The Electoral Commission

Data protection resource for Electoral Registration Officers and Returning Officers

General Data Protection (GDPR) and Data Protection Act 2018

February 2018 (updated May2021)

SAA
Scottish Assessors Association

Contents

1 Purpose....2
2 Data controllers....3
3 Lawful basis for processing....5
4 Privacy notices: the right to be informed....9
5 Document retention....11
6 Data storage....13
7 Using contractors and suppliers....14
8 Data sharing agreements with external organisations....16
9 Special categories of personal data....17
10 Data protection impact assessments (DPIAs)....18
11 Inspecting council records....20
12 Subject access requests....21
13 Breaches and sanctions....23
Appendix 1 – Summary checklist of actions....25
Appendix 2 – Checklist for Privacy Notice....28
Appendix 3 – Checklist for data sharing agreement....29
Appendix 4 – Example Data Protection Impact Assessment (DPIA)....31

1 Purpose

1.1 The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 apply 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 current 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 current data protection legislation broadens the requirements, particularly in relation to demonstrating accountability and transparency, many of the key principles are the same as those in the Data Protection Act 1998 (now superseded by the Data Protection Act 2018).

1.4 Data protection legislation does not override requirements to gather and process information as set out in existing electoral law but there is impact on how

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

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 data protection rules, 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 previously 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.

1.7 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.

2Data 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, in line with current data protection legislation they are acting as '**data controllers**'.

2.2 Data controllers are required to register with the Information Commissioner's Office (ICO)[2].

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

[2] Digital Economy Act 2017

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 A "public authority" must appoint a data protection officer (DPO) to advice 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 current data protection legislation is the focus on **accountability and transparency** when processing personal data. You must be able to **demonstrate** that you comply with your obligations as a data controller, 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 You will have developed registration and election plans, and associated risk registers, that outline your processes and the safeguards that you have in place. You will need to keep these documents under review to ensure data protection remains integral and that they are compliant with current data protection legislation. They will provide a sound basis for you to meet your obligations as a data processer. 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 the electoral register and absent voting lists, 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. Data protection legislation impacts 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.

3Lawful basis for processing

3.1 For the processing of personal data to be lawful, it must be processed on a 'lawful basis'[3]. 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

[3] Art 6 GDPR 2018

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 data protection conditions for consent will not apply and **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 For example, Regulation 93A of the RPR 2001 prevents an elector from changing their edited register preference on a canvass communication. However, if you receive a response to a canvass communication 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 canvass response as a notice under Article 21 of the GDPR and amend the register accordingly. Further information on this process is set out in our guidance for running electoral registration.

3.13 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.

3.14 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.

3.15 The email invitation to register (ITR) that you must use includes 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

3.16 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".

3.17 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.

3.18 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.

3.19 As set out in paragraph **5.9**, 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.

3.20 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 **3.15** 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 Data subjects must be provided with sufficient information to enable them to understand how their personal data is used, this is achieved via a **privacy notice** or **fair processing notice**.

4.2 Current data protection legislation 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.** 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 canvass communications 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 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 the current data protection legislation. 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.

5Document retention

5.1 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 However, data protection legislation 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) how you process and store documents received due to:

-
- an application to register (i.e. application form and any documentary evidence where required)

- an application for an absent vote
- your inspection of council records or your power to require information from any other person for the purposes of maintaining the register
- a request to an applicant/elector for further information to help you determine if they are resident
- your power to require evidence as to age or nationality

5.7 For further information refer to the relevant section on Access and Supply in our guidance for EROs.

5.8 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 **5.9** 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

5.9 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.

5.10 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.

5.11 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.

5.12 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.

6Data storage

6.1 The Data Controller has a duty to protect against unauthorised or unlawful processing and against accidental loss. Article 32 of the GDPR requires that appropriate technical and organisational measures are in place to **ensure a level of security, appropriate to the risk**.

6.2 Therefore, you must determine what appropriate security measures are in place to protect personal data, for example ensuring that personal data is encrypted when it is being transferred, thus 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, current data protection legislation 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, it is required 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 compliance with current data protection legislation
- 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 data protection principles. 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 law requires that you only appoint a processor that can provide '**sufficient guarantees**' that the requirements of the current data protection legislation will be met.

7.6 This resource was shared with the Cabinet Office's Suppliers' Group network to help them prepare to support you in managing the impact data protection obligations will have 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 current data protection legislation, and that any existing contracts meet the requirements in paragraphs **7.2** and **7.3**

8Data 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 current data protection legislation 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 data protection principles 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 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: Ensure that you have written data-sharing agreements in place 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.

9Special 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. Current data protection legislation does not affect the requirement for nationality information to be provided, however, 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 Data protection legislation 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 In accordance with legislation, 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. Current data protection legislation **requires** 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), you are **not** required to conduct 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. 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 Data protection legislation 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 data protection rules. 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: Keep any DPIAs you have in place under review to 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 our guidance for EROs on Running electoral registration.

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. Subject to a few conditions, these must 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, however, you must 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 have historically charged electors for a letter confirming their residency, known as a "certificate of registration".

12.7 Under current data protection legislation 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 canvass 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 current data protection legislation, fines of up to £17.4million 8.7or 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 £8.7million (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 canvass communications, 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		

#	Action	Y/N	Comment
	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		
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	Review your 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 current 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		

#	Action	Y/N	Comment
	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 – 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 4 – 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'	