Using contractors and suppliers | Electoral Commission Data protection guidance for Electoral Registration Officers and Returning Officers You are in the Data protection guidance for Electoral Registration Officers and Returning Officers section Home Data protection guidance for Electoral Registration Officers and Returning Officers View the navigation tree Go to main guidance section: Data protection guidance for Electoral Registration Officers and Returning Officers Registering as a data controller Lawful basis for processing personal data Special categories of personal data Data protection impact assessments (DPIAs) Privacy notices - the right to be informed Inspecting council records as ERO Document retention Data storage Using contractors and suppliers Requirement for a written contract with a processor Data sharing agreements with external organisations Subject access requests Data protection breaches and sanctions Resources for Electoral Registration Officers and Returning Officers - Data protection Using contractors and suppliers As a data controller, you may use a processor to act on your behalf to process data. For example, you are using a processor 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. Last updated: 22 February 2023 Book traversal links for Using contractors and suppliers Data storage Requirement for a written contract with a processor

Lawful basis for processing personal data | Electoral Commission
Data protection guidance for Electoral Registration Officers and Returning Officers
You are in the Data protection guidance for Electoral Registration Officers and Returning Officers section Home Data protection guidance for Electoral Registration Officers and Returning Officers View the navigation tree Go to main guidance section: Data protection guidance for Electoral Registration Officers and Returning Officers Registering as a data controller Lawful basis for processing personal data Processing personal data for the performance of a public task Processing personal data and the edited register Right to object to the processing of personal data Right to be forgotten Special categories of personal data Data protection impact assessments (DPIAs) Privacy notices - the right to be informed Inspecting council records as ERO Document retention Data storage Using contractors and suppliers Data sharing agreements with external organisations Subject access requests Data protection breaches and sanctions Resources for Electoral Registration Officers and Returning Officers - Data protection Lawful basis for processing personal data For the processing of personal data to be lawful, it must be processed on a ‘lawful basis’. 1 This includes: 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 . Processing personal data without a lawful basis runs the risk of enforcement activity, including substantial fines, issued by the ICO, for further information see our guidance on data protection breaches and sanctions. The ICO have advised that in the main, the processing of personal data by EROs and 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. 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. We have provided examples of lawful processing based on processing to perform a public task vested in you by UK law. You should undertake an audit of all the personal data that you collect to determine the lawful basis on which you are collecting/processing it. 1. Article 6 General Data Protection Regulation 2018 ■ Back to content at footnote 1
Last updated: 22 February 2023 Book traversal links for Lawful basis for processing personal data Accountability and transparency of data controllers Processing personal data for the performance of a public task

Data storage | Electoral Commission Data protection guidance for Electoral Registration Officers and Returning Officers You are in the Data protection guidance for Electoral Registration Officers and Returning Officers section Home Data protection guidance for Electoral Registration Officers and Returning Officers View the navigation tree Go to main guidance section: Data protection guidance for Electoral Registration Officers and Returning Officers Registering as a data controller Lawful basis for processing personal data Special categories of personal data Data protection impact assessments (DPIAs) Privacy notices - the right to be informed Inspecting council records as ERO Document retention Data storage Using contractors and suppliers Data sharing agreements with external organisations Subject access requests Data protection breaches and sanctions Resources for Electoral Registration Officers and Returning Officers - Data protection Data storage As data controller, you have a duty to protect against unauthorised or unlawful processing and against accidental loss and are required to have appropriate technical and organisational measures in place to ensure a level of security, appropriate to the risk. 1 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. Your council will have corporate standards and processes for data handling and security. Your Data Protection Officer will be able to advise you on the processes you use as part of carrying out your specific duties as RO and/or ERO. They will also 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. You should ensure that you have processes in place to retrieve data and securely destroy it at the appropriate time, in accordance with your document retention policy. 1. Article 32 General Data Protection Regulation 2018 ■ Back to content at footnote 1 Last updated: 22 February 2023 Book traversal links for Data storage Retention of election notices published on your website Using contractors and suppliers

Data protection breaches and sanctions | Electoral Commission

Data protection guidance for Electoral Registration Officers and Returning Officers

