

To: Finance, Resources and Customer Services Policy Board

On: 30 January 2019

Report by: Director of Finance and Resources

Subject: Councillors and Data Processor Agreements

1. Summary

- 1.1 The purpose of this report is to advise Councillors of their duties as individual data controllers in relation to personal information which the Council processes on its behalf.
- 1.2 Councillors generally have three different roles which are:-
- Member of the Council
 - Representative of constituents and
 - Representative of a political party
- 1.3 The Council is the data controller of personal information which a councillor has access to in his/her role as a member of the Council. The political party is the controller when a Councillor acts on behalf of the party.
- 1.4 However, when a Councillor is using personal information to represent constituents, for example, for surgeries or to progress complaints on their behalf, the Councillor is a controller in his/her own right.
- 1.5 This means that the Councillor has an individual responsibility for data protection compliance.

- 1.6 A data processor is anyone other than an employee of a controller who processes personal information on the controller's behalf. The Council processes personal information on behalf of Councillors by providing ICT services and equipment, including an email account and network storage and clerical support to facilitate the Councillor's role in representing constituents. In such circumstances, the Council is the processor and the Councillor is the controller.
- 1.7 Article 28(3) of GDPR places a duty on controllers to have a contract in place with a processor containing details of the processing and the obligations of the processor. The key obligation is that the processor must keep the personal information secure. This contract is known as a Data Processor Agreement.
-

2. Recommendations

It is recommended that the Board:-

- 2.1 Note the requirement for a Data Processing Agreement between Councillors and the Council in respect of personal information which the Council is processing on behalf of Councillors and
- 2.2 Agree to the draft Data Processing Agreement, attached as Appendix 1, being sent to all Councillors for signing.
-

3. Background

- 3.1 Both GDPR and the Data Protection Act 2018 came into force on 25 May 2018 and regulate how controllers process people's personal information. This legislation is enforced by the Information Commissioner's Office (ICO).
- 3.2 A controller is the person who decides the purposes for and manner in which personal information is used. A processor is someone who the controller asks to process personal information on his/her behalf.
- 3.3 The Council is the controller of Council information which a Councillor uses in his/her capacity as a member of the Council, for example, as a member of a Board. However, each Councillor is a controller of any personal information processed on behalf of his/her constituents.

As the Council provides clerical and ICT support to Councillors in relation to constituent information, the Council is a processor.

- 3.4 The ICO confirmed to the Council's Data Protection Officer in mid-November 2018 that their view is that each Councillor, as a controller, is obliged, under GDPR, to have a contract with the Council, known as a Data Processor Agreement. This is to protect Councillors in their role as controllers by ensuring that the Council and its staff keep this information secure. The ICO have indicated that they now expect Councils to enter into Data Processor Agreements with Councillors, detailing the Council's responsibilities to Councillors.
- 3.5 The draft Data Processor Agreement at Appendix 1 contains the provisions required by GDPR. Each Councillor will be asked to sign a Data Processor Agreement with the Council. This will ensure that all Councillors are compliant with the obligation in Article 28(3) of GDPR to have a contract with a processor and will oblige the Council to keep constituent information secure. In addition, this will reassure constituents and other parties who provide personal information to Councillors that Council staff assisting them will keep this confidential, secure and use this only on the instructions of the Councillor.

Implications of the Report

1. **Financial** - None
2. **HR & Organisational Development** –.None
3. **Community/Council Planning** – None

4. **Legal** - Entering into a Data Processor Agreement with the Council will ensure that Councillors are complying with their legal obligations as data controllers.
5. **Property/Assets** - None
6. **Information Technology** – The Data Processor Agreement means that use of Council ICT equipment or reliance on ICT support by Councillors for constituent information is GDPR compliant.
7. **Equality & Human Rights** -
 - (a) The Recommendations contained within this report have been assessed in relation to their impact on equalities and human rights. No negative impacts on equality groups or potential for infringement of individuals' human rights have been identified arising from the recommendations contained in the report because it is for noting only and is to ensure that the Council undertake to Councillors to keep personal information processed on their behalf adequately secure. If required following implementation, the actual impact of the recommendations and the mitigating actions will be reviewed and monitored, and the results of the assessment will be published on the Council's website.
8. **Health & Safety** - None
9. **Procurement** – None
10. **Risk**- The Data Processor Agreement is to protect Councillors against the risk of information security breaches by the Council in respect of information which is controlled by Councillors.
11. **Privacy Impact** – No Data Protection Impact Assessments (DPIA) is required as the Data Processor Agreement protects privacy.
12. **Cosla Policy Position** – Not applicable

