Cabinet Office

'*BUILDING TRUST IN DIGITAL GOVERNMENT*': A REVIEW OF PERSONAL DATA HANDLING IN THE CABINET OFFICE

By Adrian Joseph OBE

March 2020

Contents

Foreword from Adrian Joseph OBE	3
Response from Sir John Manzoni	4
Executive Summary	5
Introduction	8
The policies, processes, practices and culture of personal data handling in the Cabinet Office	13
Recommendations	27
Annex: Methodology Glossary of terms	 34 35

Foreword from Adrian Joseph OBE

It was a pleasure to be asked to lead this Review into Personal Data Handling Culture across the Cabinet Office. Personal data handling has understandably gained significant prominence across the public and private sectors and this will continue as key technologies, including AI, cloud computing and automation, develop at pace.

Data is widely recognised as having the potential to transform government engagement with the public through the development of new digital services delivering improved outcomes for all. This opportunity will be significantly at risk if public trust in the Government's handling of their data is reduced. Breaches, such as that involving the New Year's Honours recipients in December 2019, are not only of detriment to the individuals affected but jeapordise this wider public trust.

The Cabinet Office already processes large volumes of personal data relating to both members of the public and Cabinet Office employees. These volumes are certain to dramatically increase with digitisation and new data usage opportunities. It is essential that the Cabinet Office develop robust structures, processes, practices and a data centric culture to successfully manage these rapidly rising volumes, and to leverage actionable insights which enhance business and societal value.

In this Review we have benefited from perspectives and experiences gathered across the Cabinet Office and more widely. We have also taken a data led approach in conducting qualitative and quantitative research. We have observed areas of good practice but also seen that these are not consistently shared across the Cabinet Office. The Review has, for example, found defined standards and processes in place but also identified concerning lapses such as the use of shared passwords. In a fast changing Department where expectations for data delivery are understandably urgent, this inconsistency of approach raises the risk of further, and potentially more severe, breaches. This is even more pertinent as the Cabinet Office assumes new responsibilities including security vetting.

The recommendations of this Review are intended to extend existing good practice, strengthen both accountability and individual responsibility, and introduce new standards and controls which will make the Cabinet Office a leader in government for personal data handling. Each recommendation has been graded as either a foundational activity that should be acted upon immediately, a strategic initiative requiring organisational implications or as a sustained capability requiring more in depth assessment. I hope that those impacted by recent breaches will take comfort in their implementation.

I am grateful for the candour of all who contributed to this Review. Cabinet Office employees who supported this Review are clearly passionate about improving current capabilities and I trust that this Review will support them in this endeavour. I would also like to thank the Review team who have worked quickly to gather inputs from the wider Cabinet Office and prepared a strongly evidenced set of observations and recommendations.

In conclusion, I believe that the values of the Cabinet Office - Respect, Collaborate and Trust - are directly applicable to the ambitions for personal data handling. Respect for personal data privacy, embedded in collaborative best practices, will build the trust required to deliver on the Government's digital ambitions. I hope that the recommendations within this Review will find wider application across other government departments and agencies.

Response from Sir John Manzoni

I am very grateful to Adrian Joseph for leading this Review into how the Cabinet Office handles personal data.

With today's new technologies, how we use personal data is changing how we work. Sharing personal data more quickly and more easily allows us to make better decisions about the services we offer and how we offer them. But doing so brings some risks that we need to mitigate against. Across the Cabinet Office, we need to continue to handle personal data in ways that are appropriate, secure and protect privacy. Getting that right is not always easy, but it is vital to maintaining public trust.

Adrian has set out in this Review some very sensible recommendations about how we can balance making better use of personal data with more robust safeguards. I commend his Review and welcome his recommendations, particularly about strengthening coordination and levels of knowledge about personal data handling across the Department. We have already taken some steps to do that, but I have asked that we now consider Adrian's recommendations in detail as we take this work forward.

Finally, I would like to thank Adrian and his team for all the hard work they have put into producing such a thorough Review, and to colleagues across the Cabinet Office who have engaged so closely with it. The Review is an excellent basis for strengthening further our personal data handling as we go forward.

Sir John Manzoni
Permanent Secretary to the Cabinet Office

EXECUTIVE SUMMARY

This Review has assessed the policies, processes, practices and culture around personal data handling in the Cabinet Office through 28 stakeholder interviews, 2 surveys and the assessment of numerous artefacts. Capabilities have been found to be mixed, with pockets of best practice identified but with limited coordination or standardisation of controls and processes across the Department.

Breaches, such as the one that impacted New Years Honours recipients in December 2019, are too easily assigned to human error where a greater consistency of process, controls and culture across Cabinet Office could have reduced the risk systemically. There is a significant risk that further and more impactful breaches will occur as the amount of personal data being handled by the Department increases.

The recommendations proposed by the Review will create scalable and sustainable protection in the system, enabling greater confidence in the innovation required for delivering personal data to enable the Digital Government agenda. This agenda crosses government and, as such, these recommendations are also expected to be of wider interest to other departments. Indeed, a number of shared development priorities have already been identified through consultation with other departments carried out by this Review.

Observations

The Cabinet Office has adequate guidance and policies to advise officials on data handling processes, but gaps in governance and organisation remain.

Guidance reviewed reflects the relevant legislation and there were no critical gaps identified but ongoing engagement with the material is limited. The most notable gap in the Department's governance and policies is the absence of a role responsible for personal data handling or information security at Executive Committee (ExCo) level. This lack of clear accountability challenges effective, coordinated and consistent delivery of personal data processing across the Department.

The imminent recruitment of a Government Chief Digital and Information Officer (GCDIO) is expected to address this gap but the Review has also identified opportunities for the existing Cyber and Information Security Risk Committee (CISRC), Government Digital Service (GDS) Information Assurance Office and Data Protection Officer (DPO) to expand on their current remit.

Good examples of processes and controls exist, but inconsistent application and lack of monitoring limit ability to protect against and respond to data breaches.

The primary control on personal data handling and storage appears to be access restrictions to files and inboxes but application of these across the Department is inconsistent. A new Information Asset Register will support identification of personal data stores but growing data volumes and lack of ownership exacerbate the risk of future breaches.

The Review recommends a number of additional controls and processes be deployed to address this, including the introduction of a regular personal data handling assessment across all business units similar to that currently run for records management.

There is considerable variation in the practical delivery of personal data handling processes across teams.

The fluid nature of Cabinet Office business is recognised as a challenge to good personal data handling practice and the Review found that larger, established business units were more effective in applying adequate controls than others. Through stakeholder interviews, the Review also found consultation with the Data Protection Officer typically occurs too late in the process resulting in a lack of personal data considerations being applied across solution design and testing processes. There is also uncertainty on the status of third party data sharing and widespread concerns about the pressure to process data through unapproved Software as a Service (SaaS) solutions.

A refreshed training curriculum, online guidance and approaches to embed data innovation are amongst the recommendations provided by this Review to improve the consistency of practice across the Cabinet Office.

Cabinet Office staff who responded to this Review did so positively and are already identifying improvement actions but more effort is needed to develop awareness across the Department.

The Review received a positive reception and it is clear that there are individuals and teams across the Department highly committed to sustaining and improving data management processes. Experienced employees reported having to resist pressure to circumvent processes so that data processing activities could be accelerated. There are multiple examples of teams being proactive in anticipating, identifying and implementing improvements. When something goes wrong, teams respond quickly and try to fix problems, but there is no single source of guidance on how to deal with a data breach.

The low response rate to the Review's Pulse Survey across all Cabinet Office staff, however, may indicate that personal data handling is not a priority for most. Continued monitoring of this awareness, a refreshed training curriculum and more accountable leadership are amongst the recommendations that have been made to address this.

Recommendations

The Review makes six overarching recommendations that address the behaviours, culture and processes around personal data processing in the Department. Within each of these recommendations the Review details specific actions, providing the components for a roadmap for the Department to implement improvements. The Review has also noted where these recommended actions can be aligned to existing initiatives either being run by the Cabinet Office or other government departments.

***Behaviours* - Recommendation 1: Enhance accountability and governance**

- *Aim*: Establish unified leadership for personal data handling supported by extension of existing best practice delivery in Cabinet Office to increase consistency of delivery.
- *Specific example*: Confirm new Group Chief Data and Information Officer role as accountable for Personal Data Handling culture and controls.

***Behaviours* - Recommendation 2: Reward the right behaviours and recognise skills**

- *Aim*: Strengthen existing business unit responsibilities through active identification and promotion of personal data handling experts.
- *Specific example*: Identify, document and list the names of Cabinet Office staff with significant experience and knowledge of personal data handling on the intranet.

***Culture* - Recommendation 3: Confirm a new Data Strategy**

- *Aim*: Define a new Data Strategy aligned to Cabinet Office values and Digital Government ambitions which will inspire current and future Cabinet Office resource.
- *Specific example: Define strategic design principles and control standards that provide guidance and capture the future value of data usage.*

***Culture* - Recommendation 4: Be transparent on progress**

- *Aim*: Develop the execution oversight and data analysis required to demonstrate progress on maturing data delivery capabilities to all stakeholders.
- *Specific example:* Build a Cabinet Office data incident management system as a single repository of logged personal data handling issues.

***Processes* - Recommendation 5: Refresh Training and Guidance**

- *Aim*: Rebuild Training and Guidance to become accessible on a sustained basis by all Cabinet Office resource.
- *Specific example:* Build an integrated 'how to' guide for handling personal data targeted at all Cabinet Office staff.

***Processes* - Recommendation 6: Establish consistent standards and technology controls**

- *Aim*: Achieve consistent leading standards and controls across personal data handling processes.
- *Specific example:* Undertake urgent action to resolve priority issues relating to the use of shared passwords and inadequate access restriction on Google Drive.

INTRODUCTION

1. Personal data plays a critical role across the Cabinet Office. This can only be expected to increase as the Government's priorities continue to evolve.

2. The Cabinet Office has amassed more than 200 million emails, documents and other digital files since it first began storing such information 20 years ago.[1] This is expected to grow by more than 50 million records a year. Although not all of these will contain personal data, we can clearly expect those figures to increase in tandem. In an organisation with diverse policy responsibilities, high-profile stakeholders and regular staff turnover, the risks involved in processing personal data are significant.

3. On 27 December 2019, the Cabinet Office published the New Year's Honours List 2020 on GOV.UK. During this process, a version of the Honours List was briefly released online which contained address details of some recipients. Action was taken to manage the consequences of this incident, and the Department reported the matter to the Information Commissioner. Conclusions of their investigation will be reported separately.

4. While the General Data Protection Regulation and Data Protection Act have been in force since May 2018, the experience of the Honours incident and other personal data breaches have underlined the importance of continually improving personal data protection in government.

5. On 7 January 2020, the former Minister for the Cabinet Office announced an independent review of how the Cabinet Office handles personal data.[2] It aimed to: review the processes, policies, practice and culture around personal data handling in the Department; establish whether appropriate controls were in place around the storage, sharing and deletion of personal data; and make recommendations to strengthen the Department's behaviours, culture and processes around personal data handling.

Data in the Cabinet Office

While the Cabinet Office does not conduct operational activities on the scale of some departments, such as the Department for Work and Pensions (DWP) or Her Majesty's Revenue and Customs (HMRC), its position at the centre of government brings with it unique responsibilities.

6. The Cabinet Office is perhaps unique in government in the diversity of its activity: from providing the traditional core function of the Cabinet Secretariat in closely supporting No10; to coordinating cross-government issues such as commercial, digital and HR; to leading policy-making on matters such as devolution. Unlike some other departments, the Cabinet Office does not interact with large sections of the public, but data processing in the Department still involves handling significant volumes of personal data.

7. Personal data is handled by several teams in the Department. Alongside regular policy teams, there are a number of areas where personal data protection is particularly important. For example:

1 Based on 2019 Cabinet Office return to the National Archives (internal source)

2 Written Ministerial Statement: https://www.parliament.uk/business/publications/written-questions-answers-statements/written-statement/Commons/2020-01-07/HCWS21/

- **Digital.** The Government Digital Service (GDS) manages digital platforms such as GOV.UK, which acts as a portal for several cross-government functions, though responsibility for data collected often falls to other departments. For instance, 'Notify UK', a system allowing government teams to issue template emails to large customer copy lists, is currently used by more than 1,800 government services.

- **Human resources.** As well as processing data on almost 8,000 employees, the Department plays a wider leadership role across the Civil Service, managing talent schemes such as the Fast Stream and Future Leaders Scheme, and outsourcing pension-related services for civil servants.

- **Security vetting.** From April 2020, the Cabinet Office will assume ownership of UK Vetting Services from the Ministry of Defence. This processes sensitive personal data on a significant portion of the 250,000 individuals who go through vetting every year, including data on relationships, financial affairs and political beliefs.

- **New and changing activity.** Teams are often established within the Cabinet Office to deliver new ministerial priorities or one-off programmes. Some of these will process data on external stakeholders, and units may be set up with challenging delivery timelines, leaving limited time to consider data handling.

Scope of Review

8. This Review considers personal data handling within the Cabinet Office, although the recommendations will be of interest to other government departments, given the importance of personal data handling to wider ambitions on digital government. The Terms of Reference are set out below.

Terms of Reference

The Terms of Reference for the review were as follows:

- To review policy and processes for handling personal information across the Cabinet Office, including in relation to the December Honours breach, to establish whether appropriate controls are in place around the storage, sharing and deletion of personal information. This includes accountability for ensuring compliance within the Department.

- To examine the culture and practice around data handling and consider the adequacy of the process around the publishing of any dataset that includes personal information, including sign-off and safeguards; whilst ensuring continued support for the Government's transparency agenda.

- The Review will be led by Adrian Joseph, supported by a team of officials and will report to the Minister for the Cabinet Office and the Permanent Secretary with recommendations to improve processes, behaviours and departmental culture. An interim report should be provided within a month of starting, with the final report to be received no later than 31 March 2020.

9. Although recent data breaches have reiterated the importance of personal data handling, this Review is not an examination of any individual incident; rather its objective is to create a set of actionable recommendations to minimise the likelihood of a similar event occuring in future.

10. Personal data refers to any information relating to an identified or identifiable individual. An identifiable person is anyone who can be identified, directly or indirectly, in particular by reference to an identification number (e.g. social security number) or one or more factors specific to their physical, physiological, mental, economic, cultural or social identity (e.g. name, date of birth, biometrics data).[3]

11. The Review was led by Adrian Joseph OBE, Managing Director, Group AI and Data Solutions at British Telecom (BT) and a former Non-Executive Director at the Home Office, with several years' experience in technology and data issues across the private sector. Adrian was supported by a small team of officials from across Whitehall and an external consultant with personal data handling expertise.

12. The Review team considered evidence from within the Department on the policies which govern the handling of personal data, the governance which guides decisions on new technologies or processes, and the culture around personal data at an individual level. Efforts to understand the various elements of personal data handling throughout the data lifecycle have been undertaken to make sure robust processes are in place to better protect personal data.

13. This Review was conducted with reference to the General Data Protection Regulation (GDPR) and the Data Protection Act (DPA). These came into force on 25 May 2018, replacing previous data protection legislation.

Areas involved

14. The Cabinet Office consists of more than 30 separate business units. This produces a great variety in the ways in which the Department interacts with personal data. Of these, 28 business units were identified as likely to process a significant amount of personal data, either of individuals within the organisation or outside it. These teams were then risk assessed according to the scale of personal data processed; the sensitivity of personal data held; and the proximity of that data to public-facing functions.

