Scrutiny Panel

Item **12**

4th July 2023

Report of	**Richard Block**	**Author**	**Nicola Cooke 07815 487380**
Title	**Capita data breach**		
Wards affected	All wards		

1. Executive Summary

1.1 Scrutiny Panel received a request from Cllr Willets to include an item on the work program relating to the Safeguarding of residents' personal data processed by the Council and/or its contractors.

1.2 This report provides information relating to this to facilitate consideration by the Scrutiny Panel.

2. Action Required

2.1 The Scrutiny Panel to consider the report and whether they wish to make recommendations to Cabinet as to any changes to the current arrangements in place with respect to the protection of data.

3. Reason for Scrutiny

3.1 Scrutiny Panel received a request from Cllr Willets to consider a work programme item as follows:

3.2 It has been widely reported in the national press, local press and in Council press releases, that personal data, collected from residents by the Council for the purpose of financial administration, was entrusted to a contractor whose security standards fell considerably short of those mandated for the Council's own processing systems.

3.3 As a matter of urgency, to review the process and procedures for letting contracts which entail contractors handling and safeguarding personal information entrusted by residents to the Council.

3.4 To review the effectiveness of the Council's process for due-diligence enquiries into the security standards of contractors to be awarded contracts involving safeguarding personal data collected by the Council.

3.5 To review the process and procedures and time-frames for the City Council to contact all residents whose personal data was made publicly visible by security failure on the part of the Council's contractors, informing relevant residents of their personal data that was inadvertently made public, and the process for the timely issue of apology for the Council's failure to safeguard that resident's personal data.

4. Background Information

4.1 This request was in response to the Council being informed by Capita that they had identified they had experienced a security breach which involved the personal data of Colchester City Council residents.

4.2 Colchester has commissioned Capita to run end of year services for Council Tax and Benefits for six years. Some data relating to this service, along with similar data from other local authorities was found on an unsecured Amazon Data Bucket provided by and controlled by Capita. A data bucket is a cloud storage resource used to save data.

4.3 10 other Councils have been affected by this incident include Adur & Worthing, Coventry, Rochford and Royal Borough of Windsor & Maidenhead.

4.4 Capita are a large and well-known company used extensively by Local Authorities and other public sector organisations for the provision of ICT solutions as well as full outsourcing services.

4.5 Capita have secured the data and it is no longer accessible. Analysis of the datasets shows that the data, is historic and relates to the financial years 2019/20 and 2020/21. Files included council tax and benefits records.

4.6 Capita have completed their investigations but have been unable to determine if any unauthorised access to the data has occurred.

4.7 This data breach meets the threshold for being reportable to the Information Commissioners Office (the ICO), the UK regulator for data protection matters. An initial report was made on Friday 12th May.

4.8 An external audit of the Council's data protection practices (conducted in 2021) concluded that "CBC are legally required to only appoint data processors who can guarantee that they have sufficient technical and organisational controls to compliantly process CBC data. Therefore, the current due diligence process should be sufficient and conducted in a method that meets this requirement." The full report is appended below.

4.9 This audit rated the Council's procedures and policies relating to contractors to be 'Partially compliant'. All audit recommendations relating to this area of the audit have subsequently been progressed or fully implemented.

4.10 When contracts are let via the tenders process suppliers are asked to respond to a series of data protection questions which are scored as part of the evaluation process. Where items are procured via the Government online purchasing portal, gCloud, the gCloud standard terms and conditions are used and have adequate data protection provisions. The Council does not have data protection clauses in the terms and conditions for items purchased via purchase order. This specific contract was procured via purchase order.

4.11 Given a large number of Council contracts were awarded before the introduction of new data protection legislation in 2018 (the EU General Data

Protection Regulations (the EU GDPR)) a review of key Council contracts has been conducted.

4.12 In the last six months the data protection team have reviewed the adequacy of the data protection provisions in 15 new or renewing contracts/agreements.

4.13 Following award of contract, the Council takes a risk based approach to auditing security standards of contractors taking additional action where there is significant cause for concern.

4.14 The Council has clear procedures in place for managing data breaches. This includes a scoring mechanism that is applied to all data breaches which helps determine the seriousness of the breach and drives the determination of whether a breach meets the threshold for reporting to the regulator.

4.15 It is rare for the Council to have a breach which is reportable and of those that are, only some require the Council to notify affected individuals.

4.16 The Council is required by law to notify individuals "without undue delay." The Council's procedures do not include timeframes for notification to individuals as each breach is unique and should be assessed on a case-by-case basis. Information might initially be unclear or incomplete and it is only after the facts are established that a full risk assessment can be conducted and suitable communications can be drafted and sent.

4.17 The Council has a duty of care to its residents not to cause further undue distress through premature notification of a data breach before an adequate risk assessment has been conducted. This is balanced against the risks that the breach itself possess to affected individuals. We now believe that we have all of the information available following investigations by Capita. This information has been thoroughly reviewed and assessed in terms of risk. Although there is no evidence that the data has been misused, we felt that due to the nature of information that was included we would need to write to a number of customers. These letters and emails have now been issued.

5. Equality, Diversity and Human Rights implications

5.1 Contractors who are due to process special category personal data and/or high volumes of data are of a higher priority for due diligence checks at contract award than those without.

5.2 Personal data breaches that involve special category data are rated at a higher risk factor than those that do not.

6. Strategic Plan References

7.1 There are no particular strategic plan references.

7. Consultation

7.1 Notification of the Capita data breach to affected individuals has been made.

8. Publicity Considerations

8.1 The Council issued press releases relating to the Capita data breach on the 12th May and 17th May. Although the press releases highlight that this security incident has been caused by Capita there might be some reputational risk to the Council.

9. Financial implications

9.1 At the time of writing there are no additional financial implications caused by this data breach.

10. Health, Wellbeing and Community Safety Implications

11.1 There are no particular health, wellbeing or community safety implications.

11. Health and Safety Implications

11.1 There are no particular health and safety implications.

12. Risk Management Implications

12.1 The Council cannot fully prevent a similar occurrence in the future by another supplier, but does have mitigations in place (as described above) to lower the risk as far as practically possible within current resource constraints.

13. Environmental and Sustainability Implications

14.1 There are no particular environmental and sustainability implications.

Appendices

Appendix A. Data Protection Audit

Background Papers

None