List of Background Papers

- (a) Background Papers - None

Author **Allison Black, Managing Solicitor (DPO), extension 7175**

Councillor Data Processor Agreement

Appendix 1

Agreement between

Councillor [NAME], elected on [DD/MM/YYYY] to represent Ward [insert Ward] of Renfrewshire Council ("the Councillor")

and

Renfrewshire Council, a Scottish Local Authority incorporated under the Local Government etc. (Scotland) Act 1994 and having its principal offices at Cotton Street, Paisley ("the Council")

together "the Parties".

Definitions

"Agreement" means this Agreement.

"Controller" has the meaning given in Data Protection Laws.

"Processor" has the meaning given in Data Protection Laws.

"Data Protection Laws" means the Data Protection Act 2018 and any enactments thereunder or amendments thereto, the General Data Protection Regulation (Regulation EU 2016/679) ("GDPR"), the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications) and any legislation that, in respect of the United Kingdom, replaces, or enacts into domestic law, GDPR or any other law relating to data protection, the Processing of personal data and privacy as a consequence of the United Kingdom leaving the European Union.

"Data Subject Rights" means the exercise of any rights of a data subject in terms of Data Protection Laws, including a subject access request.

"Personal Data" has the meaning given in Data Protection Laws.

"Processing" has the meaning given in Data Protection Laws and cognate expressions shall be construed accordingly.

"Special Category Data" has the meaning given in Data Protection Laws.

1. It is agreed that the Personal Data described in the Schedule (Data Protection) to this Agreement will be processed by the Council on behalf of the Councillor. For the purposes of any such Processing, the Parties agree that the Council acts as the Processor and the Councillor acts as the Controller. The Processor has been instructed by the Controller to allocate staff to carry out this Processing on its behalf.

The Council must:-

- 1.1. agree and comply with the terms of the data processing provisions set out in the Schedule (Data Protection);
- 1.2. process Personal Data only as necessary in accordance with obligations under this Agreement and any written instructions given by the Councillor (which may be specific or of a general nature) and not for any other purposes, unless required to do so by law to which the Council is subject; in which case the Council must inform the Councillor of that legal requirement before processing unless prohibited from doing so by that law;
- 1.3. subject to Clause 1.2 only process or otherwise transfer any Personal Data to any country outside the European Economic Area with the Councillor's prior written consent;
- 1.4. take all reasonable steps to ensure the reliability and integrity of any Council staff who have access to the Personal Data and ensure that the Council staff:-
 - a) are aware of and comply with the Council's duties under this Agreement;
 - b) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed to do so by the Councillor or as otherwise permitted by this Agreement; and
 - c) have completed the Council's mandatory training on data protection and information security.
- 1.5. implement appropriate technical and organisational measures including those set out in the Schedule (Data Protection) and in accordance with Article 32 of the GDPR to protect Personal Data against unauthorised or unlawful Processing and against accidental loss, destruction, damage, alteration or disclosure, such measures being appropriate to the harm which might result from any unauthorised or unlawful Processing accidental loss, destruction or damage to the Personal Data and having regard to the nature of the Personal Data which is to be protected;
- 1.6. not engage a sub-processor to carry out Processing in connection with the Services without prior specific or general written authorisation from the Councillor. In the case of general written authorisation, the Council must inform the Councillor of any intended changes concerning the addition or replacement of any other sub-processor and give the Councillor a reasonable opportunity to object to such changes.
- 1.7. ensure that if the Council engages a sub-processor for carrying out Processing activities on behalf of the Councillor, the same data protection obligations are imposed on the sub-processor by way of a written and legally binding contract, in particular providing sufficient guarantees to implement appropriate technical and organisational measures. The Council shall remain fully liable to the Councillor for the performance of the sub-processor's performance of the obligations.

