Corporate Policy and Resources Committee	
Date: 10 Jan 2019	

Subject: GDPR Implementation Update

Report by:	Executive Director of Resources
Contact Officer:	Steve Anderson Data Protection Officer 01427 676652 steve.anderson@west-lindsey.gov.uk
Purpose / Summary:	This report is an update on our compliance with the EU General Data Protection Regulation (GDPR). The report provides a summary of the work we've done so far, gives an assessment of our current compliance position, and sets out our plan for continuous improvement over the next 2 years.

RECOMMENDATION(S):

Members welcome and support this report and agree that future updates be provided quarterly in the Members' Newsletter.

IMPLICATIONS

Legal:

Supports compliance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018)

Financial : **N/A**

Staffing : **N/A**

Equality and Diversity including Human Rights : This report supports the rights and freedoms of all individuals by demonstrating West Lindsey District Council's compliance with the General Data Protection Regulation (GDPR) Article 5(1)(a) which states: "Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject".

Risk Assessment :

Climate Related Risks and Opportunities : N/A

Title and Location of any Background Papers used in the preparation of this report:
None.

1 Purpose

1.1 The purpose of this report is to update Members on our compliance with the EU General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA). The report summarises the work we've done so far, gives an assessment of our current compliance position, and sets out our plan for continuous improvement over the next 2 years.

2 Background

2.1 In May 2018 we saw the most significant change to data protection law in 20 years with the introduction of the GDPR. GDPR came into effect on 25 May 2018 after a 2 year implementation period alongside the DPA.

2.2 The new Regulation strengthens the rights of individuals, addresses the impacts on them of the advances in modern technology, and introduces a new principle of accountability on data controllers.

2.3 The DPA sits alongside GDPR and details provisions for how GDPR is applied in the UK. The DPA also:

- Deals with processing that does not fall within EU law (i.e. immigration);
- Transposes the EU Law Enforcement Directive into UK law;
- Ensures that processing carried out by the intelligence services is required to comply with internationally recognised data protection standards; and
- Sets out the duties, functions and powers of the Information Commissioner.

2.4 GDPR and the DPA are inter-related and one cannot be applied without the other.

2.5 In 2016, the Director of Resources agreed a plan to become compliant with the new laws based on the Information Commissioner's Office (ICO) "12 Steps for preparing for the GDPR"

2.6 The most significant task proposed in the "12 Steps" required us to carry out a complete data audit to identify the personal data held by teams in file shares, email boxes and stored in back-office systems. From this, officers developed a more detailed action plan to properly identify and cost the work needed to comply with the new regulations.

3 What have we done so far?

3.1 Major Milestones

1. Completed the applicable steps of the "12 Steps" plan.
2. Completed a data audit and used this to create a Record of Processing Activities (RoPA) to comply with GDPR Article 30.
3. Compiled and presented audit findings to team managers and agreed corrective actions.

4. Reviewed and updated our Data Protection and Data Breach Reporting policies.

5. Updated our full privacy notice to comply with Articles 13 and 14 of the GDPR and developed privacy notices for each team.

6. Appointed a Data Protection Officer (DPO) as required by Article 37 of the GDPR.

7. Procured and rolled out GDPR awareness training to all staff.

8. Started a complete review of our data processing contracts and data sharing agreements.

9. Implemented a centralised management system for the recording and management of data subject requests (subject access, right to erasure, right to object etc.).

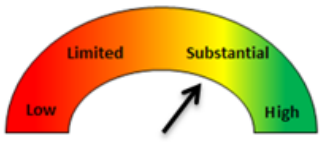
10. Integrated a Data Protection Impact Assessment (DPIA) process into the corporate project methodology to comply with Article 35 of the GDPR.

11. Achieved "Substantial Assurance" in an audit carried out by Internal Audit on our GDPR preparedness in Feb 2018.

12. Delivered 3 GDPR Awareness Sessions to Members and Parishes.

13. Co-founded a Data Protection Officer (DPO) Forum to share best practice and discuss DP issues with other Lincolnshire DPOs.

3.2 What evidence do we have to back this up?



3.2.1 To confirm that we were moving in the right direction and at the required pace to become compliant with GDPR by 25 May 2018, the Management Team commissioned an audit of our preparations. Internal Audit completed their work in Feb 2018 and gave our GDPR Readiness a "Substantial Assurance" rating.

3.2.2 We will be further testing our progress since then with a follow-up audit early in the New Year.

3.3 Cost of Implementing GDPR

3.3.1 We tried, where possible, to absorb the resource utilisation and costs of complying with GDPR into our "business as usual" activities and in the main this has been very successful. Tangible costs incurred between Jun 2017 and 1 Nov 2018 are summarised in the table below:

ITEM	DETAIL	COST
1	Subscription to Record of Processing Activities Tool	£ 445.00
2	Training/Seminars	£2981.00
3	Reference Materials/Documentation Templates	£ 269.94
4	Updates to Business Systems	£6050.00
5	Data Protection Fees (see below)	£2940.00
TOTAL		£12685.94

3.4 Data Protection Fees

3.4.1 From 25 May 2018, the Data Protection (Charges and Information) Regulations 2018 (enacted alongside the DPA) requires every organisation or sole trader who processes personal information to pay an annual data protection fee to the ICO, unless they are exempt.

3.4.2 The cost of the fee depends on the size of the organisation and turnover. There are three tiers of fee ranging from £40 and £2,900 and it is a criminal offence to pay the wrong fee.

3.4.3 Because we employ more than 250 employees (based on headcount) then we now need to pay the tier 3 fee of £2900. Members should note that in previous years the calculation was based on FTEs and we paid £35 discounted to £30 for paying by direct debit so this is a significant increase.

3.4.4 We also pay the tier 1 (£40) fee for the Electoral Registration Officer.

3.4.5 Prior to 25 May 2018, elected members were liable to pay an annual fee of £30 each for processing carried out in respect of their constituency work. These fees were managed and paid for by the Council. The fee increased to £40 on 25 May 2018 but, following a recent consultation, the Department of Culture and Media Services (DCMS) has announced that MPs and other elected officials will be exempt from paying the fee in future.

4 So where are we now?

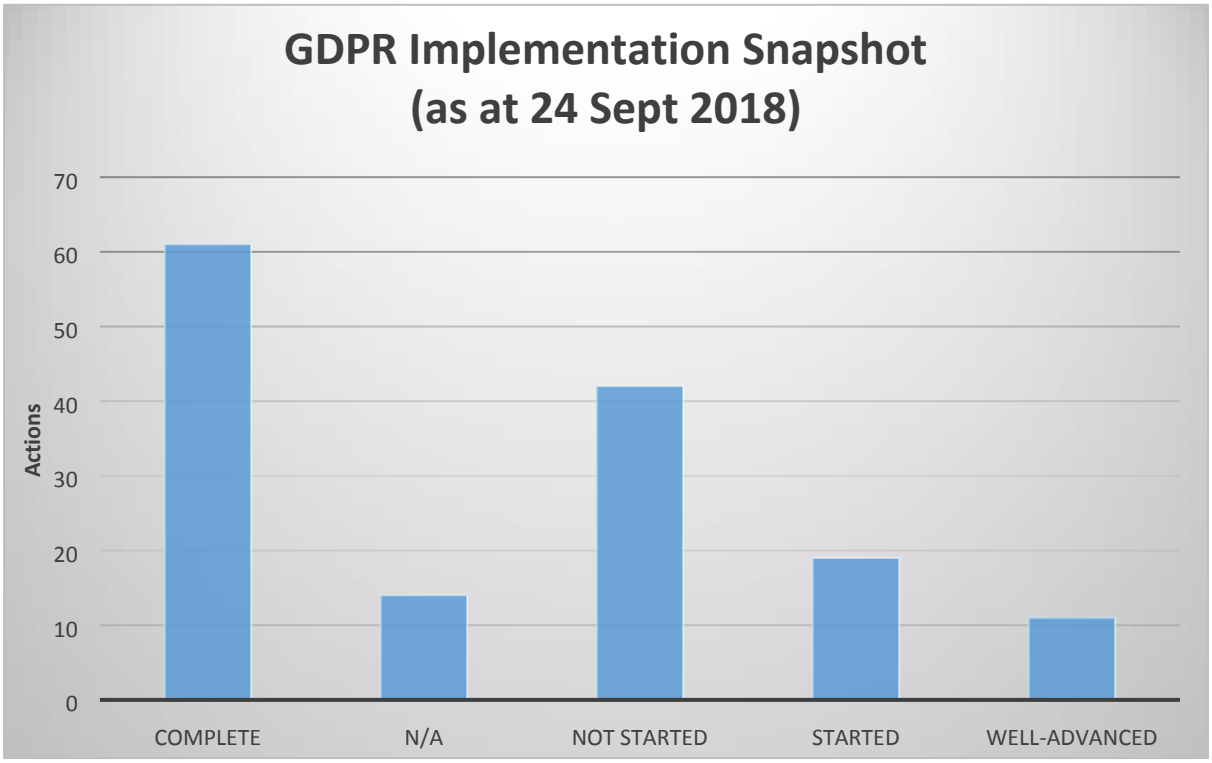
4.1 According to the Local Government Association (LGA), a district council can be responsible for delivering more than 600 individual services. We currently have 206 active processing activities listed in our Record of Processing Activities with many more planned or anticipated through the Customer First programme. This illustrates the challenge the new legislation presents to the smaller local authorities when compared to large multi-nationals who carry out fewer but more highly-intrusive activities.

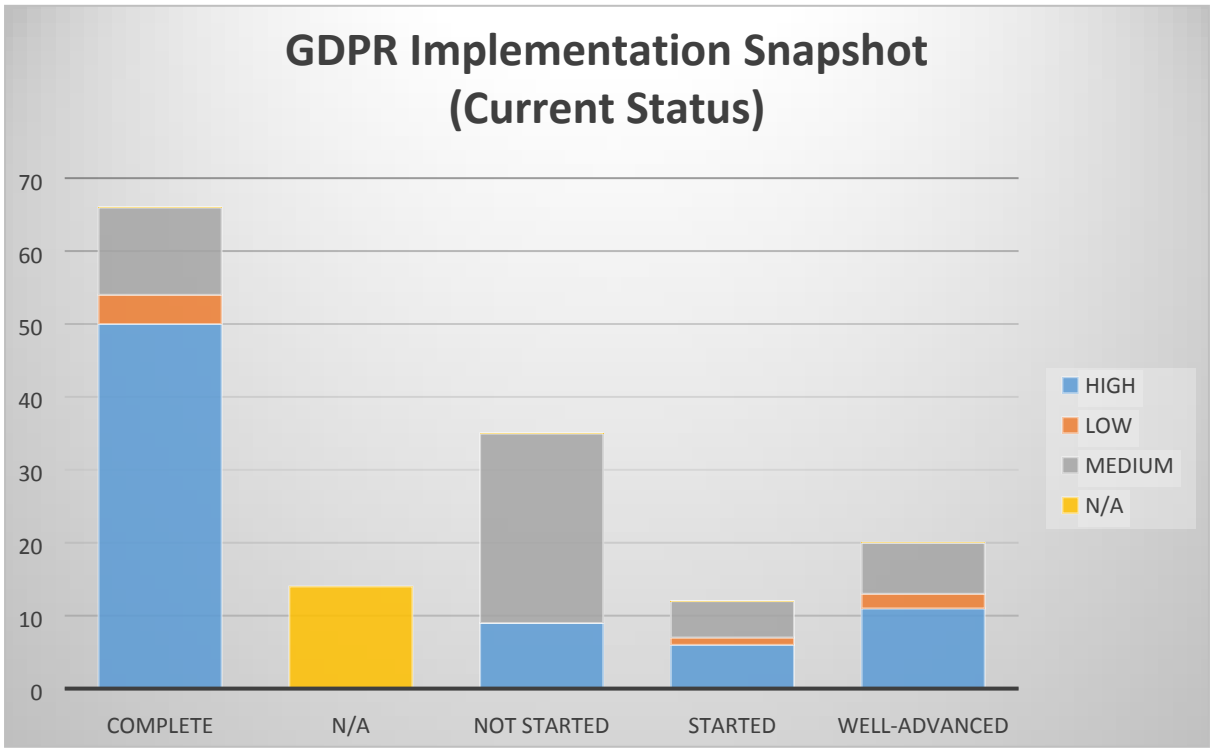
4.2 The ICO describes compliance with GDPR as “evolution, not revolution” and they have said

they will not use enforcement as the preferred tool where organisations can evidence progress towards full compliance. No-one should assume that the work we have done and the progress we've made makes us "GDPR-compliant". We are still a long way from that but anecdotal evidence suggests we are further along the journey than most.

4.3 With this in mind we can be cautiously confident that the work we have done so far and the progress we are making will minimise our exposure to the risk of enforcement action over the coming 12 months or so.

4.4 The following 2 charts show the status with regards the GDPR Implementation Project Plan actions reported to Management Team on 24 Sep 2018 and the current status. They provide a good indication of our progress towards full compliance



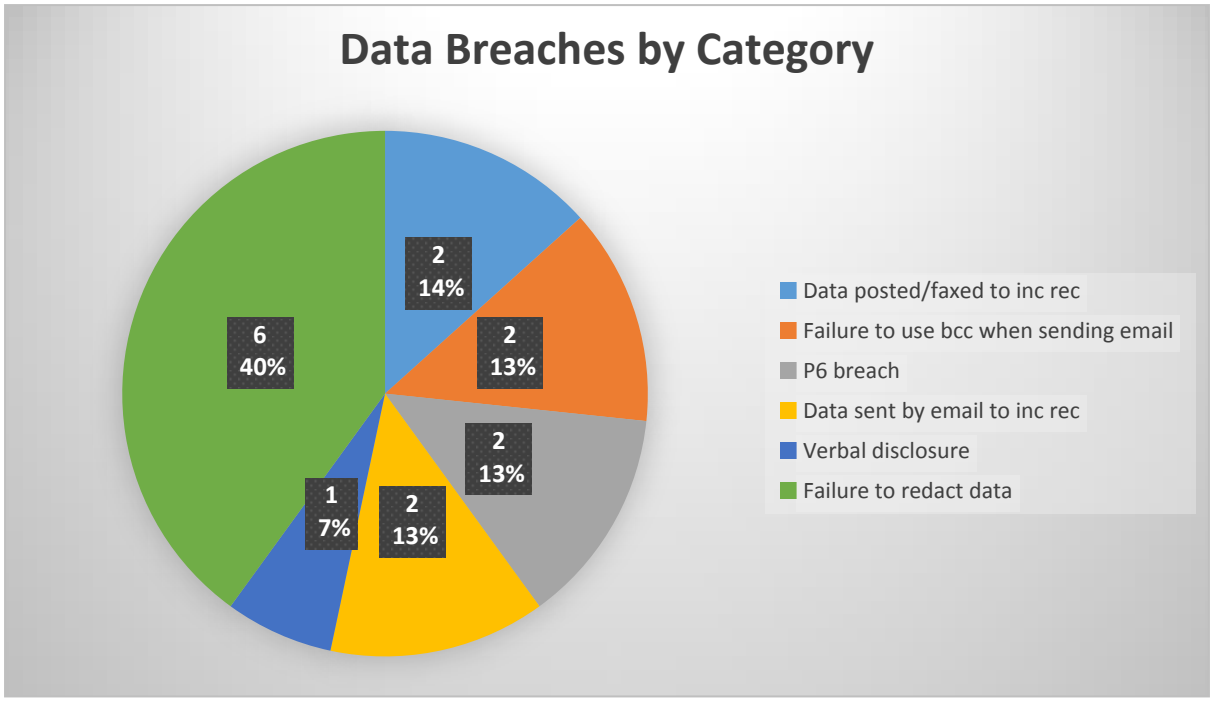

GDPR Implementation Snapshot
(Current Status)
70
60
50
40
30
20
10
0
COMPLETE
N/A
NOT STARTED
STARTED
WELL-ADVANCED
HIGH
LOW
MEDIUM
N/A

5 Data Breach Statistics

5.1 GDPR requires organisations to have a robust and effective data breach reporting and management process in place. Data breaches that pose a risk to the rights and freedoms of individuals must be reported to the ICO within 72 hours. Breaches that pose a **high** risk must be reported to the data subjects themselves without undue delay.

5.2 A small number of data breaches have occurred in the Council since 25 May 2018 and these are summarised below. Fortunately, with one exception, they have not posed any significant risk to the data subjects affected and, therefore, we have not had to report most of them to the ICO.

5.3 We have, however, reported one breach to the ICO where the contact details of 2 individuals was inadvertently published online. We are awaiting a response.



(Note: “P6 breach” = a breach of the GDPR security principle as defined in GDPR Article 5(f). i.e a risk to the confidentiality, integrity or availability of personal data)

5.4 Whilst it is too early yet to glean any real information from the statistical data, there are a couple of things we can take from them:

- Our biggest risk factor is currently “human error” as opposed to any systemic flaws in our processes and procedures.
- We may need to impose technical controls that could prove unpopular with managers and staff.

