Senior Civil Service (SCS) Database

Joint data controller memorandum of understanding under Article 26 GDPR

This MOU is made between Cabinet Office and the employing departments listed at Annex B, referred to jointly in this document as the Parties. It remains valid until superseded by a revised MOU mutually endorsed by the Parties.

MOU Purpose

The purpose of this MOU is to explain the nature of personal data collected and processed as part of the Senior Civil Service Database, and the roles of the Parties, who are joint-controllers of these data.

Overview

The SCS database holds information on all Senior Civil Servants employed across government departments. The data is updated on a quarterly basis by employing departments, sourced from both information held by the department and through departments surveying the member directly. The information is collated at Cabinet Office into an amalgamated cross government database of Senior Civil Servants.

The database contains both personal information and sensitive personal information. The data are classified as Official-Sensitive. Further detail on the data collected can be found in the 'Your data' section of the Privacy Notice.

Cabinet Office and employing government department's responsibilities as joint data controllers

Under Article 26 (Joint Data Controllers) Cabinet Office and the employing departments will act as joint data controllers, in respect of any personal data pursuant to this MOU. Cabinet Office will only process personal data to the extent necessary to meet the purposes as set out in the relevant Privacy Notices issued by both Cabinet Office and employing departments. For Cabinet Office specifically these are

- to design and implement workforce strategies and the general management/employment of the Senior Civil Service and the functions and professions;
- to analyse patterns of attrition for particular posts or groups of posts within the SCS;
- for succession planning and deployment decisions;
- to monitor performance data for individuals or groups of individuals
- to identify particular skills and experience to aid in workforce planning and to facilitate the targeting of talent management or other development initiatives;
- to monitor the effectiveness and competitiveness of Civil Service reward packages by reference to individual skills, performance history, job size and associated remuneration;

- to monitor and report management and statistical information to officials across the Civil Service and for use in the public domain including diversity monitoring information;
- to report and publish management and statistical information in a non-identifiable aggregated format including diversity monitoring information;
- to monitor and understand the career paths of different groups through the Senior Civil Service.

The parties will ensure that they have appropriate technical and organisational procedures in place to protect any personal data they are processing. This includes unauthorised or unlawful processing, and protection against any accidental disclosure, loss, destruction or damage. Cabinet Office will promptly inform employing departments, and vice versa, of any unauthorised or unlawful processing, accidental disclosure, loss, destruction or damage to any such personal data. Both parties will take reasonable steps to ensure the suitability of their staff having access to such personal data.

Specific Cabinet Office responsibilities as joint data controllers:

- Carrying out any required Data Protection Impact Assessment for the Senior Civil Service database for related Cabinet Office activities.
- Commissioning the updated quarterly departmental datasets from departments.
- Maintaining and compiling the amalgamated 'SCS database' from departmental datasets.
- Following Cabinet Office Data Security Guidance to ensure that the necessary measures are taken to protect personal data.
- Ensuring approved staff are appropriately trained in how to use and look after personal data, and follow approved processes for data handling.
- Ensuring staff have appropriate security clearance to handle personal information held as part of the database.
- Ensuring an appropriate level of technical and organisational security for the personal data, including restricting access to the database to approved staff only.
- Comply with the data protection principles, and with all relevant data protection legislation.
- Maintaining a PDPR (Personal Data Processing Record) and Privacy Notice for the cross-Civil Service SCS dataset and adhering to the retention policy and processing purposes stated therein.
- Responding to data subject requests in relation to the cross-Civil Service SCS dataset, such as for access (SARs), rectification or erasure and liaising as necessary with the employing department.
- Restrict access to the personal data to only the officials detailed in the 'Recipients' section of the Privacy Notice.
- Providing a data sharing agreement for sharing the cross-Civil Service SCS dataset with any separate data controllers.
- Secure transfer of personal data both internally and externally from CO. Details can be found at Annex A.

Specific employing department's responsibilities as joint data controllers:

- Carrying out any required Data Protection Impact Assessment for the Senior Civil Service database for departmental activities.
- Updating their departmental dataset and providing the dataset to Cabinet Office on a quarterly basis.
- Following their departmental Security Guidance to ensure that the necessary measures are taken to protect personal data.
- Ensuring staff are appropriately trained in how to use and look after personal data, and follow approved processes for data handling.
- Ensuring staff have appropriate security clearance to handle personal information.
- Ensuring an appropriate level of technical and organisational security for the personal data, including restricting access to the database to approved staff only and ensuring staff follow approved processes for data handling.
- Comply with the data protection principles, and with all relevant data protection legislation.
- Ensuring that where the cross-Civil Service SCS dataset is used for their own departmental purposes that any necessary Privacy Notices are provided to data subjects.
- Responding to data subject requests in respect of departmental SCS data, such as for access (SARs), rectification or erasure and liaising as necessary with Cabinet Office.
- Secure transfer of personal data both internally and externally from thdepartment.

Individual rights

GDPR specifies new rights for individuals over the processing of their data. These rights, and the process an individual should follow when making a request, are listed in the Cabinet Office Privacy Notice and relevant employing departments Privacy Notice.

In response to any subject access request, Cabinet Office and departments will undertake a proportionate and reasonable search and respond within one month of the original request. Depending on the details of the request, either Cabinet Office or the employing department will co-ordinate the collation of data from relevant parties and ensure that the requestor receives a response.

Data breach

Cabinet Office is responsible for reporting any breach within Cabinet Office to their Data Protection Office and the ICO within 72 hours, in consultation with the employing departments Data Protection Officer.

Employing departments are responsible for reporting any data breaches within the department to their Data Protection Officer and ICO within 72 hours, in consultation with the Cabinet Office.

Publishing this MOU

Cabinet Office will take responsibility for publishing this MOU.

Annex B

List of departments

ADVISORY, CONCILIATION AND ARBITRATION SERVICE
CABINET OFFICE
CHARITY COMMISSION
COMPANIES HOUSE
COMPETITION AND MARKETS AUTHORITY
CROWN COMMERCIAL SERVICE
CROWN OFFICE AND PROCURATOR FISCAL SERVICE
CROWN PROSECUTION SERVICE
DEFENCE EQUIPMENT AND SUPPORT
DEPARTMENT FOR BUSINESS ENERGY AND INDUSTRIAL STRATEGY
DEPARTMENT FOR DIGITAL, CULTURE MEDIA AND SPORT
DEPARTMENT FOR EDUCATION
DEPARTMENT FOR ENVIRONMENT FOOD AND RURAL AFFAIRS
DEPARTMENT FOR EXITING THE EUROPEAN UNION
DEPARTMENT FOR INTERNATIONAL DEVELOPMENT
DEPARTMENT FOR INTERNATIONAL TRADE
DEPARTMENT FOR TRANSPORT
DEPARTMENT FOR WORK AND PENSIONS
DEPARTMENT OF HEALTH AND SOCIAL CARE
ESTYN
FOOD STANDARDS AGENCY
FOREIGN AND COMMONWEALTH OFFICE
GOVERNMENT ACTUARIES DEPARTMENT
GOVERNMENT INTERNAL AUDIT AGENCY
GOVERNMENT LEGAL DEPARTMENT
GOVERNMENT PROPERTY AGENCY
HEALTH AND SAFETY EXECUTIVE
HM TREASURY
HOME OFFICE
HM LAND REGISTRY
INSOLVENCY SERVICE
INTELLECTUAL PROPERTY OFFICE
MEDICINES AND HEALTHCARE PRODUCTS REGULATORY AUTHORITY
MINISTRY OF DEFENCE
MINISTRY OF HOUSING, COMMUNITIES AND LOCAL GOVERNMENT
MINISTRY OF JUSTICE
THE NATIONAL ARCHIVES
NATIONAL CRIME AGENCY
NATIONAL SAVINGS AND INVESTMENTS
NORTHERN IRELAND OFFICE
OFFICE FOR STANDARDS IN EDUCATION CHILDRENS SERVICES & SKILLS
OFFICE OF GAS AND ELECTRICITY MARKETS
OFFICE OF RAIL AND ROAD
PLANNING INSPECTORATE
PUBLIC HEALTH ENGLAND

OFFICE OF QUALIFICATIONS AND EXAMINATIONS REGULATION
QUEEN ELIZABETH II CENTRE
SCOTLAND OFFICE
SCOTTISH GOVERNMENT
SERIOUS FRAUD OFFICE
UK EXPORT FINANCE
UK STATISTICS AUTHORITY
UK SPACE AGENCY
UK SUPREME COURT
VALUATION OFFICE AGENCY
WALES OFFICE
WATER SERVICES REGULATION AUTHORITY
WELSH GOVERNMENT