- 1.8. provide the Councillor with reasonable assistance including by such technical and organisational measures as may be appropriate in complying with Data Subject Rights under GDPR, including any subject access request and/or responding to any enquiry made, or investigation or assessment of processing initiated by the Information Commissioner's Office in respect of the Personal Data as soon as is possible.
- 1.9. Taking into account the nature of the Processing and the information available, assist the Councillor in complying with the Councillor's obligations concerning the security of the Personal Data, reporting requirements for data breaches, data protection impact assessments and prior consultations in accordance with Articles 32 to 36 of the GDPR.

These obligations include:

- a) ensuring an appropriate level of protection through technical and organisational measures that take into account the circumstances and purposes of the processing as well as the projected probability and severity of a possible infringement of the law as a result of security vulnerabilities and that enable an immediate detection of relevant infringement events;
 - b) notifying a Personal Data breach to the Councillor without undue delay and in any event no later than 24 hours after becoming aware of a Personal Data breach;
 - c) assisting the Councillor with communication of a personal data breach to a Data Subject;
 - d) supporting the Councillor with preparation of a data protection impact assessment;
 - e) supporting the Councillor with regard to consultation with the Information Commissioner.
2. At the end of the provision of Services relating to processing, the Council must, on the written instruction of the Councillor, arrange the disposal of all Personal Data and delete existing copies unless EU or UK law requires storage of the Personal Data.
 3. The Council must:-
 - a) provide such information as is necessary to enable the Councillor to satisfy itself of the Council's compliance with this Agreement;
 - b) allow the Councillor, his or her employees, auditors, authorised agents or advisers reasonable access to any relevant premises, during normal business hours, to inspect the procedures, measures and records referred to in this Agreement and contribute as is reasonable to those audits and inspections;
 - c) inform the Councillor if in its opinion an instruction from the Councillor infringes any obligation under Data Protection Laws

4. The Parties acknowledge that the inspecting party will use reasonable endeavours to carry out any audit or inspection under Clause 3 b) with minimum disruption to the Council's day to day business.
5. The Council must maintain written records, including in electronic form, of the categories of Processing activities carried out in performance of the Services or otherwise on behalf of the Councillor containing the information set out in Article 30(2) of the GDPR.
6. If requested, the Council shall make records referred to in clause 5 available to the Information Commissioner and co-operate with the Information Commissioner's Office in the performance of its tasks.

SCHEDULE (DATA PROTECTION)

Part 1: Data Processing provision as required by Article 28(3) GDPR.

1. Subject matter and duration of the Processing of Personal Data

The processing of personal data for the Councillor by the Council to support the activities of the Councillor as an elected representative

This agreement will extend from the date of signature until the Councillor no longer holds office.

2. The nature and purpose of the Processing of Personal Data

The Council will provide appropriate IT services and equipment, including an email account and network storage, and clerical support to facilitate the Councillor's role as an elected representative.

3. The types of Personal Data to be Processed

Name, address, contact details, details of issues which may include special category data, details of third parties.

4. The categories of Data Subject to whom Personal Data relates

Constituents, their families, and other individuals relevant to constituency work.

Part 2: Practical security measures

In compliance with its obligations under clause 1.5 with regard to the processing of personal data on behalf of the Councillor, the Council, as a minimum requirement, shall give due consideration to the following types of security measures:

- 2.1.1 Technical security;
- 2.1.2 Physical security;
- 2.1.3 Access control;
- 2.1.4 Security and Privacy Enhancing Technologies;
- 2.1.5 Staff awareness raising and training;
- 2.1.6 Incident Management/Business Continuity; and
- 2.1.7 Audit controls/due diligence.