Report of	Meeting	Date
Director of Governance	Governance Committee	Wednesday, 16 March 2022

GDPR Update

Is this report confidential?	No

Is this decision key?	Not applicable

Purpose of the Report

1. To inform members of the actions taken to review the Councils compliance with the General Data Protection Regulations (now Data Protection Act 2018).

Recommendations

2. That members note the report.

Reasons for recommendations

3. The report is for information and enables members to draw some assurance as to the compliance of the council with their obligations under the GDPR.

Other options considered and rejected

4. None.

Corporate priorities

5. The report relates to the following corporate priorities: (please bold all those applicable):

Involving residents in improving their local area and equality of access for all	A strong local economy
Clean, safe and healthy communities	**An ambitious council that does more to meet the needs of residents and the local area**

Background to the report

6. The requirements of the General Data Protection Regulations came into force in May 2018.
7. The Council delivered and adopted a compliant framework which met our obligations under the legislation. This included adoption of new policies on data use and processing, data use statements and internal controls. In addition, the councils standard terms of contract were updated to ensure clarity in responsibility between council and contractors.
8. It had been intended to undertake a full review in 2020/21. This was to review whether the adopted policies remained compliant but also whether they were being used appropriately.
9. This review was delayed due to the impact of covid. This was not seen as a significant risk to the organisation. The Council already had robust and compliant procedures in place to process personal data due to our longstanding obligations under the Freedom of Information and Data Protection Legislation. Further, our operating controls within our Information Security Framework are compliant for the purposes of securing access to digital data.
10. The review was undertaken by legal services in the final quarter of this year.

Policy compliance

11. Although the policies are owned by services, the review was undertaken by the legal team to provide some quasi independent assessment. The following policies were reviewed:-
    a. Corporate Data Use Policy
    b. Data Breach Policy
    c. Data Retention and Erasure Policy
    d. Employee privacy policy
    e. Information classification policy
    f. Information security policy
    g. Privacy notice
    h. Privacy standard
    i. Subject access policy
    j. International data transfer procedure.

    The policies were considered compliant with the legislation by legal services and they found only some minor amendments to be made.

12. It was noted however that there was no evidence of internal reviews by services owning the documents being undertaken. Teams were reminded that reviews should be recorded. This did not undermine council overall compliance.
13. This report has already referenced the council Information Security Framework. This was not reviewed by legal services as while compliance with it supports GDPR compliance it is not in itself a GDPR policy. IT who own this document have been asked to undertake a review of it.

Data retention

14. In addition to the corporate Data Retention and Erasure Policy which sets out the corporate approach and retention periods, individual teams could have their own specific policies setting out different periods. This is appropriate as data controllers should consider personal data on an individual basis and there will be no “one size fits all” position on data retention.
15. These policies have not been reviewed within this process as they follow the corporate model and only the periods change. In the course of the year the Data Protection Officer has reminded Data Controllers to review both the retention periods and compliance by the teams with them.

16. This will be subject to a piece of work by Internal Audit.

Data Controllers

17. The Council appointed a number of Data Controllers to lead on compliance within teams. It is apparent, that due to changes in working necessitated by covid, changes relating to shared services and the movement of staff that there are some outstanding vacant data controller roles.
18. This does not mean that the council are none compliant, however, it is harder to show ownership within teams of the issues. The current data controller list is being refreshed with teams nominating to vacant roles.

Training

19. The Council have on line training for all staff on the principles of data protection and enhanced training for data controllers. This training is mandatory. The training has been refreshed and will be rolled out in April. It will be mandatory for all staff to complete this training and it will form part of induction training also.

Data Breaches

20. The Council take a robust approach to self reporting to the Information Commissioners Office. Since 1 April 2021 we have self reported twice, neither incident was viewed as serious internally, however, we view data security seriously and accept the trust the public have placed in us needs to be maintained.
21. In both cases the council had acted swiftly to correct the issue but also to provide additional training or change processes to limit the risk of the incident happening again.
22. In light of our actions the ICO took no action on either self-report.
23. Members can take some assurance that the GDPR framework is operating and embedded due to the limited number of data breaches. It is also important to note that these are self identified breaches and not reports by third parties suggesting that staff are aware of mistakes and are prepared to raise them.

Adequacy Decision

24. One of the concerns that arose in relation to BREXIT was the sharing of data with other EU countries. This was resolved in June last year when the EU provided an adequacy decision confirming that the UK legislation, which implemented the GDPR, was compliant. This will run until June 2025.

Climate change and air quality

25. The work noted in this report does not impact the climate change and sustainability targets of the Councils Green Agenda and all environmental considerations are in place.

Equality and diversity

26. There are no equality and diversity implications in this report.

Risk

27. There are 2 key risks that arise through failing to have and maintain a robust GDPR framework.
28. As data controller the council have a significant financial risk should there be systemic failings in the processing of sensitive personal data. The ICO can levy fines in the order of £5million for serious breaches.
29. More importantly, there is a significant reputational risk should any systemic failings in data processing be identified. The Council hold a significant amount of personal data and need to do so in order to properly fulfil our functions and serve the public interest. If the trust in the council is undermined the public may not be willing to share this data and this will inhibit our ability to deliver services.

Comments of the Statutory Finance Officer

30. There are no direct financial implications of this report.

Comments of the Monitoring Officer

31. It is imperative that the Council ensures compliance with its obligations under Data Protection legislation. This review is a clear indicator that the Council takes this duty seriously.

Background documents
There are no background papers to this report.

Appendices
There are no appendices.

Report Author:	Email:	Telephone:	Date:
Chris Moister (Director of Governance)	chris.moister@southribble.gov.uk	01257 51	