Data Protection & Information Governance

General Data Protection Regulation (GDPR) and Data Protection Policy
For
Abhimantrit GuruPrasadam Ayurveda Herbal Foods Pvt. Ltd. Indra Puri, Loni Road, Ghaziabad – 201102 India.

Document Type: Policy

Version No: 1.0

Guru Prasadam

Issue Date: 27 Mar 2019

Purpose of this document :
To provide illustrative GDPR Information Security Policy

VERSION HISTORY

Version	Date Issued	Brief Summary of Change	Owner's Name
V1.0		New Policy	Tarinderjeet Singh

Document Prepared By:	Amit Jaiswal
Date of Issue	2nd April 2019
Reference	EU General Data Protection Regulation (GDPR) and Data Protection Act 2018
Copyright Status	

Policy title:	General Data Protection Regulation (GDPR) and Data Protection Policy

Issue date:	2nd April 2019	**Review date:**	2nd April 2020

Version:	1.0	**Issued by:**	

Aim:	**To achieve GDPR compliance**

Scope:	**Website Domain/Mobile**

Associated documentation:	**Legal Framework:** The Data Protection Act (1998), Copyright Designs & Patents Act (1988), Computer Misuse Act (1990), Health & Safety at Work Act (1974), Human Rights Act (1998) etc. **Policies:** Staff NDA, email, Internet & Media
Appendices:	
Approved by:	Sant Shri Trilochan Das Ji Sachkhand Nanak Dham
Date:	2nd Apr, 2019

Review and consultation process:	Annually from review date provided above. Trust Information Governance Board to oversee process
Responsibility for Implementation & Training:	Data Protection Officer (DPO)

HISTORY

Revisions:	New Policy	
Date:	**Author:**	**Description:**

Distribution methods:	Email, intranet address, paper distribution to all departmental secretaries, paper circulation by all department heads to their staff.

1 Introduction

This Policy sets out the obligations of company "Abhimantrit GuruPrasadam Ayurveda Herbal Foods Pvt. Ltd.", whose registered office is at " Indra puri, Loni Road, Ghaziabad – 201102 India." ("the Company") regarding data protection and the rights of customers, suppliers and employees, ("data subjects") in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation ("GDPR"), current UK data protection legislation and applicable amendments.

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 the Company's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

The Company 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.

2 The Data Protection Principles

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

2.1 Processed lawfully, fairly, and in a transparent manner in relation to the data subject.

2.2 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.

2.3 Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

2.4 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 it is processed, is erased, or rectified without delay.

2.5 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 GDPR in order to safeguard the rights and freedoms of the data subject.

2.6 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 The Rights of Data Subjects

The GDPR sets out the following rights applicable to data subjects (please refer to the parts of this policy indicated for further details):

3.1 The right to be informed (Part 12).
3.2 The right of access (Part 13);
3.3 The right to rectification (Part 14);
3.4 The right to erasure (also known as the 'right to be forgotten') (Part 15);
3.5 The right to restrict processing (Part 16);
3.6 The right to data portability (Part 17);
3.7 The right to object (Part 18); and
3.8 Rights with respect to automated decision-making and profiling (Part 19).

4 Lawful, Fair, and Transparent Data Processing

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

4.1.1 The data subject has given consent to the processing of their personal data for one or more specific purposes;

4.1.2 The 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 with them;

4.1.3 The processing is necessary for compliance with a legal obligation to which the data controller is subject;

4.1.4 The processing is necessary to protect the vital interests of the data subject or of another natural person;

4.1.5 The 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 data controller; or

4.1.6 The processing is necessary for the purposes of the legitimate interests pursued by the data 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.

4.2 If the personal data in question is "special category data" (also known as "sensitive personal data") (for example, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation), at least one of the following conditions must be met:

4.2.1 The data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless EU or EU Member State law prohibits them from doing so);

4.2.2 The processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by EU or EU Member State law or a collective agreement pursuant to EU Member State law which provides for appropriate safeguards for the fundamental rights and interests of the data subjects;

4.2.3 The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

4.2.4 The data controller is a foundation, association, or other non-profit body with

a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects;

4.2.5 The processing relates to personal data which is clearly made public by the data subject;

4.2.6 The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;

4.2.7 The processing is necessary for substantial public interest reasons, on the basis of EU or EU Member State law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;

4.2.8 The processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of EU or EU Member State law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the GDPR;

4.2.9 The processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of EU or EU Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or

4.2.10 The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the GDPR based on EU or EU Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

5 Specified, Explicit, and Legitimate Purposes

5.1 The Company collects and processes the personal data set out in Part 21 of this Policy. This includes:

5.1.1 Personal data collected directly from data subjects.

5.2 Data subjects are kept informed at all times of the purpose or purposes for which the Company uses their personal data. Please refer to Part 12 for more information on keeping data subjects informed.

6 Adequate, Relevant, and Limited Data Processing

6.1 The Company will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Part 5, above, and as set out in this Policy.

7 Accuracy of Data and Keeping Data Up-to-Date

7.1 The Company shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Part 14, below.

7.2 The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

8 Data Retention

8.1 The Company shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.

8.2 When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

8.3 For full details of the Company's approach to data retention, including retention periods for specific personal data types held by the Company, please refer to our Data Retention Policy.

9 Secure Processing

9.1 The Company shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided in Parts 20 to 25 of this Policy.

10 Accountability and Record-Keeping

10.1 The Company employs the services of a Data Protection Officer

10.2 The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Company's other data protection-related policies, and with the GDPR and other applicable data protection legislation.

10.3 The Company shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

- **10.3.1** The name and details of the Company, its Data Protection Officer, and any applicable third-party data processors;
- **10.3.2** The purposes for which the Company collects, holds, and processes personal data;
- **10.3.3** Details of the categories of personal data collected, held, and processed by the Company, and the categories of data subject to which that personal data relates;
- **10.3.4** Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;
- **10.3.5** Details of how long personal data will be retained by the Company (please refer to the Company's Data Retention Policy); and
- **10.3.6** Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

11 Data Protection Impact Assessments

11.1 The Company shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data [which involve the use of new technologies and the processing involved is likely to result in a high risk to the rights and freedoms of data subjects under the GDPR].

11.2 Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:

11.2.1 The type(s) of personal data that will be collected, held, and processed;

11.2.2 The purpose(s) for which personal data is to be used;

11.2.3 The Company's objectives;

11.2.4 How personal data is to be used;

11.2.5 The parties (internal and/or external) who are to be consulted;

11.2.6 The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;

11.2.7 Risks posed to data subjects;

11.2.8 Risks posed both within and to the Company; and

11.2.9 Proposed measures to minimise and handle identified risks.

12 Keeping Data Subjects Informed

12.1 The Company shall provide the information set out in Part 12.2 to every data subject:

12.1.1 Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and

12.1.2 Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:

a) if the personal data is used to communicate with the data subject, when the first communication is made; or

b) if the personal data is to be transferred to another party, before that transfer is made; or

c) as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

12.2 The following information shall be provided:

12.2.1 Details of the Company including, but not limited to, the identity of its Data Protection Officer;

12.2.2 The purpose(s) for which the personal data is being collected and will be processed and the legal basis justifying that collection and processing;

12.2.3 Where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data;

12.2.4 Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;

12.2.5 Where the personal data is to be transferred to one or more third parties, details of those parties;

12.2.6 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 28 of this Policy for further details);

12.2.7 Details of data retention;

12.2.8 Details of the data subject's rights under the GDPR;

12.2.9 Details of the data subject's right to withdraw their consent to the Company's processing of their personal data at any time;

12.2.10 Details of the data subject's right to complain to the Information

Commissioner's Office (the "supervisory authority" under the GDPR);

12.2.11 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; and

12.2.12 Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

13 Data Subject Access

13.1 Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which the Company holds about them, what it is doing with that personal data, and why.

13.2 Employees wishing to make a SAR should do using a Subject Access Request Form, sending the form to the Company's Data Protection Officer via email to dpo@siv.org.uk

13.3 Responses to SARs shall normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

13.4 All SARs received shall be handled by the Company's Data Protection Officer.

13.5 The Company does not charge a fee for the handling of normal SARs. The Company 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 Data subjects have the right to require the Company to rectify any of their personal data that is inaccurate or incomplete.

14.2 The Company shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Company of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

14.3 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

15 Erasure of Personal Data

15.1 Data subjects have the right to request that the Company erases the personal data it holds about them in the following circumstances:

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

15.1.2 The data subject wishes to withdraw their consent to the Company holding and processing their personal data;

15.1.3 The data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so) (see Part 18 of this Policy for further details concerning the right to object);

15.1.4 The personal data has been processed unlawfully;

15.1.5 The personal data needs to be erased in order for the Company to comply with a particular legal obligation;

15.1.6 The personal data is being held and processed for the purpose of providing information society services to a child.

15.2 Unless the Company 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. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

15.3 In the event that any personal data that is to be erased in response to a data subject'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 Data subjects may request that the Company ceases processing the personal data it holds about them. If a data subject makes such a request, the Company shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

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 The Company processes personal data using automated means in order to be as efficient as possible in delivering our services to you.

17.2 Where data subjects have given their consent to the Company to process their personal data in such a manner, or the processing is otherwise required for the performance of a contract between the Company and the data subject, data subjects have the right, under the GDPR, to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers).

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

17.3.1 CSV;

17.3.2 PDF;

17.4 Where technically feasible, if requested by a data subject, personal data shall be sent directly to the required data controller.

17.5 All requests for copies of personal data shall be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed.

18 Objections to Personal Data Processing

18.1 Data subjects have the right to object to the Company processing their personal data based on legitimate interests, direct marketing (including profiling), [and processing for scientific and/or historical research and statistics purposes].

18.2 Where a data subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing immediately, unless it can be demonstrated that the Company's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

18.3 Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing immediately.

18.4 [Where a data subject objects to the Company processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under

the GDPR, "demonstrate grounds relating to his or her particular situation". The Company is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.]

19 Profiling

19.1 The Company uses personal data for profiling purposes.

19.2 When personal data is used for profiling purposes, the following shall apply:

19.2.1 Clear information explaining the profiling shall be provided to data subjects, including the significance and likely consequences of the profiling;

19.2.2 Appropriate mathematical or statistical procedures shall be used;

19.2.3 Technical and organisational measures shall be implemented to minimise the risk of errors. If errors occur, such measures must enable them to be easily corrected; and

19.2.4 All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling (see Parts 20 to 25 of this Policy for more details on data security).

20 Data Security - Transferring Personal Data and Communications

The Company shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

20.1.1 All emails containing personal data must be encrypted using a password protected zip file.

20.1.2 All emails containing personal data must be marked "confidential";

20.1.3 Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;

20.1.4 Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;

20.1.5 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;

20.1.6 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;

20.1.7 Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient via Royal Mail recorded or special delivery; and

20.1.8 All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked "confidential".

21 Data Security - Storage

The Company shall ensure that the following measures are taken with respect to the storage of personal data:

21.1.1 All electronic copies of personal data should be stored securely using passwords and data encryption;

21.1.2 All hardcopies 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;

21.1.3 All personal data stored electronically should be backed up daily with backups stored offsite. All backups should be encrypted.

21.1.4 No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the Company or otherwise without the formal written approval of and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary; and

21.1.5 No personal data should be transferred to any 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 the Company 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 the Company that all suitable technical and organisational measures have been taken).

22 Data Security - Disposal

22.1.1 When 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. For further information on the deletion and disposal of personal data, please refer to the Company's Data Retention Policy.

23 Data Security - Use of Personal Data

The Company shall ensure that the following measures are taken with respect to the use of personal data:

23.1.1 No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested by following internal IT security procedures.

23.1.2 No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, that outside of the expected operational duties.

23.1.3 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;

23.1.4 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; and

23.1.5 Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of The Data Protection Officer to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third- party service such as the TPS.

24 Data Security - IT Security

The Company shall ensure that the following measures are taken with respect to IT and information security:

24.1 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.

24.2 Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Company, 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;

24.3 All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. The Company's IT staff shall be responsible for installing any and all security-related updates as soon as reasonably and practically possible, unless there are valid technical reasons not to do so; and

24.4 No software may be installed on any Company-owned computer or device without the prior approval of the ICT Manager.

25 Organisational Measures

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

25.1 All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the GDPR and under this Policy, and shall be provided with a copy of this Policy;

25.2 Only employees, agents, sub-contractors, or other parties working on behalf of the Company 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 the Company;

25.3 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so;

25.4 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised;

25.5 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;

25.6 Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

25.7 All personal data held by the Company shall be reviewed periodically, as set out in the Company's Data Retention Policy;

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

25.9 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the GDPR and this Policy by contract;

25.10 All agents, contractors, or other parties working on behalf of the Company 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 Company arising out of this Policy and the GDPR; and

25.11 Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

26 Transferring Personal Data to a Country Outside the EEA

26.1 The Company may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA.

26.2 The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:

26.2.1 The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data;

26.2.2 The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;

26.2.3 The transfer is made with the informed consent of the relevant data subject(s);

26.2.4 The transfer is necessary for the performance of a contract between the data subject and the Company (or for pre-contractual steps taken at the request of the data subject);

26.2.5 The transfer is necessary for important public interest reasons;

26.2.6 The transfer is necessary for the conduct of legal claims;

26.2.7 The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or

26.2.8 The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

27 Data Breach Notification

27.1 All personal data breaches must be reported immediately to the Company's Data Protection Officer.

27.2 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.

27.3 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 29.2) 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.

27.4 Data breach notifications shall include the following information:

27.4.1 The categories and approximate number of data subjects concerned;

27.4.2 The categories and approximate number of personal data records concerned;

27.4.3 The name and contact details of the Company's data protection officer (or other contact point where more information can be obtained);

27.4.4 The likely consequences of the breach;

27.4.5 Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its

possible adverse effects.

28 Implementation of Policy

This Policy shall be deemed effective as of 27th March 2019. 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:

Signature

Name of Approver	:	**Sant Shri Trilochan Das Ji**
Position	:	President Head and Patron
Policy Owner Name	:	**Tarinderjeet Singh**
Position	:	Head IT
Witness Name	:	
Address	:	
Date	:	2nd April 2019
Place	:	

Policy Guidelines under EU General Data Protection Regulation (GDPR) and Data Protection Act 2018 As Is

1. Purpose

1.1 The EU General Data Protection Regulation (GDPR) took effect on 25 May 2018. Together with the Data Protection Act 2018, which adopts the GDPR standards for all general data in the UK, it replaced the Data Protection Act 1998 (DPA 1998), and applies to the processing of **all** personal data. Electoral Registration Officers (EROs) and Returning Officers (ROs) are **personally responsible** for ensuring that they comply with the requirements of data protection legislation.

1.2 We have been working with the Association of Electoral Administrators (AEA), Cabinet Office, the Information Commissioner's Office (ICO), the Scottish Assessors Association (SAA) and the Society of Local Authority Chief Executives (SOLACE) to identify the impact of the GDPR on Electoral Registration Officers (EROs) and Returning Officers (ROs).[1]

1.3 It is important to remember that data protection requirements have been in place for many years. Although the GDPR does broaden the requirements, particularly in relation to demonstrating accountability and transparency, many of the key principles are the same as those in the DPA 1998.

1.4 The new data protection legislation does not override requirements to gather and process information as set out in existing electoral law but there will be an impact on how this information is processed and the responsibilities of EROs and ROs to keep data subjects informed.

1.5 This resource is designed to support you in meeting your obligations, as they relate to your electoral administration responsibilities. We have included practical examples where possible.

Where we consider that there is a particular consideration or action you should take in light of the GDPR, we have highlighted this in break-out boxes like this one throughout the resource. We have summarised these actions in checklist form in **Appendix 1**.

1.6 We have shared this resource with the Cabinet Office's Suppliers' Group network to help them prepare to support you in managing the impact of the GDPR on your delivery of well-run elections and electoral registration.

[1] **In this resource we use 'RO' as a generic term to refer to all types of Returning Officer.**

1.7 This resource will be updated to take account of emerging examples of good practice. It should be read alongside our core guidance for EROs and ROs.

2. Data controllers

Registering as a data controller

2.1 EROs and ROs have a statutory duty to process certain personal data to maintain the electoral register and for the purpose of administering an election. As such, they will be subject to the requirements of the GDPR as '**data controllers**'.

2.2 Under the Data Protection Act 1998, data controllers were required to register with the Information Commissioner's Office (ICO). Although there is no such requirement under GDPR, the Digital Economy Act 2017 makes provision for data controllers to register with the ICO from 1 April 2018.

2.3 Advice from the ICO is that **all data controllers will need to ensure that they are registered.** This means that EROs and ROs must be registered separately to their council. The ICO have advised that where the ERO and the RO are the same person, one registration can cover both roles. The ICO have also confirmed that where you have an additional role as a Regional RO, Police Area RO, Combined authority RO etc… one registration can be used for all titles but this needs to be included in the 'name' of the organisation when registering. In Scotland, where the ERO and the Assessor are the same person, the ICO have advised that one registration can also cover both roles, but both titles need to be included in the 'name' of the organisation when registering.

2.4 In relation to the fee to register as a data controller, the ICO have provided further guidance on their website, including examples of how the fee should be calculated. It should be noted that when calculating the number of staff you employ, this should be determined pro rata, i.e. evened out throughout the year. For example, if you are an RO and you only employ staff in April and May to administer an election, the total staff employed in April and May would need to be apportioned throughout the year to determine the number of staff you employ. As such, it is likely that the fee would always fall into the lower category. If you are using a joint registration as ERO/RO, you will need to be careful when calculating the number of staff since you will need to consider the total staff across both functions.

2.5 Questions in relation to registering as a data controller should be directed towards the ICO.

Appointing a data protection officer

2.6 Under the GDPR, a "public authority" must appoint a data protection officer (DPO) to advise on data protection issues. As ERO or RO, you are not currently included in the definition of a "public authority" contained in Schedule 1 to the Freedom of Information Act 2000 and are therefore **not** required to appoint a DPO for the conduct of your duties. However, you can choose to appoint a DPO if you wish. Your appointing council must have a DPO in place and you should liaise with them over good practice in relation to data protection.

Accountability and transparency

2.7 A key element of the GDPR is the increased focus on **accountability and transparency** when processing personal data. You must be able to **demonstrate** that you comply with your obligations under the GDPR, ensuring that personal data is processed lawfully, fairly and in a transparent manner. The key to achieving this is to have and maintain written plans and records to provide an audit trail.

2.8 In many cases, you will already have these plans and records in place. For example, you will already have registration and election plans, and associated risk registers, that outline your processes and the safeguards that you have in place. Although you will need to review these documents to ensure data protection remains integral and that they are GDPR compliant, they will provide a sound basis for you to meet your obligations under the GDPR. However, you are also likely to need to implement further demonstrable processes to show that you are processing personal data lawfully, fairly and in a transparent manner.

2.9 We have produced a cover sheet for the inspection of the register which sets out how it may be used and the penalty for misuse.

2.10 Records should also be maintained of every person or organisation supplied with absent voting lists. Similarly, records should be maintained of every person organisation supplied with the electoral register, not just those who pay to receive it. You should ensure that every person/organisation receiving the register, whether on publication, by sale, or on request, is aware that:

- they must only use the register for the purpose(s) specified in the Regulations permitting its supply
- once the purpose for which the register has been supplied has expired, they must securely destroy the register
- they understand penalty for misuse of the register

2.11 The information suggested above is included in the cover sheets we have made available for the sale and supply on request of the electoral register.

Action: If you have not already done so, speak to your council's data protection officer/information officer. The GDPR will impact on your council as a whole, so you should not need to address the requirements in isolation. You should also utilise the ICO's website which has detailed guidance to support you in meeting your obligations, including specific guidance on accountability and transparency.

Action: Review all of your processing activities and consider if there are further measures you can put in place to **demonstrate** that you are processing personal data lawfully, fairly and in a transparent manner.

3. Lawful basis for processing

3.1 For the processing of personal data to be lawful, it must be processed on a 'lawful basis' as set out in Article 6 of GDPR. These include:

- **Legal obligation**: the processing is necessary to comply with the law (not including contractual obligations); or

- **Public task**: the processing is necessary to perform a task in the public interest or in the exercise of official authority vested in you as the data controller; or
- **Legitimate interests**: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks); or
- **Consent**: the individual has given clear consent for you to process their personal data for a specific purpose. For further information see the ICO's guidance on consent.

3.2 Processing without a lawful basis runs the risk of enforcement activity, including substantial fines, by the ICO (see 'Breaches and sanctions' for further information).

3.3 In the main, the ICO have advised that the processing of personal data by EROs/ROs is likely to fall under the 'lawful basis' that it is 'necessary for the performance of a task carried out in the public interest or in the exercise of the official authority vested in the controller'.

3.4 It is for you to determine what the lawful basis for processing the data is, and to document your approach. You must clearly set out in your privacy notice which lawful basis you are relying on for processing and cite the relevant UK law where applicable. You may rely on more than one legal basis if you consider it appropriate.

3.5 We have provided examples below of lawful processing based on processing to perform a public task vested in you by UK law.

Action: Undertake an audit of **all** the personal data that you collect to determine the lawful basis on which you are collecting/processing it.

Processing for the performance of a public task

3.6 This lawful basis covers public functions and powers that are set out in UK law or the performance of specific tasks in the public interest, also set out in UK law.

3.7 For example, Regulation 26 of the Representation of the People Regulations 2001 (RPR 2001) sets out the requirements for an application to register, requiring an ERO to process National Insurance numbers and dates of birth as part of the application. This is part of the ERO's overall statutory duty to maintain the register of electors under Section 9 of the Representation of the People Act 1983 (RPA 1983). Similarly, Rule 6 of the Parliamentary Election Rules requires an RO to process personal data relating to a candidate for nomination purposes. This is part of the RO's overall statutory duty to administer the election in accordance with the Parliamentary Election Rules under Section 23 of the RPA 1983. **In these situations, the lawful basis for the processing is the performance of a public task (i.e. maintaining the register of electors, and administering the election) in the public interest, as provided for in electoral law.**

3.8 You will also need to consider the appropriate lawful basis for the processing of personal data not covered by electoral legislation. For example, employment legislation may require you to process personal data relating to the right of polling station staff or canvassers to work in the UK.

Action: Where you are processing personal data because it is necessary for the performance of a public task, determine and record what the basis for that public task is. This will enable you to demonstrate the lawful basis on which you are processing all personal data. The legislative references in the Commission's guidance for EROs and ROs may help with this.

The edited register

3.9 Regulation 93 of the RPR 2001 requires an ERO to publish an edited register. While electors may 'opt-out', EROs are required to include their details in the edited register if they do not do so.

3.10 The ICO have confirmed that as legislation provides for a statutory opt-out, coupled with the duties placed on EROs, this means that EROs are processing personal data for inclusion on the edited register on the 'lawful basis' that it is necessary to perform a public task. Therefore the GDPR conditions for consent will not apply and the **GDPR will not impact on the edited register**.

Right to object

3.11 Article 21 of the GDPR includes the "right to object" meaning that the data subject can object to the processing of their personal data. This right **does** apply when processing is required for the performance of a public task (such as maintaining the electoral register).

3.12 Section 11 of the Data Protection Act 1998 allowed electors the right to require you to exclude them from the edited register (also known as the open register) on a permanent basis (or until further notice). This continues under Article 21.

3.13 For example, Regulation 93A of the RPR 2001 prevents an elector from changing their edited register preference on a HEF. However, if you receive a response to the HEF and the elector has themselves clearly indicated on the form that they want to be removed from the open register until further notice, you should treat the HEF response as a notice under Article 21 of the GDPR and amend the register accordingly. Further information on this process is set out in Chapter 4 of Part 3: 'Annual canvass'.

3.14 The right to object to processing cannot however be applied to information where the collection of or the nature of the processing is specified in electoral law. For example in relation to electoral registration, the data subject can object to the processing of their email or telephone contact details but not to the use of their name or home address for the purpose of maintaining the electoral register.

3.15 Similarly to demonstrate that you are complying with the principles of processing personal data, ensuring that it is processed lawfully, fairly and in a transparent manner, you should maintain records to detail any request made under the right to object to processing. Your Electoral Management Software provider may have the facility to record consent against elector records and you should liaise with them to understand how to manage the process in practice.

3.16 The email invitation to register (ITR) that you must use has been updated to include an unsubscribe option to allow electors to make a request under the right to object to the use of their contact information for this purpose.

Action: Review your existing email templates and ensure that where you communicate with electors by email, you include an 'unsubscribe' option on all emails to allow the data subject to object to the use of their contact information for this purpose.

Right to be forgotten

3.17 Article 17 of the GDPR introduces the "right to be forgotten" meaning that a data subject can request that you delete their information without "undue delay".

3.18 The right to be forgotten does **not** apply when processing is required for the performance of a public task (such as the maintaining of electoral registers) or where it is necessary for archival in the public interest.

3.19 For example, an elector cannot contact an ERO and ask to be removed from 'old/historical' electoral registers since their inclusion on that register originated from a legal obligation on the ERO. However, they may request that information collected on grounds of consent (for example, where an elector gives consent to use of their email address) is deleted or removed at any time.

3.20 As set out in paragraph **5.8**, the RO is required to publish notices relating to an election. These may include personal information relating to candidates, subscribers and agents. Although a person could not use the 'right to be forgotten' to require that their details are removed from a statutory notice, they could exercise the right to have their details removed from a notice you have made available on your council website after the election, if the deadline for an election petition had passed (when the notice serves no further purpose) Therefore, you should either remove notices published on your website, or remove the personal data contained in these notices, once the petition deadline for that election has passed.

3.21 You should consider whether it is appropriate to retain that data (see 'Document retention'). For example, if you have existing records of email addresses or phone numbers collected through an application to register, at the time that you next use that information, you should take appropriate measures such as:

- explain the data subjects right to object to further processing
- link to your privacy notice
- the inclusion of the 'unsubscribe' option mentioned in paragraph **3.16** which allows the data subject to object to the use of their contact information for this purpose

4. Privacy notices: the right to be informed

4.1 The data protection principle that the data subject must be provided with sufficient information to enable them to understand how their personal data is used continues under the GDPR. This has traditionally been achieved via a **privacy notice** or **fair processing notice**.

4.2 The GDPR sets out the following requirements for notifying data subjects:

- When data is collected directly from the data subject, the notice must be given at the point of collection. For example, a notice needs to be included in letters requesting documentary evidence under the exceptions process, or on application forms for the appointment of election staff. It is not necessary to provide a link to a privacy notice on poll cards. Poll cards do not collect personal information, they contain information from the electoral register and absent vote lists which are

publically available under electoral law. However, your privacy notice should set out that personal data contained in the electoral register and absent voting lists will be used to issue poll cards in advance of an election;

- When data is not collected directly, the notice must be given to the data subject within one month or at the first point of contact. This is not necessary if the data subject was notified of the terms of the privacy notice when the data was originally collected by the primary data controller (for example, if you use personal data collected by council tax to verify an applicant for registration, a notice is not required if one was given to the applicant by the council tax department when the personal data was originally collected).

4.3 The information in a privacy notice must be provided in clear plain language, particularly when addressed to a child, and be provided free of charge.

4.4 It is important that your privacy notice is specific to your local circumstances and the personal data that you process. It must be kept up to date to meet any changes in your approach to processing data. Your council's data protection/information officer will be able to help you with the contents of the required notices. **You will need to ensure you have a privacy notice published on your website from 25 May 2018.** This can be a standalone privacy notice or can be included as part of your council's privacy notice.

4.5 Due to the differences across ERO/RO functions due to devolution, shared services, differences in EMS suppliers and internal structures and processes within each council it is not appropriate for the Commission to provide a template privacy notice. However, **Appendix 2** provides a checklist for what a privacy notice must contain.

4.6 In particular, your privacy notice needs to set out how you will use the personal data that is collected. The following bullet points are not an exhaustive list, but give an indication of the sort of things that could be covered in your privacy notice:

- the fact that personal data contained in the electoral register will be used to conduct an annual canvass, including issuing HEFs to all households and following up with non-responding properties
- how information in the electoral register may be used using the prescribed wording to describe the electoral register and the open/edited register (as included on the voter registration form)
- the fact that personal data contained in the electoral register and absent voting lists will be used to issue poll cards in advance of an election
- that a postal voter's signature (where required) and date of birth provided on a postal voting statement will be compared against that postal voter's signature and date of birth held on the personal identifiers record

4.7 Our letter templates and absent voting forms, and the HEF and voter registration forms have been updated to reflect enhanced data protection messaging. The Cabinet Office have similarly updated www.register-to-vote.gov.uk.

Action: Be clear for what purpose you collect, hold and use people's data – and ensure that you are not using it for other unrelated purposes. You should periodically review your privacy notices with your council's data protection officer/information officer to ensure they remain compliant with GDPR. The checklist provided in **Appendix 2** may help you with this. Ensure your privacy notice is clearly visible on your website and is referenced when communicating with electors and others.

Sharing good practice
The electoral services team at Redcar & Cleveland Borough Council have developed a tri-fold leaflet – included at **Appendix 3** – that explains to electors how their personal data is handled and used.

5. Document retention

5.1 Under the GDPR, it continues to be the case that personal data processed for any purpose shall not be kept for longer than is necessary for that purpose. Therefore, once the purpose for collecting the data has passed, you need to consider if there is a reason for you to retain that data.

5.2 The GDPR does permit personal data to be stored for longer periods if the data will be processed solely for archiving purposes in the public interest, or for scientific, historical, or statistical purposes and subject to the implementation of appropriate safeguards. Examples of this might include old electoral registers held to determine the eligibility of overseas applicants, or election results.

Action: Practice data minimisation – don't ask for, and process, personal data if you don't need it. For every document you possess, ask yourself "for what reason am I keeping this document?"

Document retention policy

5.3 Maintaining your **document retention policy** will help you to demonstrate that you are complying with the principles of processing personal data, ensuring that it is processed lawfully, fairly and in a transparent manner.

5.4 Your document retention policy should set out the following for all documents you receive and hold:

- whether the document contains personal data
- the lawful basis on which any personal data was collected (see 'Lawful basis for processing')
- your retention period
- your rationale for the retention period (which might relate to a requirement in electoral law, for example, home address forms at UK Parliamentary elections must be destroyed after 21 days)

5.5 In some cases this will be straightforward since electoral legislation will require a set period for which documents are retained. For example, at a UK Parliamentary election, Rule 57 of the Parliamentary Election Rules requires that specific documents relating to the election must be retained for one year and then, unless otherwise directed, be destroyed. In other cases, you will need to make a local decision and justify this in your document retention policy.

5.6 If you are an ERO, your document retention policy will include (but will not be limited to) documents received due to:

- an application to register (i.e. application form and any documentary evidence where required) (see Chapter 4 of Part 4: 'Maintaining the register throughout the year' for further information on the retention period for application documents)

- an application for an absent vote (see Chapters 2 and 3 of Part 5: 'Absent Voting' for further information on the retention period for application forms)
- your inspection of council records or your power to require information from any other person for the purposes of maintaining the register (see Chapter 2 of Part 4: 'Maintaining the register throughout the year' for further information)
- a request to an applicant/elector for further information to help you determine if they are resident (see Chapter 3 of Part 2: 'Registration framework' for further information)
- your power to require evidence as to age or nationality (see Chapter 3 of Part 2: 'Registration framework' for further information)

5.7 Part F of our guidance for Returning Officers for each election type contains specific advice on the retention of election documents. You will also need to consider notices published for the election (see paragraph **5.8** below) and staff records, including appointment and payment records. Your retention plan should reflect your approach to the retention of all documents, for each election type. For example, in relation to UK Parliamentary election nomination papers, Part C: 'Administering the poll' of our guidance says that: "… you should store the nomination papers securely for one year after the election due to the time limit for prosecution in case of an election petition. The home address form must be destroyed after 21 days."

Election notices published on your website

5.8 Notices published for an election should be made available on your website and so you will need to ensure that they are removed at the appropriate time.

5.9 You will need to consider whether it is appropriate or necessary for the notices to remain published on your website beyond the expiry of the petition period for that election. For example, the notices serve specific purposes, i.e. advising who will be a candidate at the election. Once the election is over, and the opportunity to question that election has passed, they serve no further purpose. Therefore, you should either remove notices published on your website, or remove the personal data contained in these notices, once the petition deadline for that election has passed.

5.10 Part F of our guidance for Returning Officers for each election type contains specific advice on post-election activities, including supplementary resources on the retention and inspection of election documents.

5.11 It is essential that, unless there is a reason not to, for example a legal challenge, you **securely destroy** documents in accordance with your document retention policy. Therefore you will need to appropriately label documents and tag electronic files with destruction dates, and these should be referenced in your electoral registration and election plans.

Action: Ensure your document retention policy is up-to-date, covers every document you process, and that you and your staff adhere to it.

6. Data storage

6.1 There are no specific changes in the GDPR concerning the storage of data. The principle remains to protect against unauthorised or unlawful processing and against accidental loss. Article 32 requires

that appropriate technical and organisational measures are in place to **ensure a level of security, appropriate to the risk.**

6.2 The GDPR also does not make any relevant changes to the mechanisms for supplying or transferring personal data, including encryption standards.

6.3 Therefore, it remains for you to determine that appropriate security measures are in place to protect personal data, ensuring that you act as a '**guardian**' for that data.

Action: Your council will have corporate standards and processes for data handling and security. You should review your processes with advice from your data protection officer and information management/IT departments. They will be able to help you identify any risks to the security of the data you hold, whether on paper or stored electronically on your systems. Ensure you have processes in place to retrieve data and securely destroy it at the appropriate time, in accordance with your document retention policy.

7. Using contractors and suppliers

7.1 As a data controller, you may use a 'processor' to act on your behalf to process data. For example, if you send register data to a contractor to provide an automated response facility during the canvass or send absent vote data to a contractor to produce postal ballot packs for an election, you are using a processor.

Requirement for a written contract

7.2 Whenever you use a processor, the GDPR imposes a **legal obligation** to formalise the working relationship in a written contract which sets out:

- the subject matter, nature and purpose of the processing
- the obligations and rights of the data controller
- duration of the processing and
- the types of personal data and categories of data subjects

7.3 In addition, the GDPR requires that the contract must set out specific obligations on the processor, including that they:

- comply with your instructions
- are subject to a duty of confidentiality
- keep personal data secure and notify you of any breach
- maintain written records of the processing activities they carry out for you
- only use a sub-processor with your consent
- submit to audits and inspections and provide you with whatever information you need to ensure GDPR compliance
- delete or return all personal data to you as requested at the end of the contract

7.4 As the data controller, you remain ultimately responsible for ensuring that personal data is processed in accordance with the GDPR. However, if a processor fails to meet any of its obligations, or acts against your instructions, then it may also be liable to pay damages or be subject to fines or other

penalties or corrective measures. The ICO has provided guidance 'Contracts and liabilities between controllers and processors' which you should consider in relation to your contracts with data processors.

Appointing processors

7.5 The GDPR requires that you only appoint a processor that can provide '**sufficient guarantees**' that the requirements of the GDPR will be met.

7.6 We have shared this resource with the Cabinet Office's Suppliers' Group network to help them prepare to support you in managing the impact of the GDPR on your delivery of well-run elections and electoral registration.

Action: Ensure that data protection is integral in any tender exercise (documenting your decision-making process) and that the requirements in paragraphs **7.2** and **7.3** are met in any contract awarded.

Satisfy yourself that your existing contractors/suppliers are aware of their obligations under the GDPR, and that any existing contracts meet the requirements in paragraphs **7.2** and **7.3** from 25 May 2018.

8. Data sharing agreements with external organisations

8.1 As ERO, you may be obtaining personal data from partners (for example: student data from universities; resident data from care homes). In this situation, the partner will be a data controller in their own right.

8.2 Although the GDPR does not require a written agreement when sharing data between data controllers, it is strongly recommended that you agree with your partner a data sharing agreement/protocol. This will help you both demonstrate that you are acting in accordance with the GDPR and, importantly, will help to avoid any liability implications of one party being seen as a controller and the other being seen as a processor.

8.3 In **Appendix 4** we have made available a checklist that you can use when developing a data sharing agreement/protocol. Your council may already have developed a template agreement and, in any case, you should discuss any data sharing agreement with your council's Data Protection Officer/Information Officer.

Supply of the register

8.4 The RPR 2001 provides a statutory framework for the supply of the electoral register, and the ERO must supply the register in accordance with those Regulations. Similarly, the recipient must only use the register for the purposes specified in those Regulations. Whilst an ERO could have a data sharing agreement with an organisation in relation to the supply of the register (for example, a credit reference agency), there is no requirement for them to do so and each ERO would need to be careful

that the provisions contained in any such agreement did not go beyond the requirements in the Regulations.

Action: Put in place written data-sharing agreements with external organisations where you are receiving/sharing data on an ongoing basis. The checklist in **Appendix 4** may help you with this.

Sharing good practice
The Scottish Assessors Association (SAA) have made available the data sharing agreement being used by EROs to share data in Scotland.

9. Special categories of personal data

9.1 Regulation 26 of the RPR 2001 requires an applicant for registration to provide their nationality or nationalities, or, if they are not able to provide that information, the reason they are not able to do so. The ERO processes this nationality data in order to determine which elections the elector is entitled to vote at. The GDPR will not affect the requirement for nationality information to be provided, however, under the GDPR, nationality data is classed as a special category of personal data because it may reveal an individual's racial or ethnic origin.

9.2 You may also deal with special categories of personal data through: documents received as part of the documentary exceptions process; documents received as part of an application for anonymous registration; or staff appointment information.

9.3 The GDPR prohibits the processing of special categories of personal data unless an additional lawful basis beyond those for the main purposes of processing data is met. The appropriate lawful basis for processing special categories of personal data for electoral purposes would be that it is necessary for reasons of substantial public interest and with a basis in UK law (see for example, paragraph **3.7**).

9.4 The Data Protection Bill takes this further, stating that the special requirements **only** apply if the data controller has in place a 'Policy Document'. Therefore, as introduced, the Data Protection Bill requires that in order to process nationality data – whether as part of an application to register, or in relation to staff appointments – you must have in place a **policy document** which, amongst other things, must explain:

- the procedures for complying with the data protection principles
- the policies for retention and erasure.

9.5 Therefore, your policy document will need to reflect your local processing procedures and your policies for the retention and erasure of personal data. This policy document must be kept until six months after the processing ceases, be reviewed and updated at appropriate times and be made available to the ICO on request. We can provide a copy of the Commission's own policy document upon request for your reference. However it is important to note that the Electoral Commission processes different data to ERO's and RO's.

Action: Ensure you have a policy document which will enable you to process special categories of personal data in accordance with data protection legislation.

10. Data protection impact assessments (DPIAs)

10.1 Data protection impact assessments (known previously as **privacy impact assessments**) help to identify, assess and mitigate risks, ensuring that data protection principles are integral to the design of processes. They are currently considered good practice under the 1998 Act, but the GDPR will **require** that a DPIA is undertaken **before** processing when:

- You are using **new data processing technologies**. For example, if you have a new initiative to issue canvassers with tablets, you need to undertake a DPIA first. Where your processing is already underway (i.e. your canvassers are already using tablets), the GDPR does **not** require a retrospective DPIA. However, you should ensure that data protection principles are integral to your existing processing operations, and a DPIA can help evidence this.
- The processing is likely to result in a **high risk** to the rights and freedoms of individuals. Recital 75 of the GDPR provides further information as to what constitutes high-risk processing. Processing applications for anonymous registration is an example of high risk processing (see paragraph **10.3** for further information).

10.2 A DPIA is **not** required where a processing operation has a lawful basis that regulates the processing **and** a DPIA has already been undertaken.

10.3 In relation to applications for **anonymous registration**, the lawful basis for these is Section 9B of the RPA 1983 and Regulations 31G to 31J of the RPR 2001 which detail the processing required. This processing is high risk to anonymous electors/applicants since it relates to personal safety. **If you do not have a DPIA in place for processing anonymous registration applications, you should undertake one.**

10.4 You should undertake DPIAs as a matter of best practice when you undertake *any* new process. This will support the accountability principle enabling you to demonstrate that data protection is integral to the process. At **Appendix 5** we have included a template DPIA used by the Electoral Commission. It relates to our activities, so you will need to adapt it to make it relevant, but it may support you in undertaking your own DPIAs. You should speak to your council's Data Protection Officer/Information Officer before undertaking a DPIA.

Requirements of a DPIA

10.5 The GDPR does not specify a particular process to be followed when undertaking a DPIA but does set out minimum required features:

- A description of the proposed processing and the purposes – in relation to anonymous registration, this should include what the personal data is; who will have access; how it will be stored; who it will disclosed to
- An assessment of the necessity and proportionality of the processing – in most cases for an ERO or RO this will be processing for the performance of a public task (see for example, paragraph **3.7**)
- An assessment of the risks to the rights of the individuals affected
- The measures envisaged to address the risks and demonstrate compliance with the GDPR. For example, in relation to anonymous registration, the measures you put in place to keep the identity of anonymous electors secure.

10.6 Where a set of similar processing operations present similar high risks, a single DPIA may be undertaken to address all of those processing operations.

10.7 The ICO has provided guidance on DPIAs on their website which includes examples of good practice.

Action: Review any DPIAs you have in place and determine if your processing operations require any further DPIA to be undertaken.

Consider how you can ensure data protection is integral to **all** of your processing. In addition to undertaking DPIAs, you should ensure that all your training – whether for canvassers, polling station staff, or your electoral services team – reflect data protection requirements. This will help you to embed the data protection principles in your work and demonstrate compliance. Ensure you discuss any data protection training with your council's Data Protection Officer/Information Officer.

11. Inspecting council records

11.1 Guidance on inspecting council records (under Regulation 35 and 35A of the RPR 2001), is contained in Chapter 2 of Part 4: 'Maintaining the Register throughout the year' and in Section 2 of the Ministerial Guidance, also in Part 4.

11.2 As ERO, you will need to demonstrate that all information obtained – whether from inspecting council records, or disclosed by your council – complies with the principles of processing personal data, ensuring that it is processed lawfully, fairly and in a transparent manner. Therefore, you should record details of:

- The records to be checked.
- A schedule of when those checks are carried out.
- The lawful basis on which you are processing that information. For example, Section 9A places an obligation on the ERO to inspect records that they are permitted to inspect as part of their duty to maintain the electoral register. Section 9A therefore provides the statutory basis by which you process personal data obtained through council records.
- Measures to ensure appropriate security are in place to protect the data (for example, encrypting/password protecting data whenever it is transmitted, and using secure storage).
- What action you have taken on the basis of the information you have obtained.
- Retention and secure disposal of data (in accordance with your document retention plan).

11.3 Maintaining such records will help you to demonstrate that you are complying with your obligations under the GDPR and your duties under Regulation 35 and 35A of the RPR 2001.

Action: Ensure you maintain records of the council records you inspect, in accordance with paragraph **11.2**. You could make these records form part of your registration plan.

12. Subject access requests

12.1 Subject access requests (SARs) remain under the GDPR. However, subject to a few conditions, these must now be provided **free of charge**, i.e. the £10 fee has been removed. Subsequent copies may be charged for, but the charge must be "reasonable" and "based on administrative costs".

12.2 **A data subject is entitled to see personal information that is held about them.** Information requested by data subjects must be provided without delay and in any event within one month (although it can be extended to two months in certain conditions).

12.3 There is no requirement for the request to be made in writing under GDPR. You must, however, be satisfied of the requesters' identity before fulfilling the request.

Postal voting statements

12.4 Candidates and agents are not entitled to inspect the application form of an absent voter, unless it is their own personal application form. However, Regulation 85A of the RPR 2001 permits the RO to show the relevant entry in the personal identifiers record (i.e. the name, signature (unless a waiver has been granted) and date of birth of the relevant absent voter) to agents when personal identifiers are being verified.

12.5 As set out in our FAQs for postal vote rejection notices, a postal voter who has received a postal vote identifier rejection notice for example may request to see their postal voting statement. Such a request should be treated as a subject access request and, as **a data subject is entitled to see personal information that is held about them**, the postal voter should be permitted to see the information held on their postal voting statement.

Certificates of registration

12.6 We are aware that some EROs currently charge electors for a letter confirming their residency, known as a "certificate of registration".

12.7 Under GDPR no charge can be made for fulfilling a subject access request unless the request can be deemed excessive or repetitive. In the majority of instances, providing confirmation of a data subject's entry on the register via a certificate of registration will not meet this test and therefore no charge should be made.

Action: Taking account of the fact that subject access requests must be provided free of charge, you should review any charges you apply that are not set out in law.

Access requests for crime prevention

12.8 Schedule 2 of the DPA 2018 provided an exemption to data processing rules for the purposes of the prevention or detection of crime, or the apprehension or prosecution of offenders. Therefore, where you receive a request for information that you hold you will need to consider:

- the person or organisation making the request,
- the purpose of the request, and
- the enactment quoted requesting access

12.9 If satisfied that the request meets the purpose detailed above then you should supply the data.

12.10 It should be noted that Regulation 107 (Regulation 106 in Scotland) of the RPR 2001 provides for the ERO to supply the full register to the council that appointed them. An employee or councillor of that council may, disclose or make use of information contained in it, where necessary for the discharge of a statutory function of the council (or, in England and Wales, any other local authority) relating to security, law enforcement and crime prevention. If the request relates to the council's copy of the register, you should direct this to your council's Monitoring Officer.

