Central
Bedfordshire
Council
Priory House
Monks Walk
Chicksands,
Shefford SG17 5TQ

TO ALL MEMBERS OF THE
AUDIT COMMITTEE

29 December 2017

Dear Councillor

AUDIT COMMITTEE – MONDAY, 8 JANUARY 2018

Further to the agenda and papers for the above meeting, previously circulated, please find attached the following report together with a replacement Appendix A which is in a revised format:

10. Update on Preparations for the General Data Protection Regulation (GDPR)

To consider an update on preparations for the General Data Protection Regulation and the Council's plans for compliance.

Should you have any queries regarding the above please contact me.

Yours sincerely

Leslie Manning
Committee Services Officer

email: leslie.manning@centralbedfordshire.gov.uk
tel: 0300 300 5132

This page is intentionally left blank

Central Bedfordshire Council

AUDIT COMMITTEE 8 JANUARY 2018

UPDATE ON PREPARATIONS FOR THE GENERAL DATA PROTECTION REGULATION (GDPR)

Advising Officer: Stephan Conaway, Chief Information Officer (Stephan.conaway@centralbedfordshire.gov.uk)
Contact Officers: Sean Dykes, Information Security Manager (sean.dykes@centralbedfordshire.gov.uk)
Maria Damigos, Corporate Lawyer, LGSS Law Ltd

Purpose of this report

1. The report seeks to provide an update on preparations for the General Data Protection Regulation (GDPR) and the Council's plans for compliance.

RECOMMENDATIONS
The Committee is asked to:

i. Note the progress regarding preparations for the GDPR.

Overview and Scrutiny Comments/Recommendations

2. This report is to update the committee on preparations for the GDPR following the last Audit Committee on 27 Septempber 2017. No decision is necessary and the report has not been considered by the Overview & Scrutiny Committees.

Introduction

3. At the Audit Committee meeting of 27 September 2017, Members were briefed on the GDPR and the Council's preparations. This brief is to update on those preparations.

Background

4. How personal data is dealt with in the UK is currently governed by the Data Protection Act 1998 (DPA) which was enacted to bring the

European Union (EU) Data Protection Directive 1995 into UK law.

5. The GDPR is an EU Regulation by which the European Parliament, the Council of the European Union and the European Commission intended to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulations within the EU.

6. The regulation was adopted on 27 April 2016. It becomes enforceable from 25 May 2018 after a two-year transition period. It does not require any enabling legislation to be passed by national governments and is thus directly binding and applicable whilst the UK is a member of the EU. The UK government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

7. A Data Protection Bill is currently progressing through Parliament which will incorporate the requirements of the GDPR into UK legislation. It is likely that the GDPR requirements will be applicable after the UK leaves the EU.

Summary of Changes

8. The GDPR extends the rights and responsibilities contained in the DPA. Apart from private use, it will apply to all individuals and organisations storing or using personal data and will include a 'data processor' (someone who acts on a data controller's behalf).

9. Under the DPA the data controller was responsible for the data. Data processors will now have specific obligations in relation to record keeping and processing and will have more legal liability in the event of a breach.

10. The key areas of change are:

    a. Lawful processing

    For processing to be lawful under both the DPA and the GDPR, a lawful basis must be identified. The requirements for lawful processing under GDPR will change slightly.

    b. Consent and Privacy Notices

    The definition of consent under the GDPR is more strictly defined than under the DPA. . Simple procedures for withdrawing consent must be in place.

    The Council as a public authority and an employer will need to take particular care to ensure that consent is freely given (or rely on another basis for processing).

Where consent is not given or required individuals must be provided with a notice detailing what information is held and why, what will be done with the information and the persons rights in respect of that data.

c. Children's personal data

The GDPR contains new provisions intended to enhance the protection of children's personal data.

d. Individual's Rights

The GDPR both strengthens existing rights under the DPA and creates new rights for individuals.

e. Accountability and Governance

The GDPR includes specific provisions that promote accountability and governance which complement the GDPR's transparency requirements.

f. Breach Notification

The GDPR will introduce a duty to report all incidents where there has been a significant breach to the ICO within 72 hours. The Council already has a successful reporting system in place which will only need minor updates to comply with the timescale for reporting.

g. Transfers of personal data to third countries or international organisations

The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations, in order to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

11. The GDPR also significantly increases the maximum fine for a data protection breach which can be imposed from £500,000 to either 10 million euros or 20 million euros (or 2% or 4% of global turnover in the preceding financial year respectively) depending on the type of breach.

Current Position

12. A GDPR Working Group has been set up to monitor and implement the requirements of the GDPR within the Council. The group is made up of the Information Security Manager, LGSS Corporate Lawyer, Head of Internal Audit, Deputy Chief Information Officer, Records and Risk Officer and Information Request Officer. Updates are provided to the

Monitoring Officer, SIRO/Chief Information Officer, CMT and the Information Assurance Group (IAG) as necessary.

13. The IAG includes senior officers from Human Resources, Internal Audit, IT, Children's Services, Adult Services and the Caldicott Guardian and can provide further support, initial approval and sense checking of proposed draft documents and procedures.

14. Appendix A sets out the ICO Recommended Actions and updates the Council's status as regards those actions as at 13 December 17.

15. The template for consent and privacy notices has been completed and we are about to begin the build of an electronic version of this form prior to testing. Once rolled out, it is proposed that drop in sessions will be available for queries.

16. The Council's data protection training is to be reviewed and revised early 2018 and this will also take account of the new requirements of the GDPR. This will commence in January 2018.

17. At the last Audit Committee various comments were made regarding compliance, planning and training and these have been fed into the work plan and will be incorporated into preparations.

18. Council Priorities

19. Compliance with legal obligations ensures that Council delivers it priorities and contributes to the achievement of all the Council's priorities.

Corporate Implications

Risk Management

20. Failure to implement the requirements of the GDPR would be a breach of the law. This is already identified as a significant governance issue within the draft Annual Governance Statement for 2016/17. It is however anticipated that all requirements will be met or implemented.

Staffing (including Trades Unions)

21. There are none.

Legal Implications

22. The GDPR will become law in the UK on 25 May 2018. The Council will need to comply with the GDPR and any other applicable legislation.

Financial Implications

23. Although this report has no financial implications, resources will be required for implementation of, and compliance with, the GDPR which will either be met from existing budgets or will be the subject of further reports to the appropriate committee or Executive.

Equalities Implications

24. None arising directly from this report.

Conclusion and next Steps

25. Development of a detailed Action Plan with ongoing awareness raising for all staff. Drop in sessions to assist departments with specific queries are also to be arranged and delivered.

Appendices

The following Appendices are attached:

Appendix A – ICO Recommended Actions – Current Position Dec 17

Further information can be obtained from:
https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

This page is intentionally left blank

B C

Action as recommended by ICO					Date Completed
Action Ongoing	**Position as at 9/8/17**	**Position Sep 17 (Working Group 12 Sep)**	**Position Oct 17 (Working Group 24 Oct)**	**Position Nov 17**	
Your business has implemented appropriate technical and organisational measures to show you have considered and integrated data protection into your processing activities	Technical measures to be incorporated have been discussed with Hytech, the Council's information security technical consultants. Notices have been published to all staff on the changes on how they may affect them. Policies & Procedures will be updated during early 2018.	I will be contacting Hytech to further discuss this. I will need to invite them here to discuss the issue with senior IT managers who will be involved in implementing any changes to systems that may be required. I will be briefing the IT Management Team on 21 Sep.	Briefing took place in September. Our first step as far as GDPR compliance is concerned is becoming cyber essentials scheme qualified. Bernard Sykes will be working on this through December and January.	Cyber Essentials scheme preparation is due to commence during Dec 17. Actions will be identified and the process for compliance will begin during early 2018.	
Your business understands when you must conduct a DPIA and has processes in place to action this.	This was instigated at CBC during 2016. A campaign to repromote this has been commenced with email reminders sent to Directors and AD's for cascading down to Managers and Staff	I consider that this be the next big promotional push. It's in place but it is not being done. Perhaps one for discussion at IAG first?	This will be the first element of DPIA to be publicised. The system we have in place is robust and, according to ICO guidelines, sufficient but it is not being utilised. It is intended to make PIAs mandatory from 1 Jan 18.	According to the ICO, the current process for DPIA will be suitable until new guidance is prepared early in 2018. This will be notified via Council communications during early 2018 on what staff are required to do.	
Your business has a DPIA framework which links to your existing risk management and project management processes.	This was instigated at CBC during 2016. A campaign to repromote this has been commenced with email reminders sent to Directors and AD's for cascading down to Managers and Staff	Cat and I will discuss this at our meeting on 21 Sep and work out how we can make this work.	See above	See above	
Your business has designated responsibility for data protection compliance to a suitable individual within the organisation.	Information Security Manager who feed issues into the Information Assurance Group. This is then reported to Corporate Management Team on a quarterly basis.	That's me at the moment with lots of support from you wonderful people. Need Chf Exec to clarify our position. Another one to bring up at IAG.	This issue has been flagged to senior management via Monitoring Officer and DCIO.	Position unchanged from October.	
Your business has appointed a Data Protection Officer (DPO) if you are: (LIST) a public authority or you carry out large scale monitoring of individuals or you carry out large scale processing of special categories of data or data relating to criminal convictions and offences.	This is to be confirmed by the Chief Executive.	See above	See above	Position unchanged from October	
Your business supports the data protection lead through provision of appropriate training and reporting mechanisms to senior management.	Data protection and information security training will be reviewed early in 2018 with L&D to consider changes that need to be made to it and consider more specialised training for those areas where sensitive personal data is handled more extensively.	We have these in place with GDPR refinements will take place early in 2018.	A risk assessment will be undertaken during December to assess those areas that will require more in-depth training aligned to the work they are doing.	Risk assessment has taken place. We have a GDPR training framework in place which we will build into a training course at different levels dependent on the role that a staff member holds. Those that work more closely with sensitive data will be required to complete a more detailed assessment.	
Your business has reviewed the various types of processing you carry out. You have identified your lawful basis for your processing activities and documented this.	We have a lawful basis for processing, although we will study the new data protection bill for any new requirements.	Position unchanged	Position unchanged	Position unchanged	
Your business has explained your lawful basis for processing personal data in your privacy notice(s).	SD and MD LGSS will be working on a new draft privacy notice during August	Work continues on revised privacy notices and consent forms (IAG 10/10)	This work is ongoing. A draft should be ready for IAG on 12 Dec 17.	The draft is almost complete. Testing now needs to take place and then an e-form designed and built by IT.	

B C

Your business has documented what personal data you hold, where that data came from and who it is shared with.	This will be considered by SD and CAG. Will take advice from Internal Audit on how best to do it	CAG and SD will be meeting Internal Audit shortly. May be useful to include Information manager (Aidan McDonald) in discussions.	We are preparing an email for signature by CE nominated all Heads of Service as IAOs due to poor compliance levels currently. Traiuning will be offered that will include a GDPR element. By doing this we should have a clear view of what information assets we hold and what actions we need to take.	Information Security Manager is meeting with the Chief Executive on 19 Dec to gain approval for the email that will nominate all Heads of Service as IAOs. Training on the role and how it relates to GDPR will be offered. The IAOs will then be required to do an auit of their information assets.	
Your business has planned to conduct an information audit across the organisation to map data flows.	Will speak to Internal Audit on this	Meeting scheduled with Internal Audit for 21 Sep	Audit assisted with the wording of what we will require from IAOs. This will be included in the proforma forwarded to IAOs when completing a local information asset audit.	See above	
Your business has reviewed how you seek, record and manage consent.	MD LGSS and SD will be working on new consent notices for all departments shortly	Work continues on revised privacy notices and consent forms	This work is ongoing. A draft should be ready for IAG on 12 Dec 17.	The draft is almost complete. Testing now needs to take place and then an e-form designed and built by IT.	
Your business has reviewed the systems currently used to record consent and implemented appropriate mechanisms in order to ensure an effective audit trail.	SD to speak to Hytec (Information Security technical experts) regarding this.	See Ser No 5	See Ser No 5	See Ser No 5	
Decision makers and key people in your business are aware that the law is changing to the GDPR and appreciate the impact this is likely to have.	Yes. CMT and Members have been made aware of the changes and the likely effect.	We intend to increase the amount of publicity that we are giving the GDPR. Higher management are aware of the changes and have been informed of them for some time. Hard to judge what level of engagement they have.	A meeting is scheduled for 30 Nov with Corporate Comms to work out an effective awareness campaign.	A full communications campaign has been agreed with Corporate Communications and will commence with an overview of the GDPR followed more detailed guidance leading up to May 2018.	
Your business has identified areas that could cause compliance problems under the GDPR and has recorded these on the organisation's risk register.	We are working with Internal Audit on this	MD LGSS will be looking at identifying these and will take appropriate action to add to the risk register.	Head of Audit has been made aware of issues that may need to be added to the Corporate Risk Register.	Hd of Audit has been requested to flag GDPR up on the risk regiuster to raise the profile and encourage engagement.	
Your business is raising awareness across the organisation of the changes that are coming.	Regular updates have been published in local media (Staff Central, Managers Emails) since the beginning of 2017. More detailed information on the changes coming is now being directed at Directors and AD's.	Regular updates and reminders continue. The GDPR WG will have a piece in SC shortly and need to push PIAs	A meeting is scheduled for 30 Nov with Corporate Comms to work out an effective awareness campaign.	A full communications campaign has been agreed with Corporate Communications and will commence with an overview of the GDPR followed more detailed guidance leading up to May 2018.	
Your business has set out the management support and direction for data protection compliance in a framework of policies and procedures.	We already have this in place. All policies and procedures will be reviewed early in 2018 to assess the need for change to reflect the new regulation.	See Column B	See Column B	A full review of all data protection, records management and information security policies will take place early in 2018.	
Your business monitors compliance with data protection policies and regularly reviews the effectiveness of data handling and processing activities and security controls.	Policies are reviewed every two years currently. All our information governance policies will be reviewed early in 2018 and amended to reflect the new regulations. These will only be published generally once GDPR is law. Our training package is being reviewed in conjunction with L&D beginiing in Jan 2018.	In addition to actions at Column B, this is something we should engage with IAOs on. Following on from Audit Committee it has been suggested we upgrade the policies we already have (Comment 27/9)	Policy reviews will take place during Jan 2018 alongside a new IAO campaign	Position unchanged	

B C

Your business has developed and implemented a needs-based data protection training programme for all staff.	See above. This will be developed with L&D colleagues from Jan 2018.	Any training amendments will need to be reflected in all revised policies (Comment 27/9)	A risk assessment of training needs will be undertaken with L&D colleagues during Dec 2017.	Work will being on this during Jan 2018.	
Your business has documented what personal data you hold, where that data came from and who it is shared with.	All our information sharing arrangements are documented and must be approved by an authorisation group consisting of Caldecott Guardian, LGSS Corporate Lawyer, Information Security Manager and Records & Risk Officer. We will need to check how personal data holdings are recorded.	CAG and SD will be contacting IAOs using script provided by Internal Audit to provide information on current holdings (Comment 27/9)	We are preparing an email for signature by CE nominated all Heads of Service as IAOs due to poor compliance levels currently. Training will be offered that will include a GDPR element. By doing this we should have a clear view of what information assets we hold and what actions we need to take.	Information Security Manager is meeting with the Chief Executive on 19 Dec to gain approval for the email that will nominate all Heads of Service as IAOs. Training on the role and how it relates to GDPR will be offered. The IAOs will then be required to do an auit of their information assets.	
Your business has planned to conduct an information audit across the organisation to map data flows.	We will need to consult Internal Audit on this.	See Ser 38. We will consider all returns following Ser No 38 actions and make a decision on which areas will require a full audit (Comment 27/9)	This will be completed by newly appointed IAOs.	Position unchanged	
42 **Your business has checked your procedures to ensure that you can deliver the rights of individuals under the GDPR.**	This action is ongoing	Work continues on Privacy Notices and Consent Forms. During Jan 2018 we will start to promote SAR compliance changes	See Column C	See Column C	
Your business has reviewed your procedures and has plans in place for how you will handle requests from individuals for access to their personal data within the new timescales outlined in the GDPR.	We will be working on this from Jan 2018. The system we have will be easy to change and we will ensure that all users are aware of the changes in plenty of time prior to implementation.	See Ser No 42	See Ser No 42	See Ser No 42	
Your business has reviewed your procedures and has plans in place for how you will provide any additional information to requestors as required under the GDPR.	Our system is already very robust and will require minimal alteration.	See Column B and Ser No 42	See Column B and Ser No 42	See Column B and Ser No 42	
Your business has implemented appropriate procedures to ensure personal data breaches are detected, reported and investigated effectively.	These have been in place for two years.	See Column B	See Column B	See Column B	
Your business has mechanisms in place to assess and then report relevant breaches to the ICO where the individual is likely to suffer some form of damage, e.g. through identity theft or confidentiality breach.	The Information Security Manager is notified of all breaches and will make an assessment on each incident on what action needs to be taken.	See Column B. SD to promote the need to report breaches via the current system within 72 hours from Spring 2018.	Seec Column C	See Column B	
Your business has mechanisms in place to notify affected individuals where the breach is likely to result in a high risk to their rights and freedoms.	See above. Information Security Manager, sometimes in consultation with LGSS, will assess if this action needs to be completed.	See Column B	See Column B	See Column B	

B C

If your business offers services directly to children, you communicate privacy information in a clear, plain way that a child will understand.	MD LGSS and SD will be looking at this shortly	Work is currently progressing on this	Work is currently progressing on this	Work is currently progressing on this	
If your business offers 'information society services' directly to children, your business has systems in place to verify individuals' ages and to obtain parental or guardian consent where required.	Information Society services are "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of the recipient for services". Need to find out if CBC provide such services	MD LGSS to investigate?	Awaiting LGSS investigation result	Awaiting LGSS investigation result	
If your business operates in more than one EU member state, you have determined your business's lead supervisory authority and documented this.	Not applicable	Not applicable	Not applicable	Not applicable	