15. As a result, 16 business units were selected and bespoke interviews were held with senior leaders and others involved in data protection at a working level. Evidence was also gathered from particular individuals with expertise in departmental data protection policy, practices, processes and culture, and two evidence-gathering surveys of staff were conducted. Further information and a glossary of technical terms are provided in the annex.

16. The Review did not engage with the Arms Length Bodies (ALBs) to which certain Cabinet Office functions are outsourced. Where these functions involve large volumes of personal data, interviews have been conducted with the internal Cabinet Office teams responsible for overseeing those contracts.

Future risks and opportunities

17. Two years ago the EU General Data Protection Regulation, and the UK Data Protection Act, came into force. This marked a significant change of the legislation governing personal data. These changes were driven in part by a revolution in digital technology and its use of personal data.

3 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data/

18. New technologies, and societal views about data ethics and privacy rights, are changing how organisations use data and how individuals expect information to be secured. In the 2017-2020 Government Transformation Strategy, the Government stated its ambition to use technology to "better understand what citizens need; assemble services more quickly and at lower cost; and continuously improve services based on data and evidence". [4]

19. Ernst & Young recommend five ways in which digital government could bring improvements: by helping government to understand their citizens better and achieve better outcomes; by allowing government to provide services more effectively and efficiently; in finding new solutions to policy challenges; by enabling government to engage with external partners to develop new delivery models; and through commercialising some public services and developing fresh sources of revenue.[5]

20. The use of personal data will undoubtedly play a part in the Cabinet Office's thinking about its use of digital technology. Data protection is one element of that bigger picture. As well as evaluating its adherence to current legislation, the Cabinet Office should consider how it can use data more intelligently, in the Department and across government, to streamline and improve the functioning of government and the services it provides.

Other Government departments

21. The Review team liaised with other government departments to understand how their data handling processes differ from the Cabinet Office and to identify areas of best practice across government. Broadly, other government departments have identified similar issues with their personal data management and are at different stages of implementing measures and controls to make processes more robust.

22. The Department for Digital, Culture, Media and Sport (DCMS) leads on data policy, including the data protection framework. Following implementation of the GDPR and DPA, DCMS led on reviewing cross-government adoption of the legislation and convening the Whitehall community of data protection experts via a Data Protection Officers' Network. This network is now self-run, chaired by Data Protection Officers in DWP and the Home Office (HO), and meets regularly to offer peer-to-peer advice on data breaches in departments, and share best practice.

23. The use of data in the public sector is formally overseen by the Data Leaders Network and the Data Advisory Board, which is chaired by the Chief Executive of the Civil Service, with the secretariat provided by DCMS.[6] The Board is responsible for driving better use of data in government, including via the National Data Strategy. Some departments have also created their own specific strategies. DCMS also runs the Centre for Data Ethics and Collaboration, a unit which connects policymakers, industry, civil society, and the public to develop the right governance regime for data-driven technologies. The Centre is also working with the Automation Task Force in the

4 Government Transformation Strategy (2017-2020): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/590199/Government_Transformation_Strategy.pdf

5 How Does Digital Government Become Better Government? https://www.ey.com/en_gl/government-public-sector/how-does-digital-government-become-better-government

6 https://www.gov.uk/government/groups/data-advisory-board-and-data-leaders-network

Cabinet Office to consider ethical questions and transparency issues around automated decision-making.[7]

24. At a departmental level, one recurring question is where data protection expertise should fit within wider organisational structures. While it often traditionally sits alongside information management or security teams, there is a live discussion as to whether data protection should be established as its own profession.
25. In DWP, the DPO and team sit within their Security and Resilience unit. The Department's compliance with data protection legislation is managed through annual staff training and annual maturity assessments of all business units. Separately, DWP has its own Chief Data Officer (CDO), a Director-level position based in the Department's Digital Group. The CDO is responsible for broader policy questions about digital transformation and automated decision-making, which bring their own data protection considerations, and the CDO leads the departmental data strategy on how DWP can legally and ethically make better use of data. The CDO also chairs the Data Protection Board. Together, these arrangements have reportedly brought significant improvements to the data protection culture in DWP.

26. The Home Office has its own structure to manage data protection considerations. An Office of the Data Protection Officer is complemented by Data Protection Implementation Leads across the organisation, and Data Protection Practitioners are embedded in all business units to report issues and cascade key messages. Decisions are made by a monthly Data Protection Board or escalated to the Executive Committee. In 2019, the Home Office commissioned its own independent review of data protection procedures. This led to a series of recommendations on further improvements to processes, culture and technology in the Department, including setting up a new, central, data protection compliance team. This will allow the Office of the Data Protection Officer to refocus towards its core undertakings of preventative training and awareness raising, incident investigations and management, and compliance monitoring and assurance work.

27. Other government departments have developed distinct governance structures and policies around the use of data, to fit their different needs. Some practices which are appropriate in considerably larger departments may not be feasible in the Cabinet Office. This existing body of best practice, cross-Whitehall expertise, and peer networks should be assessed as the Cabinet Office implements activity to improve their data handling processes.

28. A new Government Chief Digital and Information Officer (GCDIO) role is currently understood as being resourced. Whilst this role will have cross-government responsibilities, it will sit within the Cabinet Office. It is expected that this role will be accountable for personal data handling in the Cabinet Office.

7 https://www.gov.uk/government/organisations/centre-for-data-ethics-and-innovation

THE POLICIES, PROCESSES, PRACTICES AND CULTURE OF DATA HANDLING IN THE CABINET OFFICE

Policies

The Cabinet Office has adequate guidance and policies to advise officials on data handling processes. However, ongoing engagement with the material is limited.

29. The Cabinet Office has issued a number of documents on Cabinet Office Intranet to guide best practice on data handling. This includes the General Data Protection Regulation hub, a guide to Managing Information, the Information Management Standards Framework, the Information Management Policy, the Retention and Destruction Policy and guidance on responding to Freedom of Information Act (FOIA) requests.

30. Whilst different documents exist, they are not regularly updated or promoted throughout the Department. The GDPR Hub, for example, has not been updated since May 2019. Officials are likely to be overwhelmed by the length of most advice on the intranet and could miss vital information amidst the various sources of information. Many officials directly consult the Data Protection Officer for advice.

31. Over the past six months, the GDPR hub landing page has generated 180-250 monthly views, while the first page of GDPR guidance has generated between 100-220 monthly views. Taken as a proportion of the Department this indicates a low level of engagement with the guidance from the officials it targets.

32. The Department's 'Name-Store-Check-Share' policy is a good example of succinct guidance that is both easy-to-follow and actively promoted throughout the Department. It is instituted within the induction process and captures on one page the key records management processes.

The guidance reflects the relevant legislation and, if followed completely, will strengthen compliance across the Department.

33. On the Cabinet Office intranet, there is advice that covers the three relevant pieces of legislation: the Data Protection Act (2018), which legislated for derogations to GDPR, extended it to areas outside EU competence, and implemented the Law Enforcement Directive; the Public Records Act (1967); and the Freedom of Information Act (2000).

34. The GDPR hub covers the DPA (2018) and the Department's personal data charter sets out the standards customers can expect for the collection and management of their personal data. In addition, the Department's information management policy and guidance are intended to support compliance with the Public Record Act (PRA 1958) and the guidance on responding to FOIs follows the instruction of the FOIA (2000) closely.

35. No critical gaps were observed in this guidance. However, there are vulnerabilities in the accessibility of the guidance and the extent to which it is engaged with and implemented by officials. For example, one newly formed team had created none of the relevant GDPR documentation for the personal data that they were managing, despite being aware of likely obligations under GDPR.

The Cyber and Information Security Risk Committee (CISRC) provides oversight of data handling and has potential to provide more practical support to business units.

36. The Government Security Group sets cross-government security policy and in November 2018, it issued guidance that removed the requirement for a Senior Information Risk Owner (SIRO). As a result, the Cabinet Office abolished the role of SIRO and the SIRO working group. The SIRO had served as a central point of contact for information security queries that exceeded the Department's risk appetite.

