Chorley Council

Report of	Meeting	Date
Director of Policy and Governance	Governance Committee	21 November 2018

GDPR UPDATE

PURPOSE OF REPORT

1. To inform members of the implementation of the General Data Protection Regulations.

RECOMMENDATION(S)

2. Members note the report.

EXECUTIVE SUMMARY OF REPORT

3. The General Data Protection Regulations (EU 2016/679) came into force on 25 May 2018. The aim of the Regulations was to give control to individuals over their personal data and provide a simplified regulatory regime.
4. The Regulations apply to all organisations who process personal data within the European Union and this includes Local Authorities.
5. The Regulations introduce or restate a number obligations placed on organisations in relation to how they process and share personal data. The obligations serve to protect the integrity of individuals personal data and ensure it is only used for authorised purposes.
6. Chorley Council were obliged to be compliant with the requirements of the GDPR from 25 May this year. The report confirms the actions taken to attain compliance and details the arrangements for maintaining it.

Confidential report Please bold as appropriate	Yes	**No**

CORPORATE PRIORITIES

7. This report relates to the following Strategic Objectives:

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

BACKGROUND

8. In 2016 the European Union adopted for implementation from 25 May 2018 the General Data Protection Regulations. These regulations had direct effect in member countries jurisdictions and effect any organisations processing data within the European Union. To confirm the UK have given these regulations effect and they will continue to operate after Brexit.
9. Chorley Council process significant amounts of personal data and as a result must comply with these regulations. As a local authority we are also required to appoint a Data

Protection Officer who audits the performance of the council and is a single point of contact for individuals and the Information Commissioners Office.

10. The main thrust of the Regulations is that personal data should only be processed for the purpose it has been provided or otherwise only with explicit consent. The Regulations also place additional responsibilities on organisations to manage the security of the data held.
11. Breach of the Regulations is serious, with the Information Commissioners Office being able to levy fines of up to £5 million or 1% if global turnover (whichever is higher) or £10million / 2% of global turnover for breaches relating to special data. It should be noted though that these sanctions apply to all organisations and the risk must be set against the potential misuse. As a local authority who does not process data for "profit" the risk of a maximum level fine for a non-wilful breach is low.
12. However, there are significant reputational risks attached to breaches of the Regulations and most significantly a loss of public trust which would severely undermine the council's ability to discharge its functions.
13. It is very important for the council to ensure that we meet and exceed our obligations under the legislation to ensure continued resident confidence in our Governance arrangements'.

IMPLEMENTATION

14. As a local authority, Chorley Council has been compliant with both Data Protection and Freedom of Information legislation for many years. There were already strong policies and processes in place which demonstrated how we discharged our obligations. There was already a culture of data protection. This had both plus and negative points.
15. It was extremely positive that the Council already had a cultural awareness of data security. We already had a robust Information Security Framework against which the council could demonstrate compliance with the existing legislation. What was a challenge was to ensure the identified differences with the old legislation were communicated properly with staff. We also had to embed new roles within the organisation and ensure an understanding of the new responsibilities that went with them.
16. Corporate policies and processes were prepared and approved by the Council. These are available to all staff on the Loop. These included
    a. Corporate Data Usage Policy;
    b. Data Breach Policy;
    c. Data Retention and Erasure Policy;
    d. Employee Privacy Policy; and
    e. Information Security Policy.

    Compliance with these policies ensures the Council are able to demonstrate compliance with the Regulations.
17. There are 3 new roles identified within the Regulations
    a. Data Protection Officer;
    b. Data Controller; and
    c. Data Processor.

    The role of the SIRO (Senior Information Risk Owner) is retained and the responsibilities attached to that role continue. The Council have appointed the Monitoring Officer to the role of Data Protection Officer.
18. Data Controllers have been identified within services and work has been done with each service to prepare an Information Asset Register which details the data held by each team, what it is used for and the period it needs to be retained. This included both digital and paper based data. No distinction was drawn between personal data caught by the Regulations and none personal data. It is entirely consistent with the Council's information management approach to reduce all unnecessary data held so the strict approaches directed by the Regulations meet the Council's priorities.
19. Having completed the information audit, Data Controllers prepared service specific retention periods which have been used to update the corporate policies.

TRAINING

20. To ensure that staff have the requisite understanding, it is mandatory for all members of staff to have completed the GDPR module on the Emerge eLearning portal. All members of staff who were present (not on long term sick, maternity leave or other reasons) have completed this course. This provided ongoing testing during the module to ensure understanding of the Regulations.
21. Data Controllers have received enhanced training provided by an external trainer ActNow. This training went into greater depth than that given to data processors, particularly into the data principles. This was necessary as it enabled Data Controllers to understand the why behind the policies. Understanding why the policy operates enables the Data Controllers to constantly review and test their processes, challenging appropriately to improve the service delivery.

OPT IN AND CONSENT

22. The vast majority of the personal data held by the Council has been provided under legislation or in order for the Council to deliver a service. As long as the Council only use the personal data for the reasons it has been provided no further consent is required from our residents.
23. In order to ensure that residents receive the best possible service however, the Council have set up processes to enable them to opt in to receive information about other Council services.

COUNCILLORS

24. Councillors are also Data Processors in relation to information received from the Council and Data Controllers in relation to information received directly from residents. All Councillors have been duly registered as Data Controllers with the Information Commissioners Office and have been provided with access to the eLearning module on Emerge. In addition the Data Protection Officer provided a face to face session for all councillors.
25. Councillors can take comfort that the iPads and computer systems provided are secure, so as long as any data saved digitally is kept on the Council equipment they will be compliant. Also Councillors will only receive personal information for use for the purpose it is supplied and therefore will not need any additional consents.

THIRD PARTIES

26. Specific agreements have been put in to place with third parties concerning the use of personal data provided by the Council. These conditions have been incorporated into the Council's standard terms and conditions. The conditions require the third party to process the data only in accordance with the requirements of the GDPR and for no other purpose.

DATA PROTECTION OFFICER

27. The DPO has 3 main areas of duty in relation to the Regulations
    a. Advising and Training;
    b. Monitoring and Audit; and
    c. Point of contact for the Information Commissioners Office.

    To discharge these duties the DPO will work with the SIRO to ensure that adequate training is provided annually. This will be part of the Council's Organisational Development Strategy under Learning and Development. Members of the Legal Team have received additional training to ensure that the Council are adequately supported in relation to the interpretation and operation of the Regulations.
28. Detailed audits will be undertaken for all services. Services with the highest risk of a data breach will be prioritised, although it is intended that all services and teams will be audited.

An audit plan will be developed and presented to the Committee for information at the next meeting on 23 January 2019. The plan will commence in year 2019/20.

IMPLICATIONS OF REPORT

29. This report has implications in the following areas and the relevant Directors' comments are included:

Finance	✓	Customer Services	
Human Resources		Equality and Diversity	
Legal	✓	Integrated Impact Assessment required?	
No significant implications in this area		Policy and Communications	

30. As mentioned in the body of the report whilst there are significant financial penalties for breach of the Regulations, the most significant risk is reputational. This risk is being managed through the adoption of robust policies and procedures and through mandatory training.
31. The audit process mentioned will also serve to mitigate the risk not only to the Council but also to resident personal data.

COMMENTS OF THE STATUTORY FINANCE OFFICER

32. All cost implications of implementation and training have been met within existing resources.

COMMENTS OF THE MONITORING OFFICER

33. The position is correctly stated in the body of the report.

CHRIS MOISTER
MONITORING OFFICER

Report Author	Ext	Date
Chris Moister	5260	