is ☐ high-risk ☒ risk

7. Did the controller notify the affected data subjects?

   ☒ Yes ☐ No

   If the controller notified the affected data subjects, does the notification contain the minimum required information? (Reg. 2018/1725 Art. 35(2))

   ☐ Yes ☒ No

   Missing information:

   ☐ communicate the name and contact details of the data protection officer

   ☒ describe the likely consequences of the personal data breach; (they say the outcome-the content of the complaint was revealed [redacted] but do not go further about any risks. However it is obvious to the data subject that their sexual preferences were revealed as they were the content of the complaint)

   ☐ describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects

   If the affected data subjects were not informed, does the case officer considers necessary to communicate them the data breach? (Reg. 2018/1725 Art. 35(1), 35(3), 35(4) case manual 4.8)

   ☐ Yes ☐ No

   Data subject was informed.

8. The severity of the incident is (case manual 4.6): ☒ low ☐ medium ☐ high

   Reasoning:

   ☐ There is high risk for the individuals

   ☐ The number of individuals concerned is particularly high

   ☐ A significant number of persons outside the EUI is affected

   ☐ The incident has received an echo in the media.

   ☒ Other reasons: While this error revealed the sexual preferences of the other complainant to [redacted] this was something that he had manifestly made public through his twitter account. The same was with the fact that he had complained about the European Commission not starting an infringement case after their complaint. An ad ditional risk would be for [redacted] to publish this information along with the data subjects'address, so that they would receive unwanted mail or even threatening visits to their house. However, given the fact that [redacted] confirmed deletion of the erroneously received data, the likelihood if this risk seems very low.

   Line to take and proposed course of action (case manual 4.7):

   LTT proposed for:

☐ For the HoU ☐ For the Supervisors

Does the case officer deems it necessary to communicate the data breach to the public (case manual 4.7)?

☐ Yes ☒ No

Reasoning: Data subject was informed.

Proposed course of action for replying to the controller:

☒ Close the case.

☐ Require the data controller to inform the DPO.

☐ Require the data controller to communicate the data breach to affected data subjects.

☐ Other actions: Wait for conclusive information

9. If a follow up is needed or expected, the actions should be (case manual 4.9):