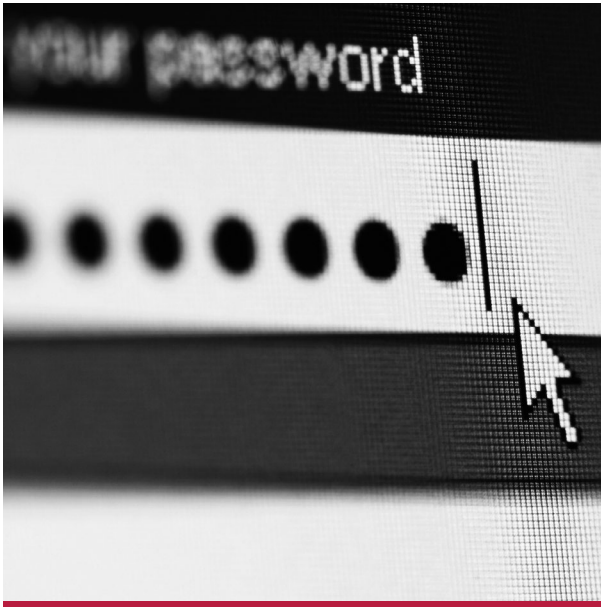
National Audit Office

Statement on the management of personal data at the National Audit Office



April 2018

www.nao.org.uk

Introduction

The Comptroller and Auditor General (C&AG) and the National Audit Office (NAO) take the protection of personal data very seriously. The NAO's Code of Conduct for staff includes a statement on how we handle personal data. All staff must reaffirm on an annual basis that they understand their responsibilities under the Code of Conduct to treat personal data appropriately and in accordance with our policies and procedures.

We have privileged and wide-ranging access to personal data and information to support our work and ensure that the C&AG's reports to Parliament are factual, accurate and complete. We have a duty to respect this privileged access and to ensure that the personal data entrusted to us is safeguarded properly.

We have robust procedures for managing personal data in accordance with the Data Protection Act 1998 and these will form the foundation of our compliance with the General Data Protection Regulation (GDPR).

GDPR provides an opportunity to review and develop our existing procedures to ensure compliance with the enhanced data protection framework and reaffirm our commitment to the proper management of personal data in line with our legal responsibilities.

We have established a dedicated project board to oversee our preparations for GDPR. The board is chaired by a member of NAO's senior management team and comprises colleagues from across the business including audit practice, digital, communications and corporate teams.

Our activities in respect of the new legislation run up to and beyond 25 May 2018 (the GDPR transition date) and include:

Management of personal data: comprehensive mapping of data-processing activities to ensure a complete view of data held and the legal basis for processing. Reviewing existing data protection and information security frameworks to ensure consistency with GDPR requirements alongside the provision of an efficient and effective public audit function.

Procedures and guidance: reviewing and, where necessary, building on our procedures and guidance for audit and corporate teams.

Contracts: reviewing and amending existing contracts with third parties to ensure clauses are consistent with the requirements of the new data protection regime.

Training: office-wide training supported by targeted workshops for all audit teams. All our staff undertake mandatory annual e-learning on data protection and we plan to refresh this to encompass GDPR requirements.

Communications and awareness: we have set up a dedicated intranet page to raise awareness of GDPR among all our staff. We are supporting this with a communication plan that includes blogs and FAQs to help staff understand GDPR and the expected impact on their work.

Statement on management of personal data

1 We take our obligations under the General Data Protection Regulations (GDPR) very seriously. We have appointed a data protection officer and all our staff are required to comply with formal data protection policies, guidelines and procedures designed to keep third-party data secure and support privacy by design.

2 We maintain a secure modern IT environment. We undertake regular independent security assessments, hold the UK government Security Essentials Plus certification, and our Information Security Management System is aligned to ISO27001. Our systems and back-ups are all hosted within the European Economic Area.

3 We keep our requests for personal data to the minimum necessary to complete our work and retain any personal information we obtain only for as long as we need it. We take appropriate measures to safeguard the confidentiality, integrity and availability of data we hold according to its volume and sensitivity as laid out in our data protection policies. Where appropriate, we conduct data protection impact assessments, which may result in additional controls being applied. We keep a record of our data-processing activities, as required under the GDPR.

4 To help you understand our commitment, we have developed a series of Personal Data Statements below, which all our staff subscribe to:

- We will only request personal data for use in discharging our statutory and other audit functions and for lawful purposes. We request the minimum amount of information necessary to carry out our work. We have protocols which specify the measures we use for protecting personal data during transfer for the purposes of our work.
- Without constraining our statutory powers, we will work with you to implement our protocols for protecting personal data during transfer for the purposes of our work.

- All personal information will be assigned an information asset owner at director level who is personally responsible for authorising requests for personal data and for ensuring that personal data is transferred, processed, stored and destroyed in accordance with our policies and procedures.
- We will destroy, return, or store personal data as necessary on completion of our work. For financial audits this will be confirmed in our audit completion report. For other non-financial work such as value-for-money studies or investigations the approach will be communicated at the end of the work. We have protocols for the long-term storage of personal data where this is required by law or by professional standards.
- If we become aware of a potential breach of the personal data you have provided to us, we will notify you without undue delay.
- We ensure our contractors operate suitable procedures for personal data protection. From time to time we contract with third parties who support us in discharging our statutory and other audit responsibilities. Access to personal information will only be given under contract to organisations which can demonstrate that they are meeting their legal obligations under GDPR and capable of maintaining the standards defined in these statements. We secure their data protection commitments through contractual obligations that meet the requirements of the GDPR.
- We audit our compliance with our data protection policies. The NAO directors responsible for the security of data self-assess at the end of each piece of work and are required to report compliance regularly. The data protection officer monitors compliance and our suite of policies and procedures that make up our data protection framework is audited by an independent third-party company.
- We will comply with the rights of data subjects in line with the requirements of data protection legislation.
- Where information identifying individuals must be given up by law, we will release it only to those legally entitled to receive it.

About us?

The National Audit Office scrutinises public spending for Parliament and is independent of government. The Comptroller and Auditor General (C&AG), Sir Amyas Morse KCB, is an Officer of the House of Commons and leads the NAO. The C&AG certifies the accounts of all government departments and many other public sector bodies. He has statutory authority to examine and report to Parliament on whether departments and the bodies they fund, nationally and locally, have used their resources efficiently, effectively, and with economy. The C&AG does this through a range of outputs including value-for-money reports on matters of public interest; investigations to establish the underlying facts in circumstances where concerns have been raised by others or observed through our wider work; landscape reviews to aid transparency; and good-practice guides. Our work ensures that those responsible for the use of public money are held to account and helps government to improve public services, leading to audited savings of £734 million in 2016.

Contacts

For further information about the National Audit Office please contact

London Office

National Audit Office,
157–197 Buckingham Palace Road,
Victoria, London SW1W 9SP
Tel +44 (0)20 7798 7000

Newcastle Office

National Audit Office,
14th Floor, St Nicholas Building,
St Nicholas Street, Newcastle upon Tyne N1 1RF
Tel +44 (0)191 269 1820

Design and Production by NAO External Relations
DP Ref: 11724-001

National Audit Office