37. Risk ownership was instead devolved to the relevant Board member. The Information Assurance Policy, issued on the Cabinet Office intranet in July 2019, gave business unit heads decision-making responsibility - many of which are Board members. Business unit heads were empowered to take decisions on data handling, seeking advice from the Cyber and Information Security Risk Committee where appropriate.

38. The nature of the Cabinet Office's unique structure has meant that devolving accountability to individual business unit heads creates a particularly disparate governance structure.

39. The Cyber and Information Security Risk Committee brings together the Cabinet Office leads in Information Assurance, Cyber Security, Data Protection and Technology. Its purpose is to understand, review and provide advice in relation to information and cyber security risks. It is chaired by the Senior Security Advisor. In bringing together the relevant internal experts, it serves as a vehicle to simplify and coordinate the complex data handling landscape across the various disciplines.

40. As a practical resource, CISRC is under-utilised by the Department. The SIRO working group regularly advised officials on data handling and information assurance concerns. While CISRC provides policy oversight, its component parts do not necessarily have the capacity to execute the policy and provide advice to business units. This is largely because awareness of CISRC and its advisory role throughout the Department is low. This is expected to improve when the team is bolstered in the next few months by a new Head of Information Security.

The Department has one full-time internal data protection resource.

41. Unlike other departments, the Cabinet Office has no corporate data protection team. All data protection advice is currently provided by lawyers or the Data Protection Officer, a statutory office required to carry out its tasks in an independent manner. The DPO is supported by a network of GDPR leads in each business unit, but their GDPR responsibilities are in addition to their existing job roles.

42. The DPO informed the Review team that whilst he regularly assesses his resourcing needs for his statutory function, the Department would benefit from additional corporate data protection resources. The Action Plan produced alongside this Review has drafted a proposed RACI to be consulted on and implemented. This should provide relevant corporate data protection resource.

43. Greater coordination of data protection resource could support the DPO's existing work and more proactively drive a consistent approach to data handling in the Department.

The GDPR lead, Information Management Lead (IMLs) and Information Asset Owner (IAOs) networks represent significant experience but are not consistently available across the Cabinet Office.

44. Within each business unit, there should be a designated GDPR lead, IAO and IML. The GDPR lead should lead on implementation of all necessary GDPR controls; the IAO is responsible for ensuring that information assets are handled and managed correctly; and IMLs drive best practice on records management. In some cases, these responsibilities will be assigned to one person. These representatives serve as vital links between the central experts and the officials more generally, but the Department should increase the visibility and credibility of the leads.

45. Typically, these in-team experts are junior members of staff and, although many of them carry out their roles diligently, they have little authority. Delivering against the objectives of the role description is not generally considered as part of formal or informal feedback. High staff turnover in the Cabinet Office has led to incomplete coverage across the networks. By comparison, the Knowledge and Information Management team has developed a high level of engagement and compliance across its IML network by instituting quarterly assessments and mandating that IMLs are Band A or higher.

46. Our survey of GDPR leads reveals that they are confident in producing and handling relevant GDPR documentation and most have completed some relevant training. They are clear about the most appropriate routes of escalation, with 96% identifying the DPO as the person they consult most regularly. Responses indicate that teams are generally very receptive to conversations about personal data processing. Leads identified a renewed training programme and clearer central guidance as the most effective measures to improve personal data processing.

47. Officials who do not handle personal data regularly are unlikely to distinguish between the roles of each lead so the Department would benefit from greater coordination between the networks.

There is currently no accountability at the most senior level for data handling or information security.

48. At present, no Cabinet Office Executive Committee (ExCo) member has been assigned responsibility for data handling, with the risk devolved to individual business unit heads as per the Government Security Group (GSG) guidance. CISRC and the associated internal experts provide sufficient oversight and support, but the governance would benefit from defined representation at ExCo.

49. This would provide a clear escalation route for data handling concerns, demonstrate the Department's commitment to good data practice and enable more effective communication to the Department at large. Defined representation would also ensure data handling is a strategic priority and is properly resourced.

50. Responsibility for data handling and information security would sit naturally with the incoming Government Chief Digital and Information Officer.

Processes

51. The Review has investigated what processes exist within the Cabinet Office's data management lifecycle. There are examples of processes and controls throughout the Department that protect personal data, but standardisation of these processes is limited. There are also notable process gaps that limit the Department's ability to protect against and respond to data breaches.

The primary control on data handling and storage are access restrictions to files and inboxes but their application is inconsistent.

52. Google Drive is the standard platform for all OFFICIAL and OFFICIAL-SENSITIVE information within the Cabinet Office. Information ranging from research, policy submissions, corporate information, HR data and other personal data is held on the platform.

53. Throughout the Review, business units identified access restriction as a common control to protect personal data. Using the functionality of Google Drive, teams limit access to personal datasets and sensitive inboxes to specific individuals. In one team interviewed, access restrictions are removed immediately after individuals leave the team and the most sensitive personal data is restricted to just two team members.

54. Across the board, however, such restrictions are often imposed too late and there are examples of personal data being accessible to whole teams. One business unit has run its recruitment process through an inbox with few access restrictions and subsequently held personal HR data, including some special category data, in a file accessible by the entire department.

Whilst regular assessments take place on records management, there are no similar processes in place for personal data management.

55. The process of regularly assessing teams is a useful control and makes sure teams actively engage with data handling policies. The Knowledge and Information Management team asks its network of Information Management Leads to complete quarterly self-assessments of their business unit's information management. The assessments are validated and moderated by the central team scrutinising the business unit drive. There is also no senior oversight from the business unit, so that IMLs feel no pressure to present an exclusively positive picture. IMLs are then given compliance action points to improve practices.

56. The Cabinet Office's information management has been assessed as Green by the National Archive representing a 'good level of assurance' that the Cabinet Office's information management is 'positioned to support efficiency, effectiveness and compliance with legal obligations'. Replicating these assessments for the work of GDPR leads and IAOs would build more protection into the system and ensure that data handling is a high priority for teams.

A number of teams have good processes for protecting the most vulnerable users.

57. Across the Department, there are pockets of best practice regarding the personal data of vulnerable customers. Individual teams have built controls into their data management processes that identify vulnerable people, protect their data and ease their interaction with government.

58. One team has established a direct line of communication with the Police, DHSC and DWP, passing cases involving vulnerable citizens to the most relevant authority. This has developed organically, and the team is now turning the process into a specific policy. Only two staff members can make the decision to pass a vulnerable case on, and consent is secured via a relevant Privacy Notice. The same team had a person dedicated to providing quality assurance on all documents and is currently migrating to a new system that automates their process and further protects personal data.

59. Elsewhere, research into how citizens interact with government digital services is set to focus on vulnerable stakeholders this year. The research will ensure people are not excluded from interacting with government online, and measures have been put in place to protect any personal data included in the findings.

Only limited testing of personal data handling processes was observed.

60. While examples of best practice exist within the Department, there are no standard testing controls in place throughout the data management life cycle. Data Protection Impact Assessments (DPIAs), Privacy Notices and Record of Processing Activity (ROPAs) are required for each new personal dataset, but there is limited guidance on controls that teams can use to test the accuracy of personal data before storing, sharing or publishing it.

61. One team has built robust quality assurance into its processes, with a team member responsible for checking each piece of personal data being shared, and a final check undertaken by another individual who hasn't been involved with the document. In another team, any dataset that generates a ROPA is given a corresponding retention trigger notifying the owner that destruction should be considered. Compliance with this is dip-tested annually to ensure documents are kept for only the stated periods.

62. Recommending similar controls as standard would improve personal data processing across the Cabinet Office.

The absence of a personal data inventory makes breach risk assessment challenging but the new Information Asset Register should help mitigate this.

63. At present, the Cabinet Office has a list of 'high-value datasets', owned by the Security team, but this is narrow in scope and is not regularly updated. Without a definitive record of the datasets across the Department and an indication of whether or not they contain personal data, it is difficult to measure risk and institute appropriate mitigations.

64. Individual teams are encouraged to save relevant GDPR documents (such as DPIAs and Privacy Notices) in a specific GDPR folder in their drive, but these are not drawn together into a coherent picture of the whole Department's data profile. Compliance with this policy is also sporadic, with some teams unaware of the obligation.

65. A new Information Asset Register is currently in development, due to roll out across the Department in the next few months. For each new dataset created, it will identify: name of dataset; owner; content; security classification; who has access; whether it is personal identifiable information; how it is used; whether GDPR checks have been carried out. It should improve the Department's understanding of its own personal data assets and associated risk exposure.

66. For it to be most effective, IAO leads must input information on all existing datasets once the register launches.

No central repository for information security breaches exists, making it difficult to respond quickly to breaches and learn from previous experience.

67. A central log of past data breaches would improve the Department's ability to respond effectively. Officials would be able to understand what immediate actions were taken previously, how effective they were, and identify improvement actions to reduce future risks. This should clearly identify personal data breaches and account for the specific measures required in these cases.

Growing volumes of orphaned data and 'digital hoarding' leave the Department vulnerable to further breaches and weakens its ability to comply with FOI and public records requests.

68. In the Cabinet Office, it is common that new teams with short-term priorities are stood up and subsequently folded once the Ministerial priority has been met. This, combined with an unusually high staff turnover rate, creates a large amount of 'orphaned' data, or data with no owner, within the Department.

69. 'Digital hoarding' is also common throughout the Department, with officials taking a 'just in case' approach to retention and destruction decisions rather than following Cabinet Office policy.

70. Both practices contribute to the creation and retention of large datasets. Under the Public Records Act, records of historical interest must be transferred to the National Archive after 20 years. Once transferred, files may be 'opened' (i.e. available for public inspection) or 'closed' (i.e. not available for public inspection). These Records must be checked for sensitive or personal information, so digital hoarding and orphaned data makes these decisions unnecessarily arduous.

71. The Knowledge and Information Management team have agreed a three year project to create a Departmental Digital Archive that enables full and effective searches of the 205 million data objects, disposal of information based on long term value and personal data identifiers and knowledge exploitation. The current estimate for delivering this Information Management Strategy is £5m and this will be subject to a Spending Review bid in 2020.

Practice

72. In order to measure how well these policies and processes are followed in practice, the Review conducted 28 interviews with key internal stakeholders and business units. Business units were selected on the basis that they handled either particularly large or sensitive sets of personal data, and covered a wide variety of disciplines. Whilst the Review found examples of good practice across the Department, there was a lack of consistency in how closely business units adhered to central policies and there was considerable variation in practical application across teams.

73. Some of the most common barriers to delivering good practice in data handling included: the fluid nature of much Cabinet Office business, with new teams often set up rapidly and at short notice; limited staff and budgets; and the lack of central oversight and accountability for proper data handling.

Expected pace of delivery and capacity challenges were often cited as an impediment to better data handling.

74. Cabinet Office structures regularly change with new business units often being stood up to deliver on urgent political priorities. The pace required to deliver on these priorities was cited by some business units and stakeholders as potentially compromising the disciplines of good personal data handling.

75. Some of the larger business units also cited lack of capacity as having a negative impact on the quality of their data handling. Interviewees mentioned both overall resourcing and persistent staffing gaps. In some cases this meant teams adopting random testing rather than conducting full quality assurance checks on every transaction; in other cases it meant supervisors accepting an unknown degree of error; in others it meant incomplete records of data assets.

Some issues are attributed to human error without considering that the risk could be reduced or eliminated through better procedures or technology solutions.

76. Some teams have built additional checks into their processes, including validating data which is being transferred between government departments, protocols for double and triple checking (by different individuals) before data is used, and additional 'sensibility' checks. These processes help to eliminate much human error; however, in some instances it would be possible to eliminate human error altogether by fixing failings in IT systems. For example, in one software system it is possible to accidentally send personal information about one individual to another, unconnected, individual whose details are also held in the same system.

New Year's Honours breach

On 27 December 2019, the Cabinet Office published the New Year's Honours List 2020 on GOV.UK. During this process, a comma separated variable (CSV) version of the Honours List was released online which contained address details of some recipients. This document was online and accessible for approximately 40 minutes before the error was identified and the link removed (although the document was still available to those who knew the specific URL address for a further 150 minutes). Action was taken to manage the consequences of this incident, and the Department reported the matter to the Information Commissioner. Conclusions of their investigation will be reported separately.

The Cabinet Office identified two main factors that had contributed to the breach: the introduction of a new IT software package, which had included an additional field with individuals' addresses; and a lack of clarity about sign-off processes for the final versions of the documents that went online, and in the context of the new IT system. The Cabinet Office recommends that steps be taken to make sure that the process for removing documents published in error, including out of hours, is more clearly understood across the Department.

It is highly likely that Cabinet Office teams will hold personal data sets that are not appropriately defined as such.

77. All business units hold at least a small quantity of personal staff data on their shared Google Drives. Interviewees also mentioned data sets such as lists of business stakeholders and guest lists. Very few teams had considered whether or not they were protecting this information adequately, and some had not identified it as personal data.

The Data Protection Officer is rarely consulted early enough about new processes.

78. Most business units in the Department consulted the DPO before implementing new data handling process. However, this consultation rarely took place before the design phase and often occurred just before deployment, with teams effectively using the DPO as a check that they had carried out the relevant GDPR-related assessments correctly. Examples of problems that could have been mitigated with earlier DPO involvement include sensitive data being shared over email, inadequate access restrictions, and incomplete Privacy Notices.

79. The Data Protection Officer is diligent in reaching out to new teams, offering both initial discussions to guide any data handling they might need to undertake, and signposting information and guidance. The Review interviewed some newer business units which had been set up at pace and, despite having been contacted by the Data Protection Officer, none had yet followed up with him. The primary reason shared was that the meeting was not a priority given their units' perceived low volumes of data handling and other pressures on staff time. All these teams confirmed that they were responsible for processing personal data, some in large quantities; in a few cases, this also included sensitive data.

Whilst some teams follow processes for implementing the statutory aspects of data processing legislation, most do not.

80. Where data handling was a core business function, the Review saw evidence that teams had processes in place designed to make sure they complied with policy and legislation. These included completing a Record of Processing Activities and a Data Protection Impact Assessment for each process, and issuing Privacy Notices. Some teams reviewed this documentation on a regular basis - usually annually - but others said the paperwork had been completed when GDPR came in and had not been reviewed since. One team was about to introduce a new software platform and said they would refresh their documentation in tandem. All these teams were in regular contact with the DPO.

81. Teams that did not handle data as a core function did not routinely complete any of these tasks. Most could point to standard Privacy Notices that they thought would cover aspects of their work, although they had not been checked. Some teams had occasional contact with the DPO although this was largely in reference to Freedom of

Information or Subject Access requests; other interviewees did not know the Department had a DPO.

The Government Digital Service was recently audited by the Government Internal Audit Agency, which commended the team on the rigour of its GDPR-compliance. DPIAs are completed as standard and feed into Article 30-compliant ROPAs which are stored in a secured drive. The quality of the data is checked by Privacy and Information Assurance teams within GDS before the ROPA is created. Privacy Notices are also produced as standard. Anything that passes through a ROPA is given a corresponding retention trigger by GDS and Information Management teams. These are audited annually to ensure documents are kept for only the stated periods. A GDS staff member is now embedded within the Digital and Technology Team, to help embed GDS standards as the benchmark for the rest of the Cabinet Office.

Teams with more experience of data handling have checks built into their processes and defined triggers for escalating risks; other teams do not.

82. Experienced teams were able to explain in detail how they monitored their data handling processes, including checking the quality of incoming and outgoing data, checking that data was tagged and cross-referenced accurately, and making sure data was stored correctly and for no longer than necessary. Some of these teams also had predefined trigger points to escalate decision-making on whether or not specific data handling actions could take place.

83. Conversely, very few other teams interviewed had considered what controls were needed for their data handling. Most of their activities were carried out on an ad-hoc basis and individuals were trusted to handle data sensibly and appropriately. This inevitably meant that actions were not always carried out in a consistent or appropriate manner, such as personal data being shared on occasion via email rather than through a secure portal.

Most teams give some thought to how they store and process data, although these activities are not carried out consistently across the Department.

84. The Cabinet Office's 'Name-Store-Check-Share' policy was recognised across the Department and staff seemed to be effectively using standard naming conventions for official work. Staff also demonstrated diligence when storing information at the right security classification, thinking about who needed access to it, and were aware of the need to set access restrictions in Google Drive on files, folders, mailboxes and calendars.

85. Teams were less consistent in establishing Google Drive structures that met information management guidelines, tagging personal data on any system, conducting regular reviews of shared drives to check access restrictions and to destroy documents that were no longer required. Of those teams which did review shared drives regularly, most said they did not include inboxes and emails in this activity.

86. There were particular inconsistencies in how quickly teams removed access permissions when staff left or moved teams. In the most concerning cases, the Review saw access given indiscriminately to large groups of people, and passwords being shared.

Some teams have improved their data handling processes by implementing simple checklists, which have helped both to protect institutional memory and to make sure different team members carry out the same tasks consistently.

Particular concern was raised regarding legacy systems and storage of data.

87. A number of teams hold data in both paper and electronic systems. In some cases this is because of the classification of the material or because the information pre-dates an existing computer system. In others it is because staff find it easier to work from paper files or because they do not trust the electronic system so keep paper files as a back-up.

88. Much of this hard copy information is not protected sufficiently, owing to a lack of space and a lack of appropriate storage facilities across the Cabinet Office's Whitehall estate. Where it was possible to do so, some teams were good at regularly sending physical files to archive. However, other teams could not do this as the files were needed on a daily basis.

89. There are also a number of legacy electronic systems to which no one in the Department currently has access. In most cases teams do not know the volume or sensitivity of the data held on those systems. The teams in question are working with IT and Security to decide what to do with these legacy systems.

Concerns exist that the risks of data being transferred outside the Cabinet Office are not being consistently addressed.

90. Some data analysis is conducted by third party providers, amongst which there is a wide variation in size and capability. Third party contracts do include compliance expectations and data protection impact assessments. There is, however, no central oversight of all contracts in place across the Cabinet Office and therefore no assurance that these controls are consistently in place. One team acknowledged that they did not conduct such robust quality checks on their third party processors as they did internally, as they assumed this was being handled elsewhere.

91. In some instances the Cabinet Office was a data controller for data processed by a third party, and staff had set up firewalls and defined the different responsibilities owned by each party. However, some teams which shared data with other government departments said they were not clear where their responsibility for the data ended, or how much assurance they should be carrying out of other departments' processes.

The Cabinet Office's Commercial team includes Information Assurance specialists who ensure that robust security and privacy schedules are included in their contracts with third party providers. These are terms that specify how third parties can use data and the controls they must have in place to do so. The template privacy schedule was drafted in collaboration between the DPO and Crown Commercial Service.

For contracts that include storing and processing personal or sensitive data,the security schedules in the contracts require the third party providers to undertake annual penetration testing, designed to identify any security vulnerabilities that could be exploited by an attacker. If vulnerabilities are found, the provider has to implement

remedial measures. The team is considering whether it could include commercial penalties to incentivise good compliance from suppliers.

Software that is not included on Cabinet Office hardware at point of issue is used widely across the Department with little oversight.

92. Many Cabinet Office staff use free versions of online tools which have not been subject to information assurance checks, meaning that in some cases data is de facto shared with providers. One interviewee remarked that 'officials with credit cards' posed the biggest risk to the Department, procuring Software as a Service (SaaS) products freely, with no consideration given to subsequent data risk.

93. This was particularly common with the use of Software as a Service (SaaS) products such as SurveyMonkey and Trello. They are used widely (either paid or free products) with very limited controls to protect data.

New technology can improve data handling, but risks arise when process requirements are not properly defined at the outset, when systems are not tested robustly, and because of incompatibility between government IT systems.

94. Interviewees raised a number of concerns around the procurement of new software to run their data handling processes. Some said that financial considerations meant that off-the-shelf solutions were chosen to run processes that, given their complexity, warranted bespoke solutions. Some individuals felt that any initial cost savings were not borne out long term due to the costs incurred in fixing problems or even re-running projects that had failed first time.

95. Another concern raised by a number of teams was that software had not undergone sufficiently robust or extensive testing in advance of being rolled out. The reasons cited included lack of both staff and money, lack of expertise within the commissioning teams, and projects being rolled out too quickly in order to meet Ministerial commitments. In all instances considered by the Review these risks had been signed off by senior managers or Ministers.

Culture

There is potential for a positive data culture in the Cabinet Office, focused on best practice that embeds data processing at the outset of a project.

96. The Review received a positive reception and interviewees conveyed a broad appetite for improving personal data processing in the Department. There are a number of internal experts throughout the Department who are committed to instilling a better data culture.

97. However, both the interviews and the responses to the Pulse Survey reflect the fact that personal data handling is not a priority for a large proportion of the Cabinet Office. We received 485 responses to the Pulse Survey - a response rate of less than 7% of the more than 7,000 staff in the Department. Similarly, there were multiple examples during business unit interviews in which personal data protection had been considered only as an afterthought, if at all.

Cabinet Office staff who responded to the Pulse Survey appear confident that they process data according to departmental guidelines and know who to consult for support. This is not reflected by practical awareness indicators.

98. In responding to the Pulse Survey, 65% of respondents said they were confident or very confident that the way they process personal data reflects the legislation and Cabinet Office's own guidelines. However, a smaller proportion of 56% felt they knew who to consult if they were unsure about how to apply those guidelines.

99. Most Cabinet Office staff that were interviewed by the Review demonstrated general awareness that care was needed when handling personal data. However, there is great variety in how much people think about this on a day to day basis, and the extent to which they recognise that data is sensitive. 37% of respondents to the survey said personal data processing features in their work daily, and a further 22% of respondents said it featured weekly.

100. Interviews with staff in teams which regularly handle large amounts of data on a daily basis revealed that they are generally familiar with forms and processes relating to the GDPR, such as Record of Processing Activities and Data Protection Impact Assessment and could provide details of the Privacy Notices relating to their work.

101. Most staff from other teams had not heard of either a ROPA or DPIA, but could answer questions about whether or not there was a Privacy Notice. In general, policy teams have little or no contact with the DPO. However, most staff were confident they would find the information they needed in the guidance on the staff intranet.

102. Some teams handle data but are not responsible for creating or storing it, and hadn't thought about whether or not they were meeting their obligations for handling personal data. Not all teams have GDPR leads. The Review surveyed GDPR leads, issued to 30 business units listed in the GDPR lead network. Of these, 25 responded and only 22 respondents confirmed that they were the designated GDPR lead for their team.

Information management is prioritised in staff training policy, but this training is not monitored.

103. There are seven mandatory training courses which must be completed by all Cabinet Office staff, including contractors. Of these, only the 'Responsible for Information'

course is mandatory on an annual basis[8]. The previous Civil Service learning and development platform allowed managers to monitor whether or not their team members had completed mandatory training, but the new system no longer provides this function and training is not monitored across the organisation. One team interviewed for the Review had set up their own training log, but most did not actively monitor which members of their teams had completed the training.

104. Beyond mandatory training, there is appetite in the Department for more advanced training for those with specific data handling responsibilities. In our survey of GDPR leads, a renewed training programme was identified by 79% of respondents as a measure which would make it easier for GDPR leads to manage personal data handling in their teams.

When something does go wrong teams respond quickly and try to fix problems, but there is no single source of guidance on how to deal with a data breach.

105. Most teams we spoke to were aware of their responsibilities for reporting breaches, or knew where to look for guidance. Breaches are reported to the Security team, which decides whether to refer to the Information Commissioner's Office, based on advice from the DPO. Breaches are investigated internally and there is evidence to suggest that teams try to implement remedial measures quickly. There is no central guide, however, to instruct staff in what further action they should take.

Examples of teams being proactive in anticipating, identifying and implementing improvements were observed.

106. In discussions with various teams, there were multiple examples of proactivity that improved processes:

- GDS is planning to share their expertise with other government departments to improve best practice in cookie management.
- The Civil Service HR team is moving all 350 government employers onto a standard interface so they only need to collect data that is relevant to their processing of employee pensions.
- The Security team has improved their record keeping relating to equipment, passes and building access.
- The Correspondence team is considering how to maintain and improve on their retention and destruction policies as their team expands and moves onto a new electronic system.
- Despite being exempt from many of the requirements of GDPR, the Honours team has implemented a number of changes to their processes to ensure they collect and hold only the minimum data necessary at any given time.

Some individuals did report having to be robust in resisting pressure from colleagues to use and share data in ways that do not comply with legislation.

107. A number of interviewees commented on a growing appetite in government to provide external data processors with personal data. This ranged from teams who wanted to use data for analytical purposes, to external stakeholders who wanted to promote services to civil service employees. Teams were good at recognising inappropriate requests for data, but also kept an open mind on recognising potential opportunities for

[8] The other six training courses are: Diversity and Inclusion, Resilience and Wellbeing, Becoming Disability Confident, Mental Health at Work, Health and Safety, Counter Fraud, Bribery and Corruption

government.

108. This growing pressure for rapid data access puts information management resource under stress. Our interviews suggest that experienced staff members who deal with personal data regularly are well equipped to insist on applying the relevant standards despite considerable pressure for a speedy delivery. However, the low response rate to the Pulse Survey does not provide confidence that such standards will be applied consistently.

RECOMMENDATIONS

Key recommendations

Behaviours

Recommendation 1: Enhance accountability and governance
Aim: Establish unified leadership for personal data handling supported by extension of existing best practice delivery in Cabinet Office to increase consistency of delivery

Recommendation 2: Reward the right behaviours and recognise skills
Aim: Strengthen existing business unit responsibilities through active identification and promotion of personal data handling experts

Culture

Recommendation 3: Confirm a new Data Strategy
Aim: Define a new Data Strategy aligned to Cabinet Office values and Digital Government ambitions which will inspire current and future Cabinet Office resource

Recommendation 4: Be transparent on progress
Aim - Develop the execution oversight and data analysis required to demonstrate progress on maturing data delivery capabilities to all stakeholders

Processes

Recommendation 5: Refresh Training and Guidance
Aim: Rebuild Training and Guidance to become accessible on a sustained basis by all Cabinet Office resource

Recommendation 6: Establish consistent standards and technology controls
Aim: Achieve consistently leading standards and controls across personal data handling processes

Detailed recommendations

Each recommendation includes a number of detailed actions. Each action is rated on a scale based on relative complexity:

- Foundational Priorities - tactical and/or urgent activities that can be actioned immediately;
- Strategic Embedding - more strategic activities that may involve organisational impact and cost;
- Sustained Capability - activities that will deliver most sustained impact but with cost implications that require further analysis.

Behaviours

Recommendation 1: Enhance accountability and governance
Aim: Establish unified leadership for personal data handling supported by extension of existing best practice delivery in Cabinet Office to increase consistency of delivery.

Action	Grouping	Category	Detail
1	Implement Unified Leadership Accountability	Strategic Embedding	Confirm new Government Chief Data and Information Officer (GCDIO) role as accountable for Personal Data Handling culture and controls. This will confirm ultimate accountability in a new senior leadership role.
2	Implement Unified Leadership Accountability	Strategic Embedding	Extend existing Cabinet Office Data Protection and Information Assurance teams to provide coverage across the whole Department. This will provide necessary coverage for expected increase in personal data handling. Consideration should also be given to extended functions' reporting line accountability into the new GCDIO, noting the criticality of DPO retaining an independent role. Once new operational remits are established, consideration should be given to strengthening the Governance role of CISRC as an escalation body.
3	Formalise Individual Accountabilities	Foundational Priorities	Formalise expected personal data handling role responsibilities across the Cabinet Office, including: - New guidelines for minimum role expectations in each business unit - A new IAOs network to identify risks and efficiency opportunities - Mandatory personal data handling attestations for all resource at onboarding and annually - Implement the RACI defined in the

			information security Action Plan, establishing corporate data protection resource
4	Assess Accountabilities for Cabinet Office Arms Length Bodies	Strategic Embedding	Extend Personal Data Handling Culture Review to Cabinet Office Arms Length Bodies. Identify priority areas for remediation and revised approach for establishing future ALB data handling processes.

Recommendation 2: Reward the right behaviours and recognise skills
Aim: Strengthen existing business unit responsibilities through active identification and promotion of personal data handling experts

Action	Grouping	Category	Detail
1	Maintain Internal Expert Details	Foundational Priorities	Identify, document and list the names of Cabinet Office staff with significant experience and knowledge of personal data handling on the intranet. Monitor for current and upcoming Internal Expert vacancies through an actionable log, prioritising long term vacancies or new business units through secondments
2	Define career path for data management professionals within Cabinet Office	Strategic Embedding	Define recognised career pathway for data management professionals. This should include mandatory experience and rotations across business units. This activity should align with current activity by cross-government DPO network to align on a consistent career pathway.

Culture

Recommendation 3: Confirm a new Data Strategy
Aim: Define a new Data Strategy aligned to Cabinet Office values and Digital Government ambitions which will inspire current and future Cabinet Office resource

Action	Grouping	Category	Detail
1	New Cabinet Office Data Strategy	Strategic Embedding	Define a new Data Vision and Strategy for Cabinet Office capturing future value of data usage, design principles and control standards to be developed. This Data Strategy should include: - Vision for expected value of Data to Cabinet Office mission and Business Units including drivers such as improved citizen outcomes

			and process efficiency - Principles for managing Data across the Cabinet Office - Measurable targets to monitor progress delivering on strategy - Capabilities and Technologies required to deliver on Data Strategy, and likely sources of skills - Technology Strategy for personal data handling including approaches to use of Google Drive, new software solutions, data minimisation, anonymisation, access and sharing protocols. This should include approaches and platforms to store sensitive data. - Approaches for managing expected increase in data volumes, both in terms of paper and digital records - Controls to be applied to all data processing activities, including personal data processes - Alignment to relevant legislation - Alignment to other relevant government initiatives including DCMS Centre for Data Ethics and Innovation Note that this Data Strategy will have likely significant dependencies on outcomes of current ICO review into Cookie usage. This activity should also be aligned to the cross Government Data Leaders Network.

Recommendation 4: Be transparent on progress
Aim - Develop the execution oversight and data analysis required to demonstrate progress on maturing data delivery capabilities to all stakeholders

Action	Grouping	Category	Detail
1	Data Culture Progress Reporting	Foundational Priorities	Develop a suite of analyses to provide indicators of achievement on improving data culture. These could include: - Implementing a quarterly review of data protection standards and action plans across all business units similar to current records management discipline - Analysis of Third Party contracts in past period to show which have been through Information Assurance processes and which have not - Resource training achievements in past period

			- Conduct regular all Cabinet Office resource personal data handling pulse surveys
2	Build Data Incident Management System	Strategic Embedding	Build a Cabinet Office data incident management system as a single repository of logged personal data handling issues.

Processes

Recommendation 5: Refresh Training and Guidance
Aim: Rebuild Training and Guidance to become accessible on a sustained basis by all Cabinet Office resource

Action	Grouping	Category	Detail
1	Revised Intranet Playbook	Strategic Embedding	Build an integrated 'how to' guide for handling personal data targeted at all levels of Cabinet Office resource. This should include: - Maintenance plan with clear responsibilities for updating, in particular, contact details of Internal Experts - Detailed workflow approaches including: 1) personal data handling guidelines for end user computing (EUC) solutions; 2) establishing new extra-HR processes including exception criteria explaining why process cannot be handled within existing HR systems, data handling purposes required, controls expected and approval paths.
2	Data Protection Chatbot	Sustained Capability	Build an automated Data Handling advice solution accessible by all Cabinet Office resource. This could be defined as a Chatbot tool able to handle common data handling issues (e.g. auto-completion of emails to all relevant stakeholders, initial risk assessment) and link to internal experts for exceptional requirements.
3	Refreshed Training Curriculum	Strategic Embedding	Create interactive, online training curriculum for all Cabinet Office resource. Materials should include mandatory and optional courses, links to related initiatives and scored assessments to support ongoing culture assessments. - Introduce training curriculum for new joiners on personal data handling topics. Should include identification of key personal data handling processes within Cabinet Office, new joiner specific responsibilities, overview of intranet resource and best practice guidelines. - Define minimum annual mandatory training

			requirements on personal data handling for all Cabinet Office resource - Business unit Data Protection induction path - Google Drive Usage Training

Recommendation 6: Establish consistent standards and technology controls
Aim: Achieve consistently leading standards and controls across personal data handling processes

Action	Grouping	Category	Detail
1	Upgrade GDPR Standards	Sustained Capability	Implement new Technology Control solutions including: - Metadata tagging for PII data - Optical Character Recognition (OCR) processing of paper records personal data tagging - GDPR workflow solution
2		Strategic Embedding	Deliver existing process improvement initiatives including: - Extension of GDS Information Assurance Processes across Cabinet Office - Integration of new IAR into GDPR processes - Data Minimisation Initiatives to reduce data volume risk
3		Foundational Priorities	Strengthen GDPR standards including: - Review template usage consistency across BUs - Participate in the current initiatives to improve consistency of ICO reporting being led by the cross-government DPO network
4	Improve Basic Hygiene	Foundational Priorities	Undertake urgent action to resolve priority issues relating to: - Shared passwords to access personal data - Personal data being stored in publicly access Google Drives - Confirm and communicate Google personal data controls currently available and to be developed
5	Introduce Data Quality Controls	Sustained Capability	Develop preventative Data Quality Controls across personal data handling life cycles which will automate sustained accuracy checks
6		Foundational Priorities	Develop detective Data Quality Controls that will indicate accuracy of personal data at point of usage

7	Introduce Data Innovation Controls	Sustained Capability	Create process to support the development of Data Ethics principles and understanding across the Cabinet Office. Examples of process components include a Data Ethics Comimittee, Data Usage Reviews, Data Discrimination Audits and Algorithimic Governance processes to identify data bias
8		Strategic Embedding	Enhance existing data innovation initiatives to further integrate personal data handling controls across the Cabinet Office. Initiatives noted by this Review that could be suitable include: - Leverage Automation activity to drive improved personal data controls through process design standards - Use current migration of HR Data from SOP to software as a service (SaaS) solution to introduce authoritative source of employees - Prove new technologies in Data Innovation Labs and test data sets to support new usage of personal data whilst necessary data security and protections assessments are conducted.
9		Foundational Priorities	Processes for managing and testing personal data in new technology solutions e.g. SaaS platforms

ANNEX

Methodology

1. This Review aims to provide an objective assessment of personal data handling within the Cabinet Office. It is not an examination of any individual personal data breach, but aims instead to identify a set of actionable recommendations to strengthen the Cabinet Office's personal data handling.

2. Individual engagement across the Cabinet Office has been high, but examples have been anonymised to ensure the highest level of transparency and honesty. The framework for determining which business units should be reviewed focused on the likely levels of risk and impact from data breaches. By focusing on the Department's most sensitive personal data and its highest priority business units, the Review combines rigour, analytic objectivity, and independence, and is focussed on making practical and pragmatic recommendations.

3. Evidence gathering and analysis comprised of a combination of qualitative and quantitative approaches, including:

   - A simple 'pulse' survey of all Cabinet Office staff to test levels of knowledge and awareness, which resulted in 485 responses from across the organisation;
   - A more detailed survey of 24 internal experts to assess more qualitative views on a range of related data topics including perceived process robustness, practices, opportunities, risks and other emerging topics of interest;
   - Follow-up interviews with approximately 23 data handling experts;
   - Conversations with other government departments to identify best practice; and
   - Interviews with over 20 business units to test the practices and processes being implemented against Cabinet Office and other guidelines.

4. The results of this evidence gathering and analysis have formed the basis of the recommendations made. These recommendations have been tested with a small group of stakeholders and shared with the Cabinet Office's Operational Committee, chaired by the Cabinet Office's Chief Operating Officer.

Glossary

Select range of relevant Acronyms, Abbreviations and Initialisms

Acronyms, Abbreviations & Initialisms	Expanded items / Full Name
CISRC	Cyber and Information Security Risk Committee
COHR	Cabinet Office Human Resources
DExEU	Department for Exiting the European Union
DHSC	Department of Health and Social Care
DWP	Department for Works and Pensions
ExCo	Executive Committee (Cabinet Office)
OpsCo	Operations Committee (Cabinet Office)
GCDIO	Government Chief Digital and Information Officer
GCS	Government Communication Service
GCSO	Government Chief Security Officer
GDS	Government Digital Service
GSG	Government Security Group
ICO	Information Commissioner's Office
IML	Information Management Leader
MCO	Minister of the Cabinet Office
NAO	National Auditor's Office
KIM	Knowledge Information Management
OVA	Office of Veteran Affairs
PACAC	Public Administration and Constitutional Affairs Committee
POG	Private Office Group
PRA	Public Records Act
SIRO	Senior Information Risk Owner

Expanded Glossary of Select Items with definitions

Acronyms, Abbreviations & Initialisms	Full Names and Descriptions
GDPR	The **General Data Protection Regulation** is a regulation on data protection and privacy. It addresses the transfer of personal data and aims primarily to give control to individuals over their personal data and to simplify the EU regulatory environment. It contains provisions and requirements related to the processing of personal data of individuals and applies to all entities.
Personal Data	Information for an identified or identifiable individual. It could be as simple as a name or a number or could include other identifiers such as an IP address or a cookie identifier etc.. If it is possible to identify an individual directly from the information being processed, then that information may also be personal data.
PII	**Personal Identity Information:** This is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for deanonymizing previously anonymous data.

DPIA	**Data Protection Impact Assessment:** A DPIA is a process designed to help analyse, identify and minimise the data protection risks of a data processing activity. DPI's help assess required compliance with data protection obligations
DPO	**Data protection officers (DPOs)** are independent data protection experts responsible for: Monitoring an organisation's data protection compliance; Informing it of and advising on its data protection obligations; Providing advice on data protection impact assessments and monitoring their performance; and Acting as a contact point for data subjects and the relevant supervisory authority Information Commissioner's Office.
ROPA	**Record of Processing Activity:** This is a record of an organization's processing activities involving personal data. Names and contact details of the data controller, data processor, data controller's representative, joint controller, and data protection officer (DPO), if applicable. Purpose (i.e., lawful basis) of processing personal data.
DPA	**Data Protection Act (UK):** The Data Protection Act 2018 was a United Kingdom Act of Parliament designed to protect personal data stored on computers or in an organised paper filing system.
Anonymization	Act of removing the association between the identifying dataset and the data subject
Special category	This is personal sensitive data requiring more protection.
Data Controller	Controllers exercise overall control over the purposes and means of personal data processing and are critical decision-makers who determine what data to process and why. They **are held accountable for processor(s) compliance**.
Data Processor	**Processors act on behalf of, and only on the instructions of, the relevant controller.** Processors do not have the same obligations as controllers under the GDPR.