Statement on the Management of Personal Data

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 General Data Protection Regulation and Data Protection Act 2018.

Our privacy statement, published on our website explains how the Comptroller and Auditor General and the National Audit Office use and protect personal data.

Statement on management of personal data

1. We take our obligations under the General Data Protection Regulations (GDPR) and Data Protection Act 2018 seriously. We have appointed a Data Protection Officer (DPO@nao.org.uk) and all our staff are provided with appropriate training and required to comply with formal data protection policies, guidelines and procedures designed to keep personal 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 Cyber Essentials plus certification and our Information Security Management Systems is aligned to ISO27001. Our systems and backups 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. Were appropriate, we conduct data protection impact assessments which may result in additional controls being applied. We keep a record of our data processing activities.
4. To help you understand our commitment, we have developed a series of Personal Data Statements below, which all our staff subscribe to.
    - 4.1. 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.
    - 4.2. 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.
    - 4.3. 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 the NAO's Data Protection Framework.
    - 4.4. 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 examinations 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.

4.5. If we become aware of a potential or actual breach of the personal data you have provided to us, we will notify you without undue delay.

4.6. 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 who can demonstrate that they are meeting their data protection obligations under applicable law and capable of maintaining the standards defined in these statements. We ensure their data protection commitments through contractual obligations that meet the requirements of the GDPR.

4.7. 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.

4.8. We will comply with the rights of data subjects in line with the requirements of data protection legislation.

4.9. Where information identifying individuals must be given up by law, we will release it only to those legally entitled to receive it.

October 2018