You are in the Data protection guidance for Electoral Registration Officers and Returning Officers section Home Data protection guidance for Electoral Registration Officers and Returning Officers View the navigation tree Go to main guidance section: Data protection guidance for Electoral Registration Officers and Returning Officers Registering as a data controller Lawful basis for processing personal data Special categories of personal data Data protection impact assessments (DPIAs) Privacy notices - the right to be informed Inspecting council records as ERO Document retention Data storage Using contractors and suppliers Data sharing agreements with external organisations Subject access requests Data protection breaches and sanctions Personal data breaches Requirement to notify when a personal data breach has occurred Sanctions and penalties for data breaches Resources for Electoral Registration Officers and Returning Officers - Data protection Data protection breaches and sanctions You should 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 and postal votes. Last updated: 22 February 2023 Book traversal links for Data protection breaches and sanctions Access requests relating to crime prevention Personal data breaches

Inspecting council records as ERO | Electoral Commission Data protection guidance for Electoral Registration Officers and Returning Officers You are in the Data protection guidance for Electoral Registration Officers and Returning Officers section Home Data protection guidance for Electoral Registration Officers and Returning Officers View the navigation tree Go to main guidance section: Data protection guidance for Electoral Registration Officers and Returning Officers Registering as a data controller Lawful basis for processing personal data Special categories of personal data Data protection impact assessments (DPIAs) Privacy notices - the right to be informed Inspecting council records as ERO Document retention Data storage Using contractors and suppliers Data sharing agreements with external organisations Subject access requests Data protection breaches and sanctions Resources for Electoral Registration Officers and Returning Officers - Data protection Inspecting council records as ERO As ERO, you will need to demonstrate that all information obtained 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. Maintaining records will help you to demonstrate that you are complying with your obligations under data protection and electoral legislation. 1 You should keep a record 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. 2 For example, your obligation as ERO to inspect records you are permitted to inspect as part of your duty to maintain the electoral register measures to ensure appropriate security are in place to protect the data, for example: encrypting or password protecting data whenever it is transmitted using secure storage the 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 You should ensure you maintain records of the council records you inspect, and should have the maintenance of records as a clear part of your overall registration plan. Further guidance on inspecting council records 3 is contained in our guidance for EROs . 1. Regulation 35 and 35A Representation of the People (England and Wales) Regulations 2001 (RPR (E&W) 2001); Regulation 35 and 35A Representation of the People (Scotland) Regulations 2001 (RPR (S) 2001) ■ Back to content at footnote 1 2. Section 9A of the Representation of the People Act 1983 (RPA 1983) provides the statutory basis by which you process personal data obtained through council records ■ Back to content at footnote 2 3. Regulation 35 and 35A RPR (E&W) 2001; Regulation 35 and 35A RPR (S) 2001 ■ Back to content at footnote 3 Last updated: 20 March 2023 Book traversal links for Inspecting council records as ERO Data protection considerations for the inspection of the electoral register Document retention

Data protection guidance for Electoral Registration Officers and Returning Officers | Electoral Commission Data protection guidance for Electoral Registration Officers and Returning Officers View the navigation tree Go to main guidance section: Data protection guidance for Electoral Registration Officers and Returning Officers Registering as a data controller Lawful basis for processing personal data Special categories of personal data Data protection impact assessments (DPIAs) Privacy notices - the right to be informed Inspecting council records as ERO Document retention Data storage Using contractors and suppliers Data sharing agreements with external organisations Subject access requests Data protection breaches and sanctions Resources for Electoral Registration Officers and Returning Officers - Data protection Data protection guidance for Electoral Registration Officers and Returning Officers The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 apply to the processing of all personal data. 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 this information is processed and the responsibilities of EROs and ROs to keep data subjects informed. You are personally responsible as an Electoral Registration Officer (ERO) and/or Returning Officer (RO) for ensuring that you comply with the requirements of current data protection legislation. This guidance, which includes practical examples where possible, is designed to support you in meeting: your duty to comply with the requirements of current data protection legislation your obligations, as they relate to your electoral administration responsibilities. It was developed in close consultation with colleagues across the electoral community including the Association of s (AEA), Department for Levelling Up, Housing & Communities (DLUHC), 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 legislation on EROs and ROs. 1 Book traversal links for Data protection guidance for Electoral Registration Officers and Returning Officers Registering as a data controller 1. In this resource we use ‘RO’ as a generic term to refer to all types of Returning Officer. ■ Back to content at footnote 1

Privacy notices - the right to be informed | Electoral Commission
Data protection guidance for Electoral Registration Officers and Returning Officers
You are in the Data protection guidance for Electoral Registration Officers and Returning Officers section Home Data protection guidance for Electoral Registration Officers and Returning Officers View the navigation tree Go to main guidance section: Data protection guidance for Electoral Registration Officers and Returning Officers Registering as a data controller Lawful basis for processing personal data Special categories of personal data Data protection impact assessments (DPIAs) Privacy notices - the right to be informed Notifying data subjects about how their personal data is used Data protection considerations for the inspection of the electoral register Inspecting council records as ERO Document retention Data storage Using contractors and suppliers Data sharing agreements with external organisations Subject access requests Data protection breaches and sanctions Resources for Electoral Registration Officers and Returning Officers - Data protection Privacy notices - the right to be informed 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 which is sometimes called a fair processing notice. 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. 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. 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. Due to the differences across ERO and 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. 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 or 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 You must 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. You should ensure your privacy notice is clearly visible on your website and is referenced when communicating with electors and others. We have produced a checklist for what a privacy notice must contain: Checklist for Privacy Notice (DOC) Last updated: 22 February 2023 Book traversal links for Privacy notices - the right to be informed Requirements of a Data Protection Impact Assessment (DPIA) Notifying data subjects about how their personal

data is used

Resources for Electoral Registration Officers and Returning Officers - Data protection | Electoral Commission Data protection guidance for Electoral Registration Officers and Returning Officers You are in the Data protection guidance for Electoral Registration Officers and Returning Officers section Home Data protection guidance for Electoral Registration Officers and Returning Officers View the navigation tree Go to main guidance section: Data protection guidance for Electoral Registration Officers and Returning Officers Registering as a data controller Lawful basis for processing personal data Special categories of personal data Data protection impact assessments (DPIAs) Privacy notices - the right to be informed Inspecting council records as ERO Document retention Data storage Using contractors and suppliers Data sharing agreements with external organisations Subject access requests Data protection breaches and sanctions Resources for Electoral Registration Officers and Returning Officers - Data protection Resources for Electoral Registration Officers and Returning Officers - Data protection Checklist for data sharing agreement (DOC) Checklist for Privacy Notice (DOC) Cover sheet for copies of full register for inspection (DOC) Cover sheet for copies of full register for sale (DOC) Cover sheet for copies of full register supplied free of charge on request (DOC) Example Data Protection Impact Assessment (DPIA) (DOC) Quality Assurance Guidance for ROs (PDF) Sharing good practice: Data sharing agreement – an example data sharing agreement Last updated: 22 February 2023 Book traversal links for Resources for Electoral Registration Officers and Returning Officers - Data protection Sanctions and penalties for data breaches

Document retention | Electoral Commission Data protection guidance for Electoral Registration Officers and Returning Officers You are in the Data protection guidance for Electoral Registration Officers and Returning Officers section Home Data protection guidance for Electoral Registration Officers and Returning Officers View the navigation tree Go to main guidance section: Data protection guidance for Electoral Registration Officers and Returning Officers Registering as a data controller Lawful basis for processing personal data Special categories of personal data Data protection impact assessments (DPIAs) Privacy notices - the right to be informed Inspecting council records as ERO Document retention Document retention policy Retention of election notices published on your website Data storage Using contractors and suppliers Data sharing agreements with external organisations Subject access requests Data protection breaches and sanctions Resources for Electoral Registration Officers and Returning Officers - Data protection Document retention Personal data processed for any purpose must not be kept for longer than is necessary for that purpose. Once the purpose for collecting the data has passed, you need to consider if there is a reason for you to retain that data. Data protection legislation does permit personal data to be stored for longer periods if, subject to the implementation of appropriate safeguards, the data will be processed solely for: archiving purposes in the public interest scientific purposes historical purposes statistical purposes Examples might include old electoral registers held to determine the eligibility of overseas applicants, or election results. You should 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?” Last updated: 22 February 2023 Book traversal links for Document retention Inspecting council records as ERO Document retention policy

