Subject: Data Incident – GLA Response

Report to:	**GLA Oversight Committee**
Report of:	**Executive Director of Strategy and Communications**
Date:	**28 September 2023**
Public Access:	**This report will be considered in public**

1. Summary

1.1 This paper sets out the reasons for, and the Greater London Authority's (GLA) response as data processor, to the data security incident relating to two Mayor's Office for Policing and Crime (MOPAC) webforms hosted on the GLA London.gov.uk website. It includes actions taken when the incident was discovered and further actions taken as a result of the incident.

1.2 MOPAC, as the data controller, led on supporting the 392 individuals notified as a result of the incident. The Police and Crime Committee (PCC) heard directly from MOPAC's Chief Executive and the GLA's Chief Officer at their meeting of the 19 July 2023. MOPAC are updating PCC members separately on the latest position on contact from individuals notified and of take-up of support offered.

2. Recommendation

2.1 **That the Committee notes the Greater London Authority's response to the data incident.**

3. Background

3.1 The GLA responded to a data security incident about information collected by two webforms hosted on the GLA's website between 11 November 2022 and 23 February 2023. The two online forms affected were: one used to enable members of the public to contact MOPAC about issues relating to victims; the other to contact MOPAC's police complaints review team.

3.2 A new version of the GLA London.gov.uk website was launched on 31October 2022 after a comprehensive and robust redevelopment process beginning in summer 2020. This aimed to:

- Review and consolidate a large number of existing GLA and partner websites.

- Address the issue that the version of the software on which our main websites operated was due to go out of support, which would make it more vulnerable.

3.3 This redevelopment and key technical decisions were governed by the then Digital, Data and Technology Board (DTB), the Digital Project Review Group, a workstream group and a project team. The Senior Responsible Owner for the project was the then Assistant Director of External Relations.

3.4 On 11 November 2022, less than two weeks after the launch of the website, a MOPAC employee noticed that the webform submissions, hosted on the GLA website, were not automatically being sent through to those who needed to process them, as had previously taken place. Access to content submitted through webforms is controlled through the configuration of permission settings in the software, so the permissions were changed by a member of the GLA's Digital team at this point to address this. Unfortunately, the wrong permissions were selected, directly causing the problem which created the incident.

3.5 The configuration error in the permissions settings made it technically possible for a visitor to the two webforms on London.gov.uk, to find and click a button, allowing them to view the content of submissions made via those webforms.

3.6 The employee responsible believed the permissions meant information could only be seen internally and had not realised the information could potentially be accessed and viewed publicly. The manual nature of the configuration error was not identified and would not have been identified by the tools that the GLA has in place which monitor for cyber security incidents.

3.7 The GLA was alerted to the configuration error by a MOPAC employee on 23 February 2023, upon discovering that it was possible for the webform data to be accessed and viewed publicly. The configuration error was corrected within minutes after being discovered. An immediate review of all webforms hosted on the GLA website was conducted. No other webforms were found to have the permissions configuration error save for the two forms mentioned at 3.1 above. The GLA's content management system was also immediately changed to prevent any recurrence of the configuration error.

3.8 MOPAC, as data owners notified the Information Commissioner's Office (ICO) within 72 hours, as is legally required in law.

3.9 The GLA engaged independent technical specialists to investigate and identify whether any information had been misused. There is no evidence that the data has been maliciously accessed or misused.

3.10 The GLA and MOPAC commissioned a range of contracts with different experts and support organisations including;

- incident management advice
- data protection advice
- cyber security advice

4. Issues for Consideration

What lessons have been learned and what action have been taken?

4.1 There was already work underway in the GLA, led by the Information Governance team, to improve our processes before this incident occurred. Actions taken subsequently are part of the wider work on information governance, and the safety and management of the data we hold, and we have increased our investment in this area to accelerate the process.

Records management improvement

4.2 As part of the work underway, the GLA refreshed its Record of Processing Activities (ROPA). We strengthened our processes around the organisation-wide Information Asset Register to ensure we have a complete understanding of data we control, and process, for different purposes.

4.3 Almost all business units have updated their contributions to the Information Asset Register and ROPA. This work has been supported through the creation of a new Records Manager role.

4.4 Information governance arrangements between MOPAC and the GLA have been enhanced with a revised suite of agreements and risk assessments in place. We can offer the assurance that required records management arrangements are in place, as data controllers and data processors. We have also refreshed our policies and training as evidence of our wider commitment to data protection.

4.5 The GLA has published a new Records Management and Lifecycle policy, as well as a data retention policy. These reflect enhancements to the way in which webform data is handled.

Training improvements

4.6 The GLA has reviewed the organisation records of GLA staff undertaking Information Governance and Cyber training (including mandatory refresher courses). The GLA/Transport for London (TfL) shared HR service has made improvements via the SAP portal to record this information and ensure that we have better visibility on this issue. We have also integrated automated reminders to staff when a refresher is due.

4.7 We have conducted additional mandatory information governance and specialist data protection training for relevant Digital team members. We are exploring further roll out of this enhanced training for all those who handle personal data.

Governance improvements to the London.gov.uk Content Management system

4.8 Immediately following the incident, the Digital Experience Unit (DEU) undertook a complete review to improve security of data collected by webforms in the London.gov.uk Content Management System (CMS). This included:

- A review of webforms which collected sensitive information.
- Management of access to webform submissions.
- Documentation of, and more restricted access to, form permissions for CMS editors.
- The development of a new testing and sign-off process for DEU staff proposing to make webform changes.

- A review was conducted of all those with access to London.gov.uk webform submissions. A clear process to create and implement a new webform has been established.

Wider digital governance improvements

4.9 We have also made enhancements to wider digital governance processes including the following:

- In addition to the work we did on our ROPA, we also ensured all processes related to data collection activities across the website have been captured.
- Enhanced training has highlighted the requirements for mandatory data governance reviews on all data products created on the digital estate.
- A review of those who should sign Escalated privileges and Data declaration forms.
- A review of privacy policies.
- Better communication of the work of Technical Design Board/Change Advisory Board
- Our incident management protocols have been updated.
- The City Intelligence Unit are reviewing the Digital Safeguarding policy to see if any changes are required in relation to the incident.
- In addition to the personal data breach protocol, the DEU have developed an enhanced digital incident management response protocol to minimise the impact of any further incidents.

5. Legal Implications

5.1 The data incident is being investigated by the ICO. We are awaiting the results of the investigation.

List of appendices to this report:

None

Local Government (Access to Information) Act 1985

List of Background Papers:

None

Contact Information

Contact Officer:	Niran Mothada, Executive Director of Strategy and Communications
E-mail:	Niran.Mothada@london.gov.uk