GDPR Policy and Methods Summary applicable to the Data Processor role

Version: 2.1

Date: 11th February, 2019

Idox Elections, Second Floor, 1310 Waterside, Arlington Business Park, Theale, RG7 4SA
T (0)870 333 7101 E marketing@idoxgroup.com W elections.idoxgroup.com | www.idoxgroup.com/elections

Version Control

This version of the “GDPR Policy” document replaces all previous versions.

Uncontrolled when printed.

Table of Contents

Purpose of this document

This document explains the approach of Idox Elections to meeting its obligations as a data processor, as that term is defined and used within the General Data Protection Regulation (EU) 2016/679 ("**GDPR**").

It does not address how the company meets its obligations as a “data controller” of data employed in its own business processes.

Within the scope of this document, the role of data controller is performed by a customer of Idox Elections employing the company as a supplier of services and/or products.

Principles of the Policy

Data Subject: Idox Elections will not enter into communication with data subjects other than to inform them of the correct contact information of the data controller. All requests concerning GDPR rights will be passed on to the data controller without further investigation

Supply Chain: Idox Elections recognises its role as a prime data processor and ensures that sub-processors will meet standards which conform to Idox Elections norms including Confidentiality and International transfers (see below). GDPR readiness and conformity of sub-processors will be audited, initially through requests for self-assessment

Information Security: Idox Elections employs information security methods and processes which have been internally assessed as adequate to provide the safeguards needed for GDPR Confidentiality, Integrity and Availability requirements. Where necessary, IE has augmented or changed its information security processes to meet GDPR requirements which were not previously explicitly adhered to (e.g. 72 hour breach reporting).

Data Protection by Design and Default (DPbD&D): Idox Elections adheres to DPbD&D methods and is engaged in a programme of continuous improvement of its internal engineering processes which deliver software and services

Impact Assessments: when software releases comprise changes which may have an impact on data protection measures relevant to GDPR (personal data) the release will be augmented by a generic impact assessment which advises customers of the considerations they may need to make in implementing the software

Destruction of Data: in principle, the default position concerning personal data provided by the data controller is that the data will be deleted from all systems as soon as practically possible. This entails, for example, that names and addresses supplied as part of a canvassing support process will be automatically deleted after completion of the canvass. Data will always be deleted immediately (legislation permitting) on explicit instructions from the data controller

Confidentiality: all personnel with access to customer data will be bound by confidentiality and non-disclosure agreements. These controls are also applied to sub-contractors and service providers and their staff as appropriate

Location of Data: neither Idox Elections nor its agents will store, process or transfer data outside the EEA

GDPR additional Data Protection clauses added to Idox Elections contracts (May 2018)

1. DATA PROTECTION

1.1 The Parties acknowledge that for the purposes of the Data Protection Legislation, the Customer's Electoral Registration Officer is the Controller and the Contractor is the Processor. The only processing that the Contractor is authorised to do is determined by the Controller and may not be determined by the Contractor.

1.2 The Contractor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.

1.3 The Contractor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Controller, include:

(a) a systematic description of the envisaged processing operations and the purpose of the processing;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the Services;

(c) an assessment of the risks to the rights and freedoms of Data Subjects; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

1.4 The Contractor shall, in relation to any Personal Data processed in connection with its obligations under this Agreement:

(a) process that Personal Data only in accordance with the Controller's written instructions, unless the Contractor is required to do otherwise by Law. If it is so required the Contractor shall promptly notify the Controller before processing the Personal Data unless prohibited by Law;

(b) ensure that it has in place Protective Measures, which have been reviewed and approved by the Controller as appropriate to protect against a Data Loss Event having taken account of the:

(i) nature of the data to be protected;

(ii) harm that might result from a Data Loss Event;

(iii) state of technological development; and

(iv) cost of implementing any measures;

(c) ensure that:

(i) the Contractor Personnel do not process Personal Data except in accordance with this Agreement and the Controller's written instructions;

(ii) it takes all reasonable steps to ensure the reliability and integrity of any Contractor Personnel who have access to the Personal Data and ensure that they:

(A) are aware of and comply with the Contractor’s duties under this clause;

(B) are subject to appropriate confidentiality undertakings with the Contractor or any Sub-processor;

(C) 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 in writing to do so by the Controller or as otherwise permitted by this Agreement; and

(D) have undergone adequate training in the use, care, protection and handling of Personal Data; and

(d) not transfer Personal Data outside of the EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

(i) the Controller or the Contractor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Controller;

(ii) the Data Subject has enforceable rights and effective legal remedies;

(iii) the Contractor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and

(iv) the Contractor complies with any reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data;

(e) at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Agreement unless the Contractor is required by Law to retain the Personal Data.

1.5 Subject to clause 1.6, the Contractor shall notify the Controller immediately if it:

(a) receives a Data Subject Access Request (or purported Data Subject Access Request);

(b) receives a request to rectify, block or erase any Personal Data;

(c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

(d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement;

(e) receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law;

or

(f) becomes aware of a Data Loss Event.

1.6 The Contractor’s obligation to notify under clause 1.5 shall include the provision of further information to the Controller in phases, as details become available.

1.7 Taking into account the nature of the processing, the Contractor shall provide the Controller with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 1.5 (and insofar as possible within the timescales reasonably required by the Controller) including by promptly providing:

(a) the Controller with full details and copies of the complaint, communication or request;

(b) such assistance as is reasonably requested by the Controller to enable the Controller to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;

(c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;

(d) assistance as requested by the Controller following any Data Loss Event;

(e) assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.

1.8 The Contractor shall maintain complete and accurate records and information to demonstrate its compliance with this clause. This requirement does not apply where the Contractor employs fewer than 250 staff, unless:

(a) the Controller determines that the processing is not occasional;

(b) the Controller determines the processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; and

(c) the Controller determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

1.9 The Contractor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.

1.10 The Contractor shall designate a data protection officer if required by the Data Protection Legislation.

1.11 Before allowing any Sub-processor to process any Personal Data related to this Agreement, the Contractor must:

(a) notify the Controller in writing of the intended Sub-processor and processing;

(b) obtain the written consent of the Controller;

(c) enter into a written agreement with the Sub-processor which give effect to the terms set out in this clause [X] such that they apply to the Sub-processor; and

(d) provide the Controller with such information regarding the Sub-processor as the Controller may reasonably require.

1.12 The Contractor shall remain fully liable for all acts or omissions of any Sub-processor.

1.13 The Controller may, at any time on not less than 30 Working Days' notice, revise this clause by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Agreement).

1.14 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Customer may on not less than 30 Working Days' notice to the Contractor amend this agreement to ensure that it complies with any guidance issued by the Information Commissioner's Office