13. Breaches and sanctions

13.1 A personal data breach includes breaches that are the result of both accidental and deliberate causes. They may include:

- **access by an unauthorised third party** – for example, your EMS system/council network being hacked
- **deliberate or accidental action (or inaction) by a controller or processor** – for example, your print supplier failing to process all absent vote data you have sent them, meaning that some electors are disenfranchised because they do not receive their postal votes in time (see paragraph **13.2** for examples of measures you should have in place to avoid this situation)
- **sending personal data to an incorrect recipient** – for example, sending an electoral register to someone who is not entitled to receive it
- **computing devices containing personal data being lost or stolen** – for example, laptops or iPads containing register or election data being stolen
- **alteration of personal data without permission** – for example, a canvasser falsifying HEF responses

13.2 Having robust proof-checking processes in place could help detect any errors and avoid data breaches before they occur. For example, when producing postal votes, you should have in place a process for checking live proofs, including those for postal proxies. You should attend the issue of postal votes to check the actual stationery being produced, which will highlight if any of the signed-off proofs have been inadvertently altered. Once they have been issued, you should monitor returns to ensure that you have received completed postal votes back from every polling district. This will help you identify

at an early stage if the issue was incomplete. These processes should be captured in your election plan. We have produced a proof checking factsheet which you can use to help quality assure your processes.

Action: Ensure that your registration and election plans and risk registers highlight the safeguards you have in place to avoid a personal data breach, particularly when you are undertaking high risk activities (such as producing poll cards, postal votes, etc.).

Requirement to notify

13.3 When a personal data breach has occurred, you need to establish the likelihood and severity of the resulting **risk to people's rights and freedoms**:

- If there is a risk, you must **notify the ICO** within 72 hours of becoming aware of the breach;
- If there is a **high** risk (as defined in paragraph **13.5** below), in addition to notifying the ICO, you must **inform the individuals concerned** directly without undue delay.

13.4 Where the risk is unlikely to impact on people's rights and freedoms, you don't have to report it to the ICO. If the risk is not high, you do not have to notify the individuals concerned. In both cases, you need to be able to justify your decision, so you should document your reasoning in line with the accountability principle.

13.5 ICO guidance defines a 'high risk' in terms of the severity of the potential or actual impact on individuals: "If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again the risk is higher. In such cases, you will need to promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach."

13.6 The ICO also has the power to compel you to inform affected individuals if they consider that there is a high risk.

Sanctions and penalties

13.7 Under the Data Protection Act 1998, the maximum fine the ICO is entitled to levy is £500,000. Under the GDPR, fines of up to €20m or 4% of turnover (whichever is greater). may be imposed for:

- failure to process personal data on a lawful basis, infringing the rights of data subjects;
- failure by a data controller in relation to the engagement of processors; or
- failure of a processor to process data only in accordance with the controller's instructions;

13.8 A maximum of €10 million (or 2% annual turnover) applies for other breaches including:

- failure to maintain security of personal data
- failure to report breaches (including to the data subject where required)
- failure to maintain records of processing activities
- failure to undertake a Data Protection Impact Assessment when required to do so

13.9 In addition to imposing fines, the ICO may audit offenders, issue reprimands and impose restrictions on the breaching party. Reputational damage could also be significant.

Action: Understand the consequences of failure to comply with your data protection obligations, and ensure you have procedures in place to detect, report and investigate any personal data breach.

Appendix 1 – Summary checklist of actions

This checklist summarises the actions highlighted throughout this resource for your reference.

#	Action	Y/N	Comment
1	Utilise your council's data protection officer to help meet your requirements and ascertain best practice		
2	Utilise the ICO's website to support you in meeting your obligations		
3	Ensure you are registered as a data controller, separately from your council		
4	Review your processing activities. How can you **demonstrate** you are processing data lawfully, fairly and in a transparent manner (see 'Accountability and transparency')		
5	Determine the lawful basis on which you are collecting/processing **all** personal data		
6	If you are processing data for the performance of a public task, determine and record what the basis for that public task is		
7	Maintain records where an elector objects to use of their contact information (see 'Right to object')		
8	Include an 'unsubscribe' option on all email communications (see 'Right to object')		
9	Consider removing election notices from your website after the petition deadline (see 'Right to be forgotten' and 'Document retention')		
10	Ensure you are using the updated HEF, voter registration forms, associated letters and email ITR available on our website		
11	Review your own forms and letters to check they contain appropriate data protection messaging (see 'Privacy notices')		
12	Ensure you are not using personal data for unrelated purposes (see 'Privacy notices')		
13	Review your existing privacy notices to ensure they remain compliant and detail the lawful basis you are relying on for processing		
14	Ensure your privacy notice is available and referenced when communicating with electors and others		
15	For every document you possess, ask yourself "for what reason am I keeping this document?" (see 'Document retention')		
16	Ensure your document retention policy is up-to-date, complete, and adhered to		
17	Review your arrangements for storing personal data taking account of any corporate standards		

#	Action	Y/N	Comment
18	Ensure you have processes in place to retrieve and securely destroy data at the appropriate time (see 'Document retention')		
19	Ensure data protection is integral in any tender exercise (see 'Using contractors/suppliers')		
20	Ensure existing contracts will be GDPR compliant		
21	Put in place written data-sharing agreements where you are receiving/sharing data (see also 'Inspecting local records')		
22	Develop a policy document to enable you to process special categories of personal data		
23	Undertake DPIAs as a matter of best practice when you undertake a new process		
24	Review existing DPIAs		
25	Ensure you have an appropriate DPIA in place for processing applications for anonymous registration		
26	Ensure that all staff training (core team, canvassers, polling station staff) reflects data protection requirements		
27	Ensure you maintain records when inspecting council records		
28	Understand that a data subject is entitled to see personal information that is held about them (see 'Subject access requests')		
29	Review any charges you apply that are not set out in law (see 'Subject access requests')		
30	Understand the penalties and sanctions for failure to comply with data protection legislation		
31	Ensure your plans and risk registers highlight the safeguards you have to avoid a data breach (see 'Breaches and sanctions')		
32	Ensure you have procedures to detect, report and investigate a data breach		

Appendix 2 – Checklist for Privacy Notice

As explained in Section 4 – Privacy Notices, information regarding how and why personal data is being processed must be provided to the data subject when data is being collected. This is achieved via a privacy notice which should contain the following:

#	Element	Y/N	Comments
1	Name of the Data Controller		
2	Contact for Data Protection Officer		
3	Purpose and lawful basis for the personal data that you process		
4	Basis of processing for special categories of data		
5	Legitimate interests claimed		
6	Recipients of the personal data that you collect and process		
7	International transfers and if applicable any safeguards in place		
8	Retention periods for the data and the criteria for setting that period (for example as set in legislation)		
9	Right to request rectification, portability and objection		
10	Right to withdraw consent		
11	Right to complain to the ICO		
12	Consequence (if any) of failure to supply data		
13	Existence of profiling and/or automated decision making		

Appendix 3 – Leaflet from Redcar & Cleveland Borough Council that explains to electors how their personal data is used

Sharing good practice

The following two pages contain a tri-fold leaflet (to be printed double-sided) developed by the electoral services team at Redcar & Cleveland Borough Council. It explains to electors how their personal data is handled and used.

Partner organisations

The process of checking citizens' personal identifiers to ensure eligibility for inclusion in the Electoral Register, is controlled by the Cabinet Office via the IER Digital Service.

This includes:

- The Department for Work and Pensions who use data provided to verify the identity of new applicants
- The Cabinet Office will inform the old local authority of people who have moved area

Information will be processed within the EEA and will not be shared with overseas recipients.
If your details are in the Open version of the Electoral Register, your name and address can be sold to third parties who may use it for any purpose. You can opt out of this version at any time and are given the opportunity annually as part of the Canvass of all households.

Can I see my records?

The Data Protection Act 2018 allows you to find out what information is held about you, on paper and computer records. This is known as 'right of subject access' and applies to your Electoral Services records along with all other personal records.

If you wish to see a copy of your records you should contact the Data Protection officer. You are entitled to receive a copy of your records free of charge, within a month.

In certain circumstances access to your records may be limited, for example, if the records you have asked for contain information relating to another person.

Do I have Other Rights?

The Data Protection Act 2018 allows you other rights; for example if there is an error in your records you have the right to make sure it is rectified or erased.

You have the right to opt out of the Open Version of the Register, at any time, and we must remove you from this version and tell the statutory recipients in the next update.

You have the right to be told if we have made a mistake whilst processing your data and we will self report breaches to the Commissioner.

Further information

If you would like to know more about how we use your information, or if for any reason you do not wish to have your information used in any of the ways described in this leaflet, please tell us. Contact the Data Protection Officer:

Name
Redcar & Cleveland Borough Council,
Contact details

You can also complain to the Information Commissioner:
https://ico.org.uk/

This is Your Personal Data

Electoral Services

How we handle your information

Information for the public

Everyone working for Electoral Services has a legal duty to keep and process information about you in accordance with the law.

This leaflet explains why we ask for your personal information, how that information will be used and how you can access your records.

Why is information recorded about me?

We use information about citizens, Electors and Voters to enable us to carry out specific functions for which we

are responsible and to provide you with a statutory service.

We keep records about potential and actual electors, voters, citizens, candidates and their agents, staff employed at an election and the people we need to pay. These may be written down (manual records), or kept on a computer (electronic records).

These records may include:

- basic details about you, for example, name, address, date of birth and nationality
- unique identifiers (such as your NI number),
- scanned application forms & dates of any letters of correspondence,
- notes about any relevant circumstances that you have told us
- details and records about the service you have received,
- your previous or any redirected address
- The other occupants in your home
- If you are over 76 or under 16/17
- Whether you have chosen to opt out of the Open version of the Register

What is the information used for?

Your records are used to help ensure that we provide you with the service that you need. We will, based on your nationality, include your name on the Electoral Register so that you are able to vote by your chosen method.

The Electoral Register is a public document which can be viewed by appointment only under strict control.

It is important that your records are accurate and up-to-date as they will help make sure that our staff are able to provide you with the help, advice or support you need.

If you do not provide us with this information then eligible citizens will not be able to vote and you may be breaking the law.

How long for?

In order to provide you with this service, we rely on our legal obligation. The Electoral Registration Officer & Returning Officer are obliged to process your personal data in relation to preparing for and conducting Elections. Your details will be kept and updated in accordance with our legal obligations and in line with statutory retention periods.

Occasions when your information needs to be disclosed (shared) include:

- To contracted printers to print your Poll cards, Postal Packs & other electoral material
- To registered political parties, elected representatives, candidates, agents and other permitted participants who are able to use it for Electoral Purposes only
- Credit reference agencies, the British Library, UK Statistics Authority, the Electoral Commission and other statutory recipients of the Electoral Register
- Details of whether you have voted (but not how you have voted) to those who are entitled in law to receive it after an election
- where the health and safety of others is at risk,
- when the law requires us to pass on information under special circumstances,
- crime prevention or the detection of fraud as part of the National Fraud Initiative

Anyone who receives information from us has a legal duty to keep it confidential

We are required by law to report certain information to appropriate authorities – for example:

- where a formal court order has been issued.
- to law enforcement agencies for the prevention or detection of a crime
- to the Jury Central Summoning Bureau indicating those persons who are aged 76 or over and are no longer eligible for jury service

Appendix 4 – Checklist for data sharing agreement

#	Element	Y/N	Comments
1	Is the purpose of sharing set out in the agreement?		
2	Is the lawful basis for sharing set out in the agreement?		
3	Has the necessity of the sharing been assessed?		
4	Have provisions for disclosure been identified?		
5	Are the organisations signing up to the protocol named in the document?		
6	Is the data to be shared described in detail?		
7	Is the method for the sharing specific, including nominated people/roles who need to send/receive the data?		
8	Is when and how often the data is to be shared set out?		
9	Have the risks of sharing been documented?		
10	Are security measures documented?		
11	Has each organisation checked/updated their privacy notice?		
12	Will any data be transferred outside the EEA, including hosting arrangements, and is this documented?		
13	Has the process for informing the data subjects been identified? Is there an exemption?		
14	Does the agreement include provision for data quality to be confirmed before sharing?		
15	Does the agreement include procedures for subject access requests, complaints and queries from data subjects?		
16	Does the agreement include specifications for staff training?		
17	Does the agreement include sanctions for failing to comply with the agreement?		
18	Does the agreement include procedures for dealing with breaches?		
19	Is the nature of security breaches clearly defined?		
20	Is there a mechanism for checking the effectives of the agreement?		
21	Does the agreement set out how it can be terminated?		

22	Does the agreement set out the basis for review, particularly in relation to the necessity of the data sharing?		

Sharing good practice
The Scottish Assessors Association (SAA) have made available the data sharing agreement being used by EROs to share data in Scotland.

Appendix 5 – Example Data Protection Impact Assessment (DPIA)

This is an example form used internally by the Commission to conduct DPIA's for your reference. It is not a complete guide to all you need to do to or consider when conducting assessments of this kind. You need to consider ICO guidance in this area and consult with your DPO to align assessments for your specific processing activities.

Complete the Y/N and team comments fields describing the activity or process for each question.

Description of the activity:				
Question	**Y/N**	**Notes**	**Team comments**	**DPO recommendations**
Will the project involve or impact on the collection and management of personal information? If yes – describe the activity		This includes the use, sharing, storage of personal data whether in the process or related activities		
Have you identified what information is **required** to be collected?		What is the minimum amount of information required for the activity?		

Have you identified the **purpose** for which you are collecting the personal information?		Is this as part of a contract? Statutory duty? Required for the public interest or needs consent?		
How will individuals be **informed** of the purpose for which their information will be held?		Via privacy notice, how will this be communicated – verbally, via system sign up? Or is there a reason not to tell data subjects about this processing?		
If consent is required how will consent/opt out be managed?		If requires consent, how will we ask for and audit consent?		
Does this activity make use of existing information for new purposes?		Reusing existing personal data for new purposes?		
Does the activity include the transfer of information outside of the organisation?		Is personal data being published? Shared with a contactor or third party?		

Does the activity include the sharing of information within the organisation?		Which team collects the information? Who else needs access?		
Where will the information be held?		Internal systems? Cloud services? Hard copy? Transferred to off-site storage?		
How many records of personal information will be held?		Expected number of data subjects concerned		
Who is the owner of the information?		Single point of contact for the day to day use and management of the data		

Further recommendations (Data Protection Officer to complete)

Area	**Notes**	**Description**
Access/security	How should this data be secured? Consistent across the media in which it is stored	
Restrictions	Does the activity relate to information which is in any way exempt from fair processing provisions?	
Accuracy checks	How frequently should accuracy be checked? How should this be managed?	

Retention/disposal	How long do we need to keep this data for? Is there a legal reason for keeping (or not keeping) the data? Where should in active records be stored?	
Policy/procedure/guidance	Is there a policy/procedure or guidance that covers this activity? Does it need updating?	
Review	What is the recommended period of review of this assessment?	
Protective marking	The minimum marking for personal information is 'Official'	

Note:

1. The Guidelines are based on the EU standards, Hence the documentation supporting companies are from UK currently. We have ignored some of the sections which are not applicable to Indian companies.

2. It is advised to fill the following:
   Appendix 1 – Summary checklist of actions
   Appendix 2 – Checklist for Privacy Notice
   Appendix 4 – Checklist for data sharing agreement
   Appendix 5 – Example Data Protection Impact Assessment (DPIA)
3. Signature on every page is required.

END OF THE DOCUMENT