South East England Councils (SEEC)
GDPR & Privacy Policy

1. Introduction and Summary

This policy sets out how South East England Councils (SEEC) handles personal data under the General Data Protection Regulation (GDPR).

GDPR defines 'personal data' as any information relating to an identified or identifiable person – for example their name, identification number, location data, physical, physiological, genetic, mental, economic, cultural, or social identity.

The procedures and principles below will be followed by SEEC, its employees, agents, contractors or other parties working on our behalf.

SEEC 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 we deal.

The vast majority of SEEC's data records comprise names, email addresses and postal addresses only and these are used to send meeting invitations, briefings and updates to elected politicians and officers across the South East. Under GDPR we will continue to do this in line with the 'legitimate interests' provisions in GDPR guidance. This reflects one of the following situations:

- Your organisation has an interest in SEEC work, demonstrated by paying SEEC's membership subscription.
- You are in a publicly-accountable role that influences policy-making affecting SEEC members and South East residents.
- You have actively registered on our database to receive SEEC updates.
- You are in an organisation entitled to free places at occasional events organised by SEEC and partners that are open to those outside the current SEEC membership.

SEEC holds information that falls into two categories:

a) Names, email addresses, postal addresses and, in some instances, personal phone numbers. The vast majority of this information is publicly available as a result of individuals' roles in publicly accountable bodies. Where we hold and use personal email addresses, we have been asked to do so by individuals who register to receive information to that address.

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 SEEC employees. This information is held in line with the 'contract' provisions in GDPR to enable SEEC and Surrey CC to fulfil the terms of individuals' employment contracts.

Information kept by SEEC is stored on SEEC's internal IT systems, which are UK-based and password protected with 2-level security (3 level security for HR information). Some personnel information, such as application forms, is also kept in hard copy format in a secure cabinet. Copies of personnel information will also be held by Surrey CC as the host organisation for SEEC.

SEEC does not rent or sell contact details or personal information in any way. Individuals can opt out of SEEC's regular emails by using the unsubscribe link.

2. Data Protection Principles

This policy aims to ensure compliance with GDPR to ensure all personal data is:

a) Processed lawfully, fairly, and in a transparent manner.

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 incompatible with the initial purpose.

c) Relevant and limited to what is necessary.

d) Accurate and up to date. Every reasonable step is taken to ensure that inaccurate personal data is deleted or corrected without delay.

e) Kept in a form which permits identification of individuals for no longer than is necessary. Personal data may be stored for longer periods if it is processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. This will be subject to appropriate measures required by GDPR to safeguard the rights and freedoms of the person involved.

f) Processed in a way that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

3. Lawful, Fair, and Transparent Data Processing

GDPR aims to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the person involved. GDPR provides that processing of personal data is lawful if at least one of the following applies:

a) Consent – a person has given consent to the processing of their personal data for one or more purposes.

b) Contract – processing is necessary to fulfil or enter a contract with an individual.

c) Legal Obligation – processing is necessary to comply with a legal obligation.

d) Vital Interests – processing is necessary to protect someone's life.

e) Public Task – processing is necessary to fulfil a task carried out in the public interest or an official function that has a clear basis in law.

f) Legitimate Interests – processing is necessary for your legitimate interests or those of a third party.

4. Processed for Specified, Explicit and Legitimate Purposes

4.1 SEEC collects and processes the personal data set out in para 21. This may include personal data received directly from individuals (for example, members' contact details or employment records kept as part of staffing information) and data from third parties (for example, contact details for lead representatives received from a local authority).

4.2 SEEC only processes personal data for the specific purposes set out in para 21 or for other purposes expressly permitted by GDPR.

5. Adequate, Relevant and Limited Data Processing

SEEC will only collect and process personal data to the extent necessary for the specific purposes set out in para 21.

6. Accuracy and Keeping Data Up To Date

SEEC will ensure that all personal data collected and processed is kept accurate and up-to-date. The accuracy of data will be checked when it is collected and then at regular intervals. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend or delete that data.

7. Timely Processing

SEEC will not keep personal data for any longer than is necessary in light of the purposes for which the data was collected and processed. When the data is no longer required, all reasonable steps will be taken to delete it without delay.

8. Secure Processing

SEEC will 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 these measures are in para 22 and 23.

9. **Accountability**

9.1 SEEC's data protection officer is Heather Bolton heatherbolton@secouncils.gov.uk

9.2 SEEC will keep written internal records of all personal data collection, holding and processing, to incorporate the following:

a) How to contact SEEC, its data protection officer and any applicable third-party data controllers;
b) The purposes for which SEEC processes personal data;
c) Details of the categories of personal data collected, held, and processed by SEEC and the categories of individual to which that personal data relates;
d) Details (and categories) of any third parties that will receive personal data from SEEC;
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 SEEC;
g) Detailed descriptions of all technical and organisational measures taken by SEEC to ensure the security of personal data.

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

SEEC will carry out a Privacy Impact Assessment as required under GDPR to outline:

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 SEEC;

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 individuals; 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 GDPR.

11. **Individuals' Rights**

GDPR sets out the following rights applicable to individuals:

a) The right to be informed;
b) The right of access;
c) The right to rectification;
d) The right to erasure;
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 Individuals Informed**

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

a) Details of SEEC, including the identity of its Data Protection Officer;
b) The purpose(s) for which the personal data is being collected and will be processed (as detailed in para 21) and the legal basis justifying that collection and processing;
c) Where applicable, the legitimate interests which underpin SEEC's 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 the European Economic Area (EEA), details of that transfer, including but not limited to the safeguards in place (see also para 24);

g) Details of the length of time the personal data will be held by SEEC (or where there is no predetermined period, details of how that length of time will be determined);

h) Details of the individual's rights under GDPR;

i) Details of the individual's right to withdraw their consent to SEEC processing their personal data at any time;

j) Details of the individual's right to complain to the Information Commissioner's Office (the 'supervisory authority' under GDPR);

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 para 12.1 shall be provided to individuals:

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

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

a) If the personal data is used to communicate with the individual 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 SEEC obtains the personal data.

13. Individuals' Access

13.1 An individual may make a subject access request (SAR) at any time to find out more about the personal data which SEEC holds about them. SEEC 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 individual shall be informed of the need for the extension).

13.2 All SARs received should be forwarded to Hayley Austin at SEEC via admin@secouncils.gov.uk

13.3 SEEC does not charge a fee for handling normal SARs. SEEC reserves the right to charge reasonable fees for additional copies of information that has already been supplied to an individual and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

14. Rectification of Personal Data

14.1 If an individual informs SEEC that personal data held by SEEC is inaccurate or incomplete, requesting that it be rectified, the personal data in question shall be rectified, and the individual informed within one month (this can be extended by up to two months in the case of complex requests, and in such cases the individual 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 Individuals may request that SEEC erases the personal data it holds about them in the following circumstances:

a) It is no longer necessary for SEEC to hold that personal data with respect to the purpose for which it was originally collected or processed;

b) The individual wishes to withdraw their consent to SEEC holding and processing their personal data;

c) The individual objects to SEEC holding and processing their personal data (and there is no overriding legitimate interest to allow SEEC to continue doing so) (see also para 18);

d) The personal data has been processed unlawfully;

e) The personal data needs to be erased in order for SEEC to comply with a particular legal obligation.

15.2 Unless SEEC has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the individual informed within one month of receipt of the request (this can be extended by up to two months in the case of complex requests, and in such cases the individual 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 an individual's 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 Individuals may request that SEEC ceases processing the personal data it holds about them. Following such a request, SEEC shall retain only the amount of personal data pertaining to that individual 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 SEEC processes and stores personal data using its internal IT systems.

17.2 Where individuals have given their consent to SEEC to process their personal data in such a manner or the processing is otherwise required for the performance of a contract between SEEC and the individual, individuals have the legal right under GDPR to receive a copy of their personal data and to use it for other purposes (eg transmitting it to other organisations).

17.3 To facilitate the right of data portability, SEEC shall make available all applicable personal data to individuals in the following formats:

a) Excel format or Word format for names, email, postal address and any phone numbers held

b) Word and pdf files for staff information.

17.4 Where technically feasible, if requested by an individual, 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 individual'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 individual shall be informed of the need for the extension).

18. Objections to Personal Data Processing

18.1 Individuals have the right to object to SEEC processing their personal data based on legitimate interests (including profiling), direct marketing (including profiling).

18.2 Where an individual objects to SEEC processing their personal data based on its legitimate interests, SEEC shall cease such processing forthwith, unless it can be

demonstrated that SEEC's legitimate grounds for such processing override the individual's interests, rights and freedoms; or the processing is necessary for the conduct of legal claims.

18.3 Where an individual objects to SEEC processing their personal data for direct marketing purposes, SEEC shall cease such processing forthwith.

18.4 Where an individual objects to SEEC processing their personal data for scientific and/or historical research and statistics purposes, the individual must, under GDPR 'demonstrate grounds relating to his or her particular situation'. SEEC 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 SEEC does not use personal data for any form of automated decision making.

20. Profiling

20.1 SEEC does not use personal data for profiling.

21. Personal Data

The following personal data is collected, held, and processed by the Company:

a) Names, email addresses, postal addresses and, in some instances, personal phone numbers. The vast majority of this information is publicly available as a result of individuals' roles in publicly accountable bodies. Where we hold and use personal email addresses, we have been asked to do so by individuals who register to receive information to that address.

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 SEEC employees. This information is held in line with the 'contract' provisions in GDPR to enable SEEC and Surrey CC to fulfil the terms of individuals' employment contracts.

22. Data Protection Measures

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

a) Avoiding duplication or emailing of personal data. Files containing personal information are stored in secure, password-protected IT systems with either 2 or 3-level password protection.

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 will be deleted and hardcopies shredded. When decommissioned from service, devices such as laptops and telephones will be have digital data removed by an appropriate professional organisation.

c) Any personal data sent to SEEC in the body of an email should be copied from that email and stored securely. The original email should be deleted from inboxes.

d) Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent personally addressed and labelled confidential by courier/ Royal Mail. SEEC may also use Surrey CC's internal postal system for HR materials.

e) No personal data may be shared informally. If an employee, agent, sub-contractor, or other party working on behalf of SEEC requires any personal data that they do not already have access to, this should be formally requested from Hayley Austin admin@secouncils.gov.uk or Heather Bolton heatherbolton@secouncils.gov.uk

f) All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked drawer, cabinet or similar;

g) No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of SEEC without authorisation of Hayley Austin admin@secouncils.gov.uk or Heather Bolton heatherbolton@secouncils.gov.uk

h) 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;

i) If personal data is being viewed on a computer screen and the computer is to be left unattended for any period of time, the user must lock the computer screen before leaving it;

j) No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to SEEC or not.

k) 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 SEEC where the party in question has agreed to comply fully with this policy (which may include demonstrating to SEEC that all suitable technical and organisational measures have been taken);

l) All personal data stored electronically will be backed up daily with backups stored offsite by SEEC's IT contractors BTP.

m) All electronic copies of personal data should be stored securely on systems using at least 2-level password security, with HR information subject to an additional level of security by being stored in areas of SEEC's IT system where access is limited to authorised staff.

n) All passwords used to protect personal data should not use words or phrases that can be easily guessed or otherwise compromised.

23. **Organisational Measures**

SEEC will ensure 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 SEEC shall be made fully aware of both their individual responsibilities and SEEC's responsibilities under GDPR and this policy;

b) Only employees, agents, sub-contractors, or other parties working on behalf of SEEC that need access to, and use of, personal data to carry out their assigned duties correctly will have access to personal data held by SEEC;

c) All employees, agents, contractors, or other parties working on behalf of SEEC and handling personal data will be trained;

d) All employees, agents, contractors, or other parties working on behalf of SEEC will be supervised;

e) Methods of collecting, holding and processing personal data will be regularly evaluated and reviewed;

f) The performance of those employees, agents, contractors, or other parties working on behalf of SEEC and handling personal data shall be regularly evaluated and reviewed;

g) All employees, agents, contractors, or other parties working on behalf of SEEC will be bound to do so in accordance with the principles of GDPR by contract;

h) All agents, contractors, or other parties working on behalf of SEEC 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 SEEC employees;

i) Where any agent, contractor or other party working on behalf of SEEC handling personal data fails in their obligations under this policy that party shall indemnify and hold harmless SEEC 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 SEEC 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 SEEC'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 individuals (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 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 para 25.2) to the rights and freedoms of individuals, the data protection officer must ensure that all affected individuals 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 individuals concerned;
b) The categories and approximate number of personal data records concerned;
c) The name and contact details of SEEC's 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 SEEC to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

26. **Implementation of Policy**

16.1 This policy will be effective as of 25 May 2018. It does not have retroactive effect and will apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

Name: Heather Bolton

Position: Director, SEEC

Date: 22 May 2018

Due for Review by: 24 May 2019

Signature: