General Data Protection Regulation

Finance Governance and Support – Strategic Risk 08-067

2018/19 Quarter 2 Update

Purpose

- To provide an update to Corporate Affairs and Audit Committee on the strategic risk around the new data protection reforms – the General Data Protection Regulation.

- Description and scoring of the strategic risk identified
- Brief historical context and timeline of the reforms
- Summary of the Council's approach to GDPR thus far
- Similar summary of the future mitigations in progress
- Highlight some other considerations for the future

GDPR strategic risk description

“Failure to have in place a **detailed and documented approach** to the General Data Protection Regulation (GDPR) may result in the organisation **not complying** with the GDPR which could result in a **breach** and **monetary penalty**, **risks to individual safety** and **significant reputational damage**.”
Finance Governance and Support – Strategic Risk 08-067

- The strategic risk is structured around the failure to have a detailed and documented approach, not just non-compliance per say.

GDPR strategic risk scoring

- **Current risk level** is reducing with significant work carried out to date and remaining work being well progressed

- **Target score** will be achieved when all mitigations are delivered and the risk managed down to acceptable levels

- *If* uncontrolled this risk would have a high probability of producing major impacts: service continuity gaps, regulatory enforcements, significant financial penalties (up to £17.5m), and reputational threats, as well as risks to life and limb.

Accountability and evidence

“**Accountability** is central to GDPR. Data Controllers are responsible for compliance with the principles and **must be able** to **demonstrate** this to data subjects and **the regulator**.”
GDPR Article 5 – the Accountability Principle

- Significant work carried out with senior managers across all Council services to document the required evidence
- Training, workshops, business analysis, audits of data, document reviews, substantial amounts of advice provided
- Progressing activity to complete this workstream – but it will evolve as Council services and data management change

Legislation and reforms timeline

Apr 2016 - General Data Protection Regulation approved by EU

Jun 2016 - Referendum vote in favour of UK leaving EU

Mar 2017 - Article 50 invoked, 2-year countdown to Brexit

Jun 2017 - Queen's Speech - intention to implement GDPR

23 May 2018 - Data Protection Act 2018 finally approved

25 May 2018 - GDPR comes into effect 2 days later

- GDPR adoption in the UK confirmed by Government – but organisations have lost 13 months of implementation time
- Data Protection Act 2018 covering critical domestic issues 'derogations' approved 2 days before GDPR comes into force

Internal Audit review

- After Government confirmation on GDPR, Council identifies the strategic risk during Summer 2017
- Critical friend work commissioned from Internal Audit
- All recommendations implemented and addressed by end of January 2018
- GDPR strategic governance and planning strengthened
- Resourcing increased and compliance approach documented

- Internal Audit to undertake a further review in 2018/19

Information security incidents

- 48 incidents were reported in 2017 including 4 that were deemed reportable to the Information Commissioner's Office (ICO)
- Breaches included data posted or emailed to the incorrect recipient, loss or theft of paperwork, and verbal disclosures
- So far in 2018/19 there have been 38 incidents reported including 9 that have been reported to the ICO
- Breaches follow existing trends and similar categories and there has been an increase in the detection/reporting of unauthorised access/disclosure – committed by individuals without permission
- Breach reporting has increased due to stricter rules under GDPR but also due to better awareness and reporting

Current mitigations

1. Project Board and Project Plan in place
2. Workstream Plans developed and in place
3. Externally facilitated and in-house workshops for all managers
4. Current policies and plans ensure partial compliance
5. Updated policies and procedures drafted
6. Data Protection Officer in post from March 2018
7. Training for Information Compliance Team completed
8. Wider training for staff launched with good engagement
9. Awareness Training for Elected Members delivered
10. Data Protection Improvement Plan in place

Future mitigations

10.	Training needs analysis for workforce and beyond	Sep 2018
11.	Updated Management Investigation Policy	Sep 2018
12.	Amend ‘Privacy Impact Assessment’ procedures	Oct 2018
13.	Communications and engagement plan refresh	Nov 2018
14.	Proposals to appoint 1 x Data Protection Assistant	Nov 2018
15.	Data Protection Audit Programme	Mar 2019

Middlesbrough
moving forward

Other considerations

- GDPR compliance will be constantly evolving as a result of changes in legislation, policy, and business decisions
- UK regulator, the Information Commissioner's Officer (ICO), expects a 2-year implementation period from May 2018
- Further impacts from GDPR/Brexit are still expected:
  - 'Adequacy' decision on UK privacy laws from EU needed?
  - A new EU e-Privacy directive expected in 2019?
  - Case law from EU *may* continue to impact UK?
  - National bodies policy/guidance still being updating including some from Government departments