SCANNING, VALIDATION AND STORAGE SERVICES

SCHEDULE 11

PROCESSING PERSONAL DATA

1. Processing Personal Data

This Schedule shall be completed by the Controller, who may take account of the view of the Processors, however the final decision as to the content of this Schedule shall be with the Authority at its absolute discretion.

1.1 The contact details of the Authority's Data Protection Officer are:

Name: [redacted]
Email: dpo@homeoffice.gov.uk

1.2 The contact details of the Supplier's Data Protection Officer are:

Data Protection Officer

Sopra Steria Limited,
Three Cherry Trees Lane,
Hemel Hempstead, HP2 7AH
Email: dpo.uk@soprasteria.com

1.3 The Processor shall comply with any further written instructions with respect to processing by the Controller.

1.4 Any such further instructions shall be incorporated into this Schedule.

Description	Details
Identity of Controller for each Category of Personal Data	**The Authority is Controller and the Supplier is Processor** • The Parties acknowledge that in accordance with Clause 23.2 to 23.15 and for the purposes of the Data Protection Legislation, the Authority is the Controller and the Supplier is the Processor of the following Personal Data.
Duration of the processing	• During the Term of this Agreement, which starts from the Effective Date and ends of the earlier of the following: (a) expiry of the Agreement; or (b) the date the Agreement is terminated.

Nature and purposes of the processing	**Passport Applications** • Processing of incoming mail, secure handling and digitisation of passport applicant's documentation, electronic transfer of digitised documentation to the Controller, cashiering and payment processing, checking and validation of documentation, physical storage and retrieval of documentation and the return of documentation to the applicant, physical transfer of documentation to and from the Controller. • Processing will be in accordance with Data Protection Legislation. • Passports are issued by Royal Prerogative and are processed under Article 6 (1) (e) of the GDPR – i.e. for the performance of a task carried out in the public interest. The Supplier must ensure that it has in place Protective Measures, which are appropriate to protect against a Data Loss Event, which the Authority may reasonably reject (but failure to reject shall not amount to approval by the Authority of the adequacy of the Protective Measures), having taken account of the: a) nature of the data to be protected; b) harm that might result from a Data Loss Event; c) state of technological development; and d) cost of implementing any measures. The Processor will organise and structure the data and make available to allow retrieval by authorised users on behalf of the Controller, who may disseminate this where there is a legal right. The Processor will compile audit information regarding the processing of the data which gives the ability to confirm user actions. This means the Processor will also hold names of employees both past and present. The Processor will not be disclosing by transmission, or otherwise disseminate, or restrict processing, unless instructed to, or agreed by the Controller, or unless legally obliged to. Erasure and destruction will follow authorised decommissioning instructions.

	Security Clearance for Personnel The Processor must take all reasonable steps to ensure the reliability and integrity of any of the Processor Personnel who have access to Personal Data.
Type of Personal Data	**Passport Applications** • Name, address, date of birth, phone number, email, parents and / or grandparents' information (where applicable), passport number, passport application counter signatory data, nationality, gender, marital status, passport application number, validity digitised image (photograph), signature; • bank/building society details; account number, sort code, Card Verification Code, expiry date, valid from; • Registration district and sub district of birth, birth certificate entry number, date and place of birth, name, surname and usual address of the birth certificate informant (if not the mother or father), date of birth certificate registration, name of birth certificate registrar; • District of marriage, place of marriage, marriage certificate entry number, date of marriage, name and surname of parties to the marriage, (age, condition, rank or profession, residence) at the time of the marriage, signatures of both parties and their witnesses of the marriage, name of the person(s) who conducted and registered the marriage, name, surname and rank or profession of each party's father; • Adoption entry number, name and surname, date of adoption order or date on which the adoption was effected, description of court by whom adoption effected, date of adoption entry, signature of officer deputed by registrar general to attest the entry; • Registration authority where the civil partnership was registered, date and place of civil partnership registration, name and surname of civil partners, date of birth, gender, condition and occupation of the civil partners, residence at the time of the civil partnership registration, father's name, surname and occupation of each civil partner, mother's name, surname and occupation of each civil partner, signatures of civil partners, name and surname of civil partnership witnesses, signature of civil partnership registrar;

	• Details contained upon Naturalisation and Registration certificates including names, date and place of birth, reference numbers, date of issuance and section for registration/naturalisation; • Details of court orders and any supporting letters/correspondence (2nd passport requests etc); and • Post Dated 2 form ("PD2") data – data contained within post-dated passport requests (future marriages). **Transfer of physical documents to the Authority** • Name, work address, work role, email address, telephone of Authority contact. **Supplier Personnel Security Clearance** • Title, Surname (current & any others), Surname at Birth, Date of Birth, National Insurance Number, Passport Number, Issuing Country, Data of Issue, Expiry Date, HO Immigration File Ref, Right to Work Expiry Date, Town of Birth, County of Birth, Country of Birth, Email Address, Current Address and Previous Address (to cover 5 years), Town, County, Country, Postcode, Start of Residence Date, Nationality information. (All nationality details including 2nd nationality if relevant) • Details for one of the following: British Passport Details, EU Passport Details or Certified passport photo and birth or adoption certificate, signature.
Categories of Data Subject	**Passport applications** • Applicants to the Controller for Passports **Transfer of physical documents to the Controller** • Authority personnel **Supplier Personnel Security Clearance** • Supplier Personnel applying for roles for employment for this Agreement

Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	**Passport Applications** • The Controller will digitally inform the Processor of any actions to be taken regarding the return of documents and the cancellation of passports (as not all submitted UK passports require cancellation). • The Processor will return documents to the address as directed by the Controller. Documents relating to 'linked' applications will be returned together to a single address unless otherwise informed by the Controller. • Digital information is stored safely and securely in conformance to industry information security management system standards (i.e. ISO27001 baseline). Digital information is purged from the Processor systems immediately after successful transmission to the Controller. **Transfer of Physical Documents to the Controller** • Once instructed by the Controller documents are specified to be dispatched safely and securely to the Controller within 24 hours. **Data and Document Retention** • The Processor shall only be required to retain any documents and data for a maximum period of 12 months at which point the Processor will inform the Authority. The Authority, on receipt of notification of documents and data approaching the 12 month retention period will provide the destruction, return or onward transfer details to the Processor. **Supplier Personnel Security Clearance** • Data is retained until clearance is granted and then destroyed, usually within 3 months but can be up to 12 months. • Physical paper forms and all supporting documents are stored securely and confidentially destroyed when clearance is granted.

	• Electronic copies of forms, emails are held until clearance is granted, then destroyed. Destruction includes the deletion of emails and files from deleted item folders and recycle bins. • Security trackers retained for 18 months and then destroyed (as per electronic data destruction above). By exception files may be kept for longer if required and retention period agreed with the security manager. Trackers held securely and password protected