Special categories of personal data | Electoral Commission
Data protection guidance for Electoral Registration Officers and Returning Officers
You are in the Data protection guidance for Electoral Registration Officers and Returning Officers section Home Data protection guidance for Electoral Registration Officers and Returning Officers View the navigation tree Go to main guidance section: Data protection guidance for Electoral Registration Officers and Returning Officers Registering as a data controller Lawful basis for processing personal data Special categories of personal data Data protection impact assessments (DPIAs) Privacy notices - the right to be informed Inspecting council records as ERO Document retention Data storage Using contractors and suppliers Data sharing agreements with external organisations Subject access requests Data protection breaches and sanctions Resources for Electoral Registration Officers and Returning Officers - Data protection Special categories of personal data Electoral legislation requires an individual applying to register to vote 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. 1 As ERO you are required to process this nationality data in order to determine which elections the elector is entitled to vote at. 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. 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 information relating to staff appointments Processing special category data 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. For electoral purposes, the appropriate lawful basis for processing special categories of personal data would be that it is necessary for reasons of substantial public interest and with a basis in UK law. For more information on this see our guidance on Lawful basis for processing personal data . To process nationality data you must have in place a policy document which must explain: the procedures for complying with the data protection principles the policies for retention and erasure Your policy document will need to reflect your: local processing procedures policies for the retention of personal data policies for the erasure of personal data This policy document must: be kept until six months after the processing ceases be reviewed and updated at appropriate times be made available to the ICO on request 1. Regulation 26 Representation of the People (England and Wales) Regulations 2001; Regulation 26 Representation of the People (Scotland) Regulations 2001 ■ Back to content at footnote 1 Last updated: 22 February 2023 Book traversal links for Special categories of personal data Right to be forgotten Data protection impact assessments (DPIAs)

Data sharing agreements with external organisations | Electoral Commission
Data protection guidance for Electoral Registration Officers and Returning Officers
You are in the Data protection guidance for Electoral Registration Officers and Returning Officers section Home Data protection guidance for Electoral Registration Officers and Returning Officers View the navigation tree Go to main guidance section: Data protection guidance for Electoral Registration Officers and Returning Officers Registering as a data controller Lawful basis for processing personal data Special categories of personal data Data protection impact assessments (DPIAs) Privacy notices - the right to be informed Inspecting council records as ERO Document retention Data storage Using contractors and suppliers Data sharing agreements with external organisations Data sharing agreements and supply of the electoral register Subject access requests Data protection breaches and sanctions Resources for Electoral Registration Officers and Returning Officers - Data protection Data sharing agreements with external organisations As ERO, you may be obtaining personal data from external partners. For example, you may receive student data from local higher education providers or receive data from care homes regarding their residents. In this situation, the external partner will be a data controller in their own right. It is strongly recommended that you agree a data sharing agreement or protocol with any external partners and have a written agreement when sharing data between data controllers, even though the legislation does not specifically require it. A written agreement or protocol will help both you and the external partner demonstrate that you are acting in accordance with the data protection principles and will help to avoid any liability implications of one party being seen as a controller and the other being seen as a processor. We have produced the following checklist that you can use when developing a data sharing agreement: Checklist for data sharing agreement (DOC) Alternatively, your council may have developed a template agreement that you can use. In any case, you should discuss any data sharing agreement with your council’s Data Protection Officer or Information Officer. Last updated: 22 February 2023 Book traversal links for Data sharing agreements with external organisations Requirement for a written contract with a processor Data sharing agreements and supply of the electoral register

Data protection impact assessments (DPIAs) | Electoral Commission
Data protection guidance for Electoral Registration Officers and Returning Officers
You are in the Data protection guidance for Electoral Registration Officers and Returning Officers section Home Data protection guidance for Electoral Registration Officers and Returning Officers View the navigation tree Go to main guidance section: Data protection guidance for Electoral Registration Officers and Returning Officers Registering as a data controller Lawful basis for processing personal data Special categories of personal data Data protection impact assessments (DPIAs) Requirements of a Data Protection Impact Assessment (DPIA) Privacy notices - the right to be informed Inspecting council records as ERO Document retention Data storage Using contractors and suppliers Data sharing agreements with external organisations Subject access requests Data protection breaches and sanctions Resources for Electoral Registration Officers and Returning Officers - Data protection Data protection impact assessments (DPIAs) Data protection impact assessments ensure that data protection principles are integral to the design of processes by helping to identify, assess and mitigate risks. Data protection legislation requires that a DPIA is undertaken before processing when: you are using new data processing technologies for example, if you introduce a new initiative to issue canvassers with tablets, you need to undertake a DPIA first. the processing is likely to result in a high risk to the rights and freedoms of individuals for example, processing applications for anonymous registration is high risk processing (see our guidance on high risk processing for further information). A DPIA is not required where a processing operation has a lawful basis that regulates the processing and a DPIA has already been undertaken. For example, if your canvassers are already using tablets and processing is underway 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. When you undertake any new process, you should undertake DPIAs as a matter of good practice. This will enable you to demonstrate that data protection is integral to your processes and support the principle of accountability.
We have produced the following template DPIA which is used by the Electoral Commission. Example Data Protection Impact Assessment (DPIA) (DOC) The template 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. DPIAs and anonymous registration applications Applications for anonymous registration contain data relating to anonymous electors’ or applicants’ personal safety. The lawful basis for processing this data is set out in legislation but the processing is high risk due to the nature of the data. You should have a DPIA in place for processing anonymous registration applications, and if you don’t you should undertake one. Last updated: 22 February 2023 Book traversal links for Data protection impact assessments (DPIAs) Special categories of personal data Requirements of a Data Protection Impact Assessment (DPIA)

Registering as a data controller | Electoral Commission Data protection guidance for Electoral Registration Officers and Returning Officers You are in the Data protection guidance for Electoral Registration Officers and Returning Officers section Home Data protection guidance for Electoral Registration Officers and Returning Officers View the navigation tree Go to main guidance section: Data protection guidance for Electoral Registration Officers and Returning Officers Registering as a data controller Accountability and transparency of data controllers Lawful basis for processing personal data Special categories of personal data Data protection impact assessments (DPIAs) Privacy notices - the right to be informed Inspecting council records as ERO Document retention Data storage Using contractors and suppliers Data sharing agreements with external organisations Subject access requests Data protection breaches and sanctions Resources for Electoral Registration Officers and Returning Officers - Data protection Registering as a data controller You have a statutory duty to process certain personal data to maintain the electoral register and/or for the purpose of administering an election. As such, in line with current data protection legislation, you are acting as a data controller. Data controllers are required to register with the Information Commissioner's Office (ICO). 1 Advice from the ICO is that all data controllers will need to ensure that they are registered. This means that you must be registered separately to your council in your capacity as ERO and/or RO. The ICO have advised that if you are both an RO and an ERO one registration can cover both roles, and 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. Registration fee The ICO have provided further guidance relating to the fee to register as a data controller on their website , including examples of how the fee should be calculated. 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 and 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. You should direct any questions in relation to registering as a data controller towards the ICO. 1. Digital Economy Act 2017 ■ Back to content at footnote 1 Last updated: 22 February 2023 Book traversal links for Registering as a data controller Data protection guidance for Electoral Registration Officers and Returning Officers Accountability and transparency of data controllers

Subject access requests | Electoral Commission Data protection guidance for Electoral Registration Officers and Returning Officers You are in the Data protection guidance for Electoral Registration Officers and Returning Officers section Home Data protection guidance for Electoral Registration Officers and Returning Officers View the navigation tree Go to main guidance section: Data protection guidance for Electoral Registration Officers and Returning Officers Registering as a data controller Lawful basis for processing personal data Special categories of personal data Data protection impact assessments (DPIAs) Privacy notices - the right to be informed Inspecting council records as ERO Document retention Data storage Using contractors and suppliers Data sharing agreements with external organisations Subject access requests Access requests relating to crime prevention Data protection breaches and sanctions Resources for Electoral Registration Officers and Returning Officers - Data protection Subject access requests A data subject is entitled to see personal information that is held about them. You must provide information requested by data subjects without delay and in any event within one month (although it can be extended to two months in certain conditions). There is no requirement for the request for a subject access request to be made in writing. You must be satisfied of the requester's identity before fulfilling the request. Subject to a few conditions, these must be provided free of charge. Subsequent copies of subject access requests may be charged for, but the charge must be reasonable and based on administrative costs. Providing Certificates of registration Under 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. Last updated: 22 February 2023 Book traversal links for Subject access requests Data sharing agreements and supply of the electoral register Access requests relating to crime prevention