5.5 To address these we are developing and improving training materials for staff and consulting on possible implementation of tighter security controls with staff through the Corporate Information Governance Group (CIGG).

6 What do we plan to do next

6.1 General

6.1.1 We must demonstrate over the next two years steady progress towards full assurance and we are developing a programme of work to achieve this. We plan to tackle some immediate and medium-term priorities and introduce a rolling programme of "Advisory Visits" to teams (see Para 6.4).

6.1.2 Whatever we do in terms of compliance, though, has to be balanced with the needs of the Council's business priorities and this could prove a significant challenge over the next 2 years. In the ICO's latest newsletter Elizabeth Denham says *"Across the world people have woken up to the importance of personal data and how it's used. Personal data has become the currency by which society does business, but* ***advances in technology should not mean organisations racing ahead of people's rights*** *– individuals should be the ones in control."*

6.2 Immediate Priorities

1. **Roll out annual GDPR/Cyber Security Awareness and Data Protection training to staff**. Module 1 of the mandatory training has been rolled out to staff. Modules 2 and 3 are scheduled to be rolled out between February and March 2019/

2. **Provide privacy information for full and part-time staff and Elected Members**. We have understandably focussed during our GDPR compliance work on our residents and service customers. However, elected members and employees have the same rights under the new regulation as everyone else. It is important that members and staff are informed about how their data is handled and what monitoring is being carried out.

3. **Consider how members can be assured of data protection compliance when making decisions in committee**. To demonstrate the GDPR principle of "accountability" and to comply with the "data protection by design and default" requirement (GDPR Article 25), elected members need to be assured that privacy has been considered in everything we do before making decisions. In particular, members need confirmation that any processing of personal data they approve is lawful. Adding a field to the committee report template had been discussed and agreed during meetings with the committee admin staff but has not yet been implemented.

6.3 Medium-Term Priorities

6.3.1 **Data Quality**. While monitoring the progress of a recent Subject Access Request (SAR) it quickly became evident that some of the data held in our business systems is of poor quality. This view was supported during a meeting with the Revenues Manager who suggested that multiple records exist of individuals making data searches unreliable. Issues highlighted include:

- Duplicate records of same individual for different services
- Multiple records due to entering names in different formats (ie J Smith; John Smith; J. Smith; Mr J Smith etc)
- Addresses incorrectly formatted or not verified to the LLPG
- Out of date records not being archived or deleted

6.3.2 The requirement to maintain accurate data is a fundamental principle of GDPR. Corrective measures will be agreed and included in individual team action plans developed during the advisory visits detailed in para 6.4.

6.3.3 Data Protection Toolkit for Managers and Staff. A lot of work has been carried out to prepare for GDPR. This has included developing training materials, recording systems for processing activities and data breaches, and various guidance and templates for use by managers and staff. This needs to be pulled together into a "Data Protection Toolkit" to provide a "one-stop-shop" for managers and staff.

6.4 Advisory Visits

6.4.1 As previously mentioned, we carried out a series of audits with teams to assess their GDPR-readiness. From these we provided them with a set of recommendations and actions.

6.4.2 Starting in October the DPO started a rolling programme of "Advisory Visits" to teams. These visits look at progress on the audit actions and examine in more depth the activities and processes to measure compliance and consider potential improvements.

6.4.3 To direct the visits, the DPO has adapted a set of checklists which the ICO provided primarily to support SMEs. The DPO will maintain a set for each team.

6.4.4 The checklists cover:

- Data Controller Actions
- Information Security Actions
- Records Management

- Data Sharing Actions
- Subject Access Actions
- CCTV Actions

6.4.5 A reporting system has been developed to present the findings for each service team, the management team, Human Resources, ICT and Corporate Policy.

6.4.6 The Records Management checklist will be brought into use when the new Information Architecture has been agreed and the new SharePoint system has been implemented.

6.5 Follow-up Audit

6.5.1 To provide the management team with added assurance that the organisation is continuing to move in the right direction towards full GDPR-compliance, Internal Audit have been invited to carry out a follow up audit in the New Year.

7 Conclusion

7.1 This report summarises the work we have done to date and confirms that we are further along the path than some. We recognise, however, that there is still a long way to go and so we have put a realistic plan in place to ensure we continue this progress towards full compliance.