

South East Strategic Partnership for Migration (SESPM)

General Data Protection Regulation

Data Protection Policy

Author: Roy Millard, South East Strategic Migration Partnership (SESPM)

Version: Version 1

Date of Version: 24th May 2018

1. Introduction and Summary

This Policy sets out how the South East Strategic Partnership for Migration (SESPM) handles data under the General Public Data Protection Regulation (GDPR).

The GDPR defines “personal data” as any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

This Policy sets out the procedures that are to be followed when dealing with personal data. The procedures and principles set out herein must be followed at all times by SESPM, its employees, agents, contractors, or other parties working on behalf of SESPM.

SESPM is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

SESPM holds and processes information that falls into the following categories:

- Names, email addresses, phone numbers and postal addresses. The vast majority of these email addresses are publicly available as a result of individuals’ roles in publicly available bodies. Where we hold and use personal email addresses we have been asked to do so by those individuals.
- Information in personnel records relating to current staff, previous staff and job applicants. The majority of this information is also held by Surrey County Council who are employment and payroll hosts for South East England Council who SESPM operate under. This information is held in line with the ‘Contract’ provisions in the GDPR to enable SESPM c/o SEEC and Surrey County Council to fulfil the terms of individuals employment contracts.
- For the legitimate purpose under ‘Public Task’ of placing people under the Home Office Refugee Vulnerable Persons Resettlement Schemes and the National Transfer Scheme for Unaccompanied Asylum Seeking Children. This task is undertaken in compliance with the Home Office Data Sharing and Data Protection Protocols set out in Schedules 5 and 6 of SESPM’s Grant Agreement for the provision of a Strategic Migration Partnership in the South East of England.

2. The Data Protection Principles

This Policy aims to ensure compliance with the Regulation. The Regulation sets out the following principles with which any party handling personal data must comply. All personal data must be:

- a) processed lawfully, fairly, and in a transparent manner in relation to the data subject;
- b) collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
- d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay;
- e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of the data subject;
- f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3. **Lawful, Fair, and Transparent Data Processing**

The Regulation seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The Regulation states that processing of personal data shall be lawful if at least one of the following applies:

- a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- b) processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;
- c) processing is necessary for compliance with a legal obligation to which the controller is subject;
- d) processing is necessary to protect the vital interests of the data subject or of another natural person;
- e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

4. **Processed for Specified, Explicit and Legitimate Purposes**

- 4.1 SESPM collects and processes the personal data set out in Part 21 of this Policy. This is for the legitimate purpose of carrying out a 'Public Task' under grant agreement with the Home Office. This may include personal data received directly

from data subjects (for example, contact details used when a data subject communicates with us) and data received from third parties (for example, data issued to us by the Home Office as part of our coordination functions under our grant agreement with them).

4.2 SESPM only processes personal data for the specific purposes set out in Part 21 of this Policy (or for other purposes expressly permitted by the Regulation). The purposes for which we process personal data will be informed to data subjects at the time that their personal data is collected, where it is collected directly from them, or as soon as possible (not more than one calendar month) after collection where it is obtained from a third party.

4.3 SESPM uses the secure MoveIT information portal operated by the Home Office which processes personal data using automated means. The processing of this data is necessary for us to fulfil our contractual obligations to the Home Office for reasons of fulfilling a Public Task. Where the MoveIT portal is not available alternative secure email arrangements will be used and measures taken to anonymise personal data. SESPM operates to the Home Office Data Sharing and Data Protection Protocols set out in Schedules 5 and 6 of SESPM's Grant Agreement for the provision of a Strategic Migration Partnership in the South East of England

5. **Adequate, Relevant and Limited Data Processing**

SESPM will only collect and process personal data for and to the extent necessary for the specific purpose(s) informed to data subjects as under Part 4, above. This is also in compliance with the Home Office Data Sharing and Data Protection Protocols set out in Schedules 5 and 6 of SESPM's Grant Agreement for the provision of a Strategic Migration Partnership in the South East of England

6. **Accuracy of Data and Keeping Data Up To Date**

SESPM shall ensure that all personal data collected and processed is kept accurate and up-to-date. The accuracy of data shall be checked when it is collected and at regular intervals thereafter. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend or erase that data, as appropriate. This is also in compliance with the Home Office Data Sharing and Data Protection Protocols set out in Schedules 5 and 6 of SESPM's Grant Agreement for the provision of a Strategic Migration Partnership in the South East of England

7. **Timely Processing**

SESPM shall not keep personal data for any longer than is necessary in light of the purposes for which that data was originally collected and processed. When the data is no longer required, all reasonable steps will be taken to erase it without delay. This is also in compliance with the Home Office Data Sharing and Data Protection Protocols set out in Schedules 5 and 6 of SESPM's Grant Agreement for the provision of a Strategic Migration Partnership in the South East of England

8. **Secure Processing**

The SESPM shall ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Further details of the data protection and organisational measures which shall be taken are provided in Parts 22 and 23 of this Policy. This is also in compliance with the Home Office Data Sharing and Data Protection Protocols set out in Schedules 5 and 6 of SESPM's Grant Agreement for the provision of a Strategic Migration Partnership in the South East of England

9. **Accountability**

- 9.1 SESPM's data protection officer is Roy Millard roymillard@secouncils.gov.uk
- 9.2 TSESPM shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:
- a) The name and details of SESPM, its data protection officer, and any applicable third-party data controllers;
 - b) The purposes for which SESPM processes personal data;
 - c) Details of the categories of personal data collected, held, and processed by SESPM; and the categories of data subject to which that personal data relates;
 - d) Details (and categories) of any third parties that will receive personal data from SESPM;
 - e) Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;
 - f) Details of how long personal data will be retained by SESPM; and
 - g) Detailed descriptions of all technical and organisational measures taken by SESPM to ensure the security of personal data.

10. **Privacy Impact Assessments/Data Protection Impact Assessments**

SESPM shall carry out Privacy Impact Assessments as and when required under the Regulation. Privacy Impact Assessments shall be overseen by the SESPM's data protection officer and shall address the following areas of importance:

- 10.1 The purpose(s) for which personal data is being processed and the processing operations to be carried out on that data;
- 10.2 Details of the legitimate interests being pursued by SESPM;
- 10.3 An assessment of the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
- 10.4 An assessment of the risks posed to individual data subjects; and
- 10.5 Details of the measures in place to minimise and handle risks including safeguards, data security, and other measures and mechanisms to ensure the protection of personal data, sufficient to demonstrate compliance with the Regulation.

11. **The Rights of Data Subjects**

The Regulation sets out the following rights applicable to data subjects:

- a) The right to be informed;
- b) The right of access;
- c) The right to rectification;
- d) The right to erasure (also referred to as the 'right to be forgotten');
- e) The right to restrict processing;
- f) The right to data portability;
- g) The right to object;
- h) Rights with respect to automated decision-making and profiling.

12. Keeping Data Subjects Informed

12.1 SESPM shall ensure that the following information is provided to every data subject when personal data is collected:

- a) Details of SESPM including, but not limited to, the identity of Roy Millard , its Data Protection Officer;
- b) The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 21 of this Policy) and the legal basis justifying that collection and processing;
- c) Where applicable, the legitimate interests upon which SESPM is justifying its collection and processing of the personal data;
- d) Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;
- e) Where the personal data is to be transferred to one or more third parties, details of those parties;
- f) Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the “EEA”), details of that transfer, including but not limited to the safeguards in place (see Part 24 of this Policy for further details concerning such third country data transfers);
- g) Details of the length of time the personal data will be held by SESPM (or, where there is no predetermined period, details of how that length of time will be determined) This is also in compliance with the Home Office Data Sharing and Data Protection Protocols set out in Schedules 5 and 6 of SESPM’s Grant Agreement for the provision of a Strategic Migration Partnership in the South East of England
- h) Details of the data subject’s rights under the Regulation;
- i) Details of the data subject’s right to withdraw their consent to SESPM’s processing of their personal data at any time;
- j) Details of the data subject’s right to complain to the Information Commissioner’s Office (the ‘supervisory authority’ under the Regulation);
- k) Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it;
- l) Details of any automated decision-making that will take place using the personal data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any consequences.

12.2 The information set out above in Part 12.1 shall be provided to the data subject at the following applicable time:

12.2.1 Where the personal data is obtained from the data subject directly, at the time of collection;

12.2.2 Where the personal data is not obtained from the data subject directly (i.e. from another party):

- a) If the personal data is used to communicate with the data subject, at the time of the first communication; or
- b) If the personal data is to be disclosed to another party, before the personal data is disclosed; or
- c) In any event, not more than one month after the time at which SESPM obtains the personal data.

13. **Data Subject Access**

- 13.1 A data subject may make a subject access request (“SAR”) at any time to find out more about the personal data which SESPM holds about them. The SESPM is normally required to respond to SARs within one month of receipt (this can be extended by up to two months in the case of complex and/or numerous requests, and in such cases the data subject shall be informed of the need for the extension).
- 13.2 All subject access requests received must be forwarded to Roy Millard roymillard@secouncils.gov.uk , SESPM’s data protection officer. .
- 13.3 SESPM does not charge a fee for the handling of normal SARs. SESPM reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

14. **Rectification of Personal Data**

- 14.1 If a data subject informs SESPM that personal data held by the SESPM is inaccurate or incomplete, requesting that it be rectified, the personal data in question shall be rectified, and the data subject informed of that rectification, within one month of receipt the data subject’s notice (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).
- 14.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification of that personal data.

15. **Erasure of Personal Data**

- 15.1 Data subjects may request that SESPM erases the personal data it holds about them in the following circumstances:
- a) It is no longer necessary for SESPM to hold that personal data with respect to the purpose for which it was originally collected or processed;
 - b) The data subject wishes to withdraw their consent to SESPM holding and processing their personal data;
 - c) The data subject objects to SESPM holding and processing their personal data (and there is no overriding legitimate interest to allow SESPM to continue doing so) (see Part 18 of this Policy for further details concerning data subjects’ rights to object);
 - d) The personal data has been processed unlawfully;
 - e) The personal data needs to be erased in order for SESPM to comply with a particular legal obligation
- 15.2 Unless SESPM has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject’s request (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).
- 15.3 In the event that any personal data that is to be erased in response to a data subject request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

16. **Restriction of Personal Data Processing**

- 16.1 Data subjects may request that SESPM ceases processing the personal data it holds about them. If a data subject makes such a request, the SESPM shall retain only the amount of personal data pertaining to that data subject that is necessary to ensure that no further processing of their personal data takes place.
- 16.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

17. **Data Portability**

- 17.1 SESPM does not undertake automated processing with any data we have collected ourselves. However, we do use the secure MoveIT information portal operated by the Home Office which processes personal data using automated means. The processing of this data is necessary for us to fulfil our contractual obligations to the Home Office for reasons of fulfilling a Public Task. Where the MoveIT portal is not available alternative secure email arrangements will be used and measures taken to anonymise personal data. SESPM operates to the Home Office Data Sharing and Data Protection Protocols set out in Schedules 5 and 6 of SESPM's Grant Agreement for the provision of a Strategic Migration Partnership in the South East of England.
- 17.2 Where data subjects have given their consent to SESPM to process their personal data in such a manner or the processing is otherwise required for the performance of a contract between SESPM and the data subject, data subjects have the legal right under the Regulation to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers, e.g. other organisations).
- 17.3 To facilitate the right of data portability, SESPM shall make available all applicable personal data to data subjects in the following format[s]:
 - a) Excel format or Word format for names, email and postal address held.
 - b) Word and PDF files for staff information.
- 17.4 Where technically feasible, if requested by a data subject, personal data shall be sent directly to another data controller.
- 17.5 All requests for copies of personal data shall be complied with within one month of the data subject's request (this can be extended by up to two months in the case of complex requests in the case of complex or numerous requests, and in such cases the data subject shall be informed of the need for the extension).

18. **Objections to Personal Data Processing**

- 18.1 Data subjects have the right to object to SESPM processing their personal data based on legitimate interests (including profiling), direct marketing (including profiling).
- 18.2 Where a data subject objects to SESPM processing their personal data based on its legitimate interests, SESPM shall cease such processing forthwith, unless it can be demonstrated that the SESPM's legitimate grounds for such processing override the data subject's interests, rights and freedoms; or the processing is necessary for the conduct of legal claims.
- 18.3 Where a data subject objects to SESPM processing their personal data for direct marketing purposes, SESPM shall cease such processing forthwith.
- 18.4 Where a data subject objects to SESPM processing their personal data for

scientific and/or historical research and statistics purposes, the data subject must, under the Regulation, 'demonstrate grounds relating to his or her particular situation'. SESPM is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

19. **Automated Decision-Making**

19.1 SESPM does not use personal data for any form of automated decision making.

20. **Profiling**

Where SESPM uses personal data for profiling purposes, the following shall apply:

- a) Clear information explaining the profiling will be provided, including its significance and the likely consequences;
- b) Appropriate mathematical or statistical procedures will be used;
- c) Technical and organisational measures necessary to minimise the risk of errors and to enable such errors to be easily corrected shall be implemented; and
- d) All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling (see Parts 22 and 23 of this Policy for more details on data security).

21. **Personal Data**

The following personal data may be collected, held, and processed by SESPM:

- a) Names, email addresses and postal addresses. The vast majority of these email addresses are publicly available as a result of individuals' roles in publicly available bodies. Where we hold and use personal email addresses we have been asked to do so by those individuals.
- b) Information in personnel records relating to current staff, previous staff and job applicants. The majority of this information is also held by Surrey County Council who are employment and payroll hosts for South East England Council who SESPM operate under. This information is held in line with the 'Contract' provisions in the GDPR to enable SESPM c/o SEEC and Surrey County Council to fulfil the terms of individuals employment contracts.
- c) For the legitimate purpose under 'Public Task' of placing people under the Home Office Refugee Vulnerable Persons Resettlement Schemes and the National Transfer Scheme for Unaccompanied Asylum Seeking Children. This task is undertaken in compliance with the Home Office Data Sharing and Data Protection Protocols set out in Schedules 5 and of SESPM's Grant Agreement for the provision of a Strategic Migration Partnership in the South East of England.

22. **Data Protection Measures**

SESPM shall ensure that all its employees, agents, contractors, or other parties working on its behalf comply with the following when working with personal data:

- a) All emails containing personal data must be encrypted using TLS encryption
- b) Where any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. Hardcopies should be shredded, and electronic copies should be deleted securely using the permanently delete function. When decommissioned from service devices such as laptops and telephones will be have digital data removed by an appropriate professional

organisation who must issue a certificate to confirm this action has been undertaken on each device.

- c) Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;
- d) Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;
- e) Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted;
- f) Where Personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;
- g) Where Personal data is to be transferred in hard copy form it should be passed directly to the recipient or sent using recorded delivery;
- h) No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of SESPM requires access to any personal data that they do not already have access to, such access should be formally requested from Roy Millard roymillard@secouncils.gov.uk or Heather Bolton heatherbolton@secouncils.gov.uk or Sarah Spain sarahspain@secouncils.gov.uk or Susan Fawcus sespm@secouncils.gov.uk or Rachael Coker smpsupport@secouncils.gov.uk
- i) All hard copies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar;
- j) No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of SESPM or not, without the authorisation of Roy Millard roymillard@secouncils.gov.uk
- k) Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors or other parties at any time;
- l) If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it;
- m) No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to SESPM or not.
- n) No personal data should be transferred to any non-work-related device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of SESPM where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the GDPR (which may include demonstrating to SESPM that all suitable technical and organisational measures have been taken);
- o) All personal data stored electronically should be backed up daily with backups stored offsite by SESPM c/o SEEC's IT contractors BTP. All backups should be encrypted using RC5 encryption
- p) All electronic copies of personal data should be stored securely using passwords and Kerberos AES or NTLM encryption data encryption
- q) All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and

lowercase letters, numbers, and symbols. All software used by SESPM is designed to require such passwords;

- r) Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of SESPM, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;

23. **Organisational Measures**

SESPM shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

- a) All employees, agents, contractors, or other parties working on behalf of SESPM shall be made fully aware of both their individual responsibilities and SESPM's responsibilities under the GDPR and under this Policy, and shall be provided with a copy of this Policy;
- b) Only employees, agents, sub-contractors, or other parties working on behalf of SESPM that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by SESPM;
- c) All employees, agents, contractors, or other parties working on behalf of SESPM handling personal data will be appropriately trained to do so;
- d) All employees, agents, contractors, or other parties working on behalf of SESPM handling personal data will be appropriately supervised;
- e) Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed;
- f) The performance of those employees, agents, contractors, or other parties working on behalf of SESPM handling personal data shall be regularly evaluated and reviewed;
- g) All employees, agents, contractors, or other parties working on behalf of SESPM handling personal data will be bound to do so in accordance with the principles of the GDPR and this Policy by contract;
- h) All agents, contractors, or other parties working on behalf of SESPM handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the SESPM arising out of this Policy and the GDPR;
- i) Where any agent, contractor or other party working on behalf of SESPM handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless SESPM against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

24. **Transferring Personal Data to a Country Outside the EEA**

24.1 SESPM does not transfer personal data to countries outside of the EEA.

25. **Data Breach Notification**

25.1 All personal data breaches must be reported immediately to SESPM's data protection officer.

25.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the data protection officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

25.3 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 25.2) to the rights and freedoms of data subjects, the data protection officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

25.4 Data breach notifications shall include the following information:

- a) The categories and approximate number of data subjects concerned;
- b) The categories and approximate number of personal data records concerned;
- c) The name and contact details of SESPM's data protection officer (or other contact point where more information can be obtained);
- d) The likely consequences of the breach;
- e) Details of the measures taken, or proposed to be taken, by SESPM to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

26. **Implementation of Policy**

This Policy shall be deemed effective as of 24th May 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

Name: Roy Millard
Position: Head of Partnership
Date: 24th May 2018
Due for Review by: 24th May 2019

Signature:

