Scottish Borders Electoral Registration Officer

Policy statement on processing special category data and personal data relating to criminal convictions and offences

Introduction

With effect from 25 May 2018, data protection law requires controllers who process special category (i.e. sensitive) personal data, (or personal data relating to criminal convictions and offences) under various parts of the Data Protection Act 2018 to have an "appropriate policy document" in place setting out a number of additional safeguards for this data.

More specifically,

"The controller has an appropriate policy document in place in relation to the processing of personal data in reliance on a condition described in paragraph 38 if the controller has produced a document which—

> (a) explains the controller's procedures for securing compliance with the principles in Article 5 of the GDPR (principles relating to processing of personal data) in connection with the processing of personal data in reliance on the condition in question, and
>
> (b) explains the controller's policies as regards the retention and erasure of personal data processed in reliance on the condition, giving an indication of how long such personal data is likely to be retained."

This document is the policy adopted by the Scottish Borders Electoral Registration Officer in relation to this processing.

Policy Statement

1: Lawfulness, fairness and transparency:

All data flows into and out of the Electoral Registration Office are being assessed to determine the legal basis under which that data is processed and the results of the assessment are being documented. I am satisfied that I will have a legal basis for holding the personal data I hold, and that I will also have a valid legal basis for disclosing this personal data to third parties where this happens. Privacy notices are presently being drafted to comply with GDPR requirements (and to reflect the legal basis of processing). Please see www.scotborders.gov.uk/eroprivacy for further details. I am presently updating my data processor agreements and data sharing agreements to reflect the new legal requirements.

2: Purpose limitation:

The purposes for which data are collected are clearly set out in the relevant privacy statements. This includes reference to further use of data for internal management information purposes.

3: Data minimisation:

In assessing the data flows, I have also taken the opportunity to critically assess the need for each of the data fields in question and where superfluous data was being captured, I have now stopped capturing this.

4: Accuracy:

The Electoral Registration Office continually check data for accuracy and, where any inaccuracies are discovered, these are promptly corrected and any third party recipients of the inaccurate data notified of the correction.

5: Storage limitation:

The Electoral Registration Office only keeps personal information for the minimum period amount of time necessary. Sometimes this time period is set out in the law, but in most cases it is based on business need. I maintain a records retention and disposal schedule which sets out how long I hold different types of information for.

Ongoing management of the Electoral Registration Office records and information is subject to the provisions of a Records Management Plan, which was developed in terms of the Public Records (Scotland) Act 2011 and approved by the Keeper of the Records of Scotland. It is available online at:

https://www.scotborders.gov.uk/info/20060/access_to_information/363/what_information_we_hold.

The Records Management Plan sets out, in much greater detail, the provisions under which the Electoral Registration Office complies with its obligations under public records legislation, data protection and information security and is complementary to this policy statement.

6: Integrity and confidentiality:

The Electoral Registration Office has an approved Information Security Policy which sets out roles and responsibilities within the organisation in relation to information security. All staff are required to take information security training. My ICT systems have appropriate protective measures in place incorporating defence in depth and the systems are subject to external assessment and validation. I have policies and procedures in place to reduce the information security risks arising from use of hard copy documentation.

May 2018