Data Protection Impact Assessment

ONLINE ABSENT VOTE APPLICATION SERVICE Public Beta

ADOPTED BY LONDON BOROUGH CAMDEN AUGUST 2023

NAME OF PROJECT/ACTIVITY :	**ONLINE ABSENT VOTE APPLICATION SERVICE Public Beta**
DATE:	07/07/2023
NEXT REVIEW DATE:	

What kind of processing and data does this proposal involve?	
Who is the Lead/Manager/Senior Responsible Owner for the policy/ project/initiative?	[redacted]
Who is the Information Asset Owner?	[redacted]

Does the project/policy/initiative involve the use of personal data we currently process, or will this be new data?	Both. Online Absent Voting Applications policy (to be implemented via upcoming secondary legislation) will enable electors to apply for apply for a postal or proxy vote online via a new GOV.UK service, and will also require electors to provide their National Insurance Number (NINO) - or suitable documentary evidence if they cannot provide this – in their application for the purposes of enabling checks on their identity to be carried out. This requirement mirrors what is currently requested for Register to Vote and, as it is done under the Register to Vote service, the Department will process NINOs against DWP records in order to confirm the identity of the elector applying. As all applications are sent to Local Authority Electoral Registration Officers (EROs), EROs will process all other personal data provided by the elector.
What is the controller/processor relationship	**Data Controller:** **Electoral Registration Officers (ERO) [nationally]** **Independent Data Controller: Department for Work and Pensions (providing data to ERO for verification checks)** **Data Processor 1: DLUHC – providing the "ERO Portal" platform to ERO to administrate online absent vote applications** Sub-processors to DLUHC: 1. Amazon Web Services (data hosting and storage) 2. Cabinet Office (Cyber Security monitoring) 3. Softcat (development, support and maintenance provider of DLUHC) 4. Google analytics (for measuring site performance) The purpose of the ERO Portal is for ERO's to provide a service to electors which has been defined by legislation. **This makes the ERO the data controller.**

	The ERO portal is a processing tool, provided by DLUHC, so that EROs can provide the service required by legislation. **This makes DLUHC a data processor.** The purpose of the identity check is to provide evidence to the ERO to support them in determining applications as they are required to in law. The databases used in this processing will only be accessed and searched by DWP and the way that check is conducted has been determined by DWP in compliance with departmental practice. For that specific relationship and process within the service **DWP is an independent data controller.**
If there is a joint controller relationship, provide an explanation of how this was determined and the roles and responsibilities of each controller	n/a
What personal data will be processed as part of the project/ policy/initiative?	<u>Applicants</u> The following personal information is the minimum level of personal data that will be collected as part of an application from an individual citizen: - 1. Applicant's name (Forename, middle name, surname, previous name where provided), 2. Date of Birth, 3. Registered Address, 4. (Registered Address) Postcode 5. Delivery Address (optional) 6. National Insurance number ("NINO") 7. Signature 8. Proxy name 9. Proxy address

	10. Proxy contact details (optional) 11. Required technical data such as IP address, 12. Phone Number (optional) 13. Email address (optional) 14. Cookie / behavioural tracking data In **some** cases where an applicant is unable to provide a NINO the Digital application also offers the elector the ability to upload documentary evidence in order to verify their identity. This will be in document format (PDF, Image file) and could consist of: One of the following **Primary documents** a. applicant's passport b. applicant's identity card issued in the European Economic Area c. applicant's biometric immigration document issued in the United Kingdom in accordance with regulations made under section 5 of the Borders Act 2007 d. applicant's electoral identity card issued in Northern Ireland e. applicant's photocard driving licence granted in the United Kingdom or driving licence granted by a Crown Dependency, which bears a photograph of the applicant. One trusted government document and two s**econdary documents** (below): a. With exception to (f), these must have been issued in the UK or CD a. Birth certificate b. Marriage or civil partnership certificate c. Adoption certificate d. Firearms certificate e. UK-issued Driving licence (not in photocard form)

	f. Driving licence granted other than in UK or CD, which has a photograph and is valid for at least 12 months from the date the applicant entered the UK g. Police bail sheet Or **four** pieces of social or financial history documents a. Financial statement; a. Mortgage statement b. Bank or building society statement or letter confirming account c. Credit card statement d. Pensions statement b. Council tax demand letter or statement c. Utility bill d. P45 or P60 issued by employer/former employer e. Statement of benefits or entitlement to benefits Special category personal data collected is dealt with in the relevant section below. The Digital application will also gather data from Cookies to enable analytic information to be gathered and analysed by Google Analytics. This data will be used to improve the performance of the service. Google Analytics does provide coarse geo-location data by deriving the following metadata from IP addresses: City (and the derived latitude, and longitude of the city), Continent, Country, Region, Subcontinent (and ID-based counterparts). For UK-based traffic, IP-address data is used solely for geo-location data derivation before being immediately discarded. It is not logged, accessible, or used for any additional use cases.

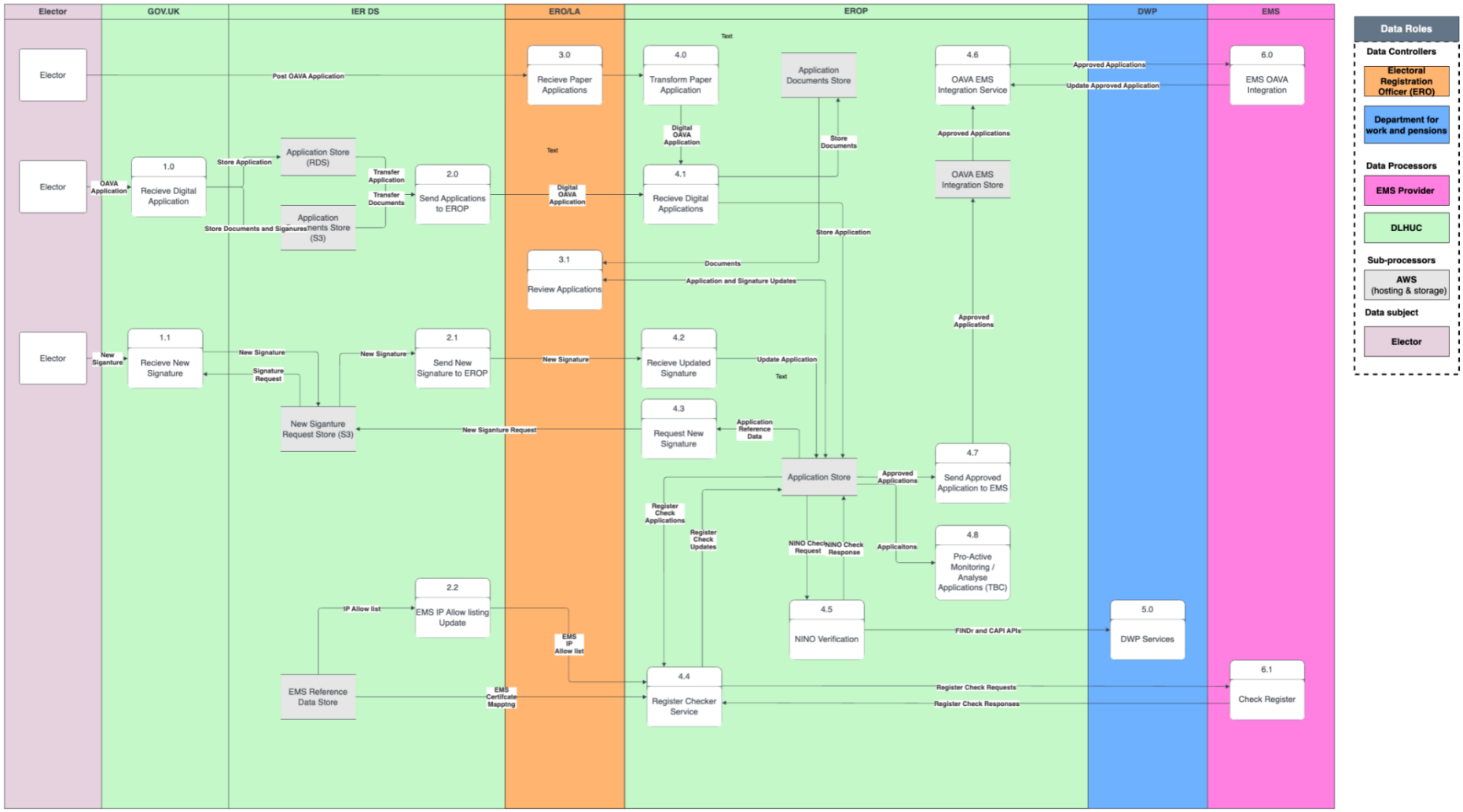
	<u>DLUHC EROP administrators</u>
	
	For accessing the ERO Portal further data is collected to allow access to the portal, this includes: -
	
	1. Name of ERO staff member accessing the portal – so DLUHC can assign them to a role
	2. User credentials (ERO staff member)
	    1. Work email address
	    2. Login
	    3. Password
	    4. Work mobile phone number (for two-factor authentication)
	    5. User ID
	3. Associated user metadata – access monitoring logs.
	4. Users of the Portal can also upload documents sent by the data subject(s) (electors)
	5. Name and address of Electoral Registration Office
	6. There will also be system generated data – dates, times, references for auditability to support processes undertaken on the portal

How many individuals' data will be involved?	We anticipate that between commencement in October 2023 and 2031/2032 over 61 million applicants (>6m per year) will submit new applications for an absent vote.
How much data will you be collecting?	DLUCH will be collecting all the necessary data described above for an application to be processed on behalf of the ERO from the citizen. It is anticipated that most applications will successfully pass the DWP NINO match but, based on current Register to Vote precedents, we estimate that between commencement in October 2023 and 2031/2032 up to 9,901,294 applications (<1m per year) will go down the exceptions and attestations route.

Describe the nature of the processing	The collection and processing of personal data for the purposes of issuing a registered elector a postal or proxy vote is not a new activity. This relationship already exists in law. However, currently that process is only supported in law if conducted through paper correspondence (only in part, as a 'wet signature' is always required). Therefore, the purely electronic submission of applications by the citizen through a digital service is a new service. The collection and processing of an elector's NINO, or documentary evidence where the NINO has not been provided, is also not new as it is already a requirement and process which takes place following the Register to Vote legislation and service. Section 2 and Schedule 2 of the Elections Act 2022 enables the SoS for DLUHC to create the process via regulations for this to happen for absent voting applications too, and the SI enabling this will be laid in Parliament on 7 July **Data source:** Electors will provide the data needed for them to receive an absent vote at the point of application. This data will be collected either digitally online, or via paper applications. DWP (NINO) and ERO ("Full" Electoral Roll) datasets will be used to verify identity of applicants. This is done through a data matching exercise which compares the applicant's first name, last name, DoB and NINO with that held by the DWP. Data is passed and a 'MATCH', 'NO MATCH or 'TOO MANY MATCHES' is returned. If a match found a subsequent call to pull the full NINO from DWP is made. An exact match comparison is made against the application data and all DWP data is erased immediately in line with the DWP Code of Connection. The DWP CoCo states that EROP will not store any data retrieved. **Controller and Processors:** The ERO will be the data controller, with DLUHC processing on their behalf. Other processors/sub-processors involved include: 1. Amazon Web Services (data hosting and storage) 2. Cabinet Office (Cyber Security monitoring) 3. Softcat (development, support and maintenance provider of DLUHC)

	4. Google analytics (for measuring site performance) **Paper application storage:** All paper applications and supporting evidence is sent direct to the ERO by the data subject for them to handle and enter the secure Portal for processing. The Controller will retain all paper forms and evidence on their own premises but should be managed in line with local data storage policies/uploaded into the EROP. **Digital application storage:** All digital applications originating from DLUHC OAVA website is first stored on a front-end secure SQL database data in encrypted format located in AWS' UK data centre, and will be pulled down into the portal by a secure API interface into AWS Aurora database. The "S3 bucket" (data store) is used for applicant documents and photos. **Data access:** All access is via the secured portal using secure login to authorised users who have completed an Access Use Policy and understand how to control and protect that data. **Data sharing:** There is no additional data sharing outside of the process described. **Deletion:** Once an application has been determined, application data will be stored in the EROP for a maximum of 12 months in line with current legislation (section176 of the RPA 1983), unless a criminal investigation is launched because of suspected electoral fraud where this period could be extended by a court. Outside of the EROP, in the ERO's chosen EMS, legal requirements mean that personal identifiers necessary for confirming the validity of the ballot must be retained for the duration of the elector's arrangement. This will be a maximum of 3 years for postal votes, and 5 years for proxy votes.

OAVA Data Flow



Requirement		Comments
Data Protection Impact Assessment **UK - GDPR Article.35**	**Data Protection Impact Assessment (DPIA):** • Has a DPIA screening process for the proposal/project/system been completed? • If yes – please attach the DPIA screen form.	Pre-screening was not undertaken as we concluded that a full DPIA was required
The Principles **UK-GDPR Article.5** • **Lawful** • **Purpose** • **Data minimisation** • **Accurate** • **Storage limitation** • **Integrity and confidentiality (security)** • **Accountability**	**Lawful:** • What is the legal basis for processing the data? • Does this require the data to be processed, or simply allow it?	The lawful basis for the processing of data via the EROP - Article 6 (1) (e) - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller ("Public Task") The public task is the new digital service which will support electors to vote by helping them apply for an absent vote whilst proving their identity, and by providing local authorities with the relevant information to process their vote. Article 6(1)(c) provides a lawful basis for processing where: "processing is necessary for compliance with a legal obligation to which the controller is subject." ("Legal obligation") It will in fact be necessary to process this data to ensure that identity checking takes place and that eligible electors can receive an absent vote, and thus cast their vote in elections.

		The vires for the processing of personal data is found in Clause 2 Schedule 2 of the Elections Act 2022 and in the Representation of the People (Postal and Proxy Voting) Regulations 2023. <u>Processing of Special Category Data</u> The special category processing condition is: Article 9(2) (g) 'necessary for reasons of substantial public interest' (provided in law) based on UK GDPR and Data Protecting domestic law which asks that the data shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. The processing of this data is also necessary for statutory or government purposes under Sch 1, Part 2, Paragraph 6 of the Data Protection Act 2018 to ensure that the data subject can successfully vote in elections by successfully applying for an absent vote.
	Purpose: • What is the business use/purpose for processing the data?	Section 2 and Schedule 2 of the Elections Act 2022 provide powers for the development of regulations enabling the creation of an online digital service through which applications for an absent vote can be submitted by the citizen. The same provisions also introduce powers to enable the introduction of an identity checking process for absent vote applicants, which will apply to paper applications as well as to applications made online. The purpose for processing the data is to ensure that eligible electors will be able to vote when the new requirements and the new online system are in place. We therefore must enable EROs to adequately meet new legal obligations towards citizens, and DLUHC's Online Absent Vote Service

		will be critical to the successful implementation of the new changes for both the ERO and the citizen. The benefit to the ERO is to assure themselves that that they will be able to meet their legal obligations. Introducing identity checks to absent vote applications is an important anti-fraud measure to strengthen the integrity of absent voting, as well as public confidence in the results of elections. The requirement intends to prevent personation fraud and ghost applications, and therefore reassure electors and administrators that the electoral system is secure. Collecting, using, and storing the personal data for confirming an elector's identity as well as processing and determining their application is an essential step in supporting this aim, whilst still granting electors their vote
	Data minimisation: • Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose. What assessment has been made to ensure the personal data is adequate, relevant and limited to what is necessary in relation to the purpose?	The conduct of elections across the UK is a no-fail event and legislation makes provision for identification checks for voters to ensure their integrity. The digital application and the Portal functionality has been developed with capture and processing of the mandatory data elements that would be required upon commencement to: 1. enable an elector to vote by allowing them to be provided with a specific absent vote arrangement (this may vary between postal and proxy journeys) and 2. enable the ERO to communicate with the elector via email / phone if required. All the data gathered by the system (summarised at p.5-6) is being collected and processed to enable eligible electors to vote in elections

		through the successful identity verification and processing of their applications. The provision of this data is legally required by legislation. No additional data is captured based on EC guidelines for any other purpose besides granting an eligible elector a vote. Additionally, none of the personal data collected is new data that an elector would not have expected to provide when applying to participating in the voting process. In fact, NINOs and suitable documentary evidence are already presently provided by electors under Register to Vote. The same purpose applies to special category data - only Personally identifying information data required to validate the elector's identity and application, will be reviewed from any 'criminal' artefacts like the bail decision record. All data collected will only be used and stored for electoral purposes – the digital journey and portal will not communicate nor integrate with systems that are outside of the electoral processing landscape. Elector will be required to provide documentation from a specified list based on the type of elector they are.
	Accurate: • How will the accuracy of the data be checked? • How will inaccurate data be corrected? • How will it be kept up to date? • What processes will be in place to manage requests for rectification?	The ERO will check the data entered / submitted and there is also validation on aspects of the elector's registration status and NINO that is automated. The data held by DWP is live and updated via several sources, primarily data from HMRC and the DWP maintains that this is typically accurate. Data shared separately between DLUHC and DWP for the purposes of the identity check is not a part of any form of DWP database maintenance or accuracy. If a service user believes there is an inaccuracy

		in the data held by DWP for the purposes of this match this must only be addressed through the DWP NINO advice line. If a match is not found DLUHC have a mitigation in place for services users to provide alternative documentary evidence to the relevant ERO in order to satisfy the confirmation of their identity for the purposes of using this service. The ERO will retain discretion on correcting source data in the application before determination and this will be supported through EROP functionality.
	Storage Limitation: • How long will the data be kept? • Is the data covered by an existing retention and deletion schedule? • If not, will one be agreed with the Departmental Records Officer? • Will you be able to delete the data when you no longer need it? If you can't delete it, can you anonymise it partly or wholly? What processes will be in place to ensure the data is securely destroyed/deleted?	Once an application has been determined, application data will be stored in the EROP in an archive for a maximum of 12 months in line with current legislation (section 176 of the RPA 1983), unless a criminal investigation is launched because of suspected electoral fraud where this period could be extended by a court. Outside of the EROP, in the ERO's chosen EMS, legal requirements mean that personal identifiers necessary for confirming the validity of the ballot must be retained for the duration of the elector's arrangement. This will be a maximum of 3 years for postal votes, and 5 years for proxy votes. Once an application has been determined, there will be digitally supported data retention processes including a secure archive function and reminders to delete data within set timeframes.

	Secure: • How will the data be secured and kept safe?	Digital applications will be collected and held securely in an encrypted SQL database called IER DS until such time it is pulled down into the '**ERO Portal'** The '**ERO Portal'** is hosted on AWS and requires user credentials with 2 factor authentication to be accessed. Authority staff will need to sign an Access Use Policy before they are given access to the Portal to review the data that belongs to them. The environment on which the Portal is hosted has undergone an external IT security health check to validate it is secure to required standards.
	Accountability How will demonstrate responsibility for what you do with personal data? • What measures and records are in place or will be put in place to demonstrate your compliance?	ICO consultation on the operation of the legal powers for data sharing will be completed ahead of the law being enacted. Data Sharing Agreements will make clear the responsibilities with regards to data. There will be a data protection guide from the EC to EROs. Applicants will be given the opportunity to view the privacy notice via a link at the foot of the digital journey to which we will be held accountable.
Transparent **UK-GDPR Article.12, 13 & 14**	**Transparent / Duty to Inform:** • How will data subjects (e.g., customers, staff) be made aware of what is happening to their data? • Do individuals have an opportunity and/or right to	Applicants for an absent vote as the data subjects will be made aware of what is happening to their data, including data sharing with Data Processors at the point of application. This will be done via the presentation of the privacy notice.

	decline to disclose or share their information?	
Subject Access **UK- GDPR Article.15**	**Subject Access Requests:** • Will the personal data be extracted and provided to the data subject through usual business processes? • If not how will subject access requests be managed?	DLUHC expectation is that all SARs and other rights requests will be referred to the ERO as the Data Controller. The ERO would be able to easily confirm personal data held relating to an individual using their application reference numbers and the information recorded on the ERO Portal. Where support may be required or the ERO may struggle to fulfil an SAR, the normal channel of DLUHC's IER service desk would be open and Elections Digital Operations could point them in the right direction to find where the data is.
Data Transfers **UK-GDPR Article.44 and 45**	**Data Transfers:** • Will the data be held or transferred outside the UK? • If yes – where will it be held or transferred to? • Will the data be held or transferred inside the EEA? • Will the data be held or transferred outside the EEA? • If yes - where will it be held or transferred to? • If yes, what processes will be place to ensure it is adequately protected?	No data will be transferred outside the UK
Lawfulness	**Lawfulness:**	The lawful basis for the processing of data via the EROP - Article 6 (1) (e) - processing is necessary for the performance of a task carried out in

UK-GDPR Article.6	Which of the following conditions will apply to how the data is used? • Consent (which is clear, informed and feely given)? • Contract (which stipulates the data processing is required)? • Legal obligation (Act of Parliament, SI)? • Vital (health) Interests (of data subject or another)? • Public Task - Fundamental to the performance of a government function?	the public interest or in the exercise of official authority vested in the controller ("Public Task") The public task is the new digital service which will support electors to vote by helping them apply for an absent vote whilst proving their identity, and by providing local authorities with the relevant information to process their vote. Article 6(1)(c) provides a lawful basis for processing where: "processing is necessary for compliance with a legal obligation to which the controller is subject." ("Legal obligation") It will in fact be necessary to process this data to ensure that identity checking takes place and that eligible electors can receive an absent vote, and thus cast their vote in elections. The vires for the processing of personal data is found in Clause 2 Schedule 2 of the Elections Act 2022 and in the Representation of the People (Postal and Proxy Voting) Regulations 2023.
Consent **UK-GDPR Article.7**	**Consent:** • If you will be relying on consent, will it be given by a confirmation or action by the individual? How will this be recorded? • Will plain language be used? • What processes will be in place to manage withdrawal of consent?	n/a
Special Categories of Personal Data	**Special Categories:**	Yes. Limited special category data may be processed, though this would be indirectly.

UK-GDPR Article.9	• Will any of the data that will be processed include information about individuals': race, ethnicity, health, religion, sex life/orientation, political views, Trade Union membership, genetic or biometric data? • Which of the following options will be applied to that processing? a. Explicit Consent? b. Necessary in compliance with legal obligation? c. Vital (health) Interests? d. By a legitimate, not-for profit body with a political, philosophical, religious or trade union aim? e. Data which has manifestly been made public by the data subject? f. Establishing / defending a legal claim or Courts acting in a judicial capacity? g. Substantial public interest? h. Preventative occupational medicine, or occupational health? i. Public interest in the public health (serious)? j. Archiving in the public interest or for historical/scientific research?	Special category data could be inferred from the data processed for identity checking – for example the accepted identity evidence includes marriage certificates (could infer sexual orientation), benefits forms (could indicate health/disability), and biometric immigration documents (could infer ethnicity). While the acceptance of documents will mean that special category data around sexual preferences, disability, and a person's ethnic origin may being processed, the sole purpose of the processing of this data is identity checking. No other processing is intended. Special category data around a person's disability may also be collected as part of the signature waiver process. Here, the purpose of the processing is enabling the person to vote by ensuring that they do not submit a signature that they then cannot reproduce. Criminal convictions or offences data may also be handled. For instance, applicants may choose to submit a police bail sheet in order to confirm their identity. Similarly to the above, this is the only intended use for processing of the data- thus it would not DPA Part 3 (Law enforcement) processing. In all of the above cases the following lawful basis will be applied to that processing: Article 9(2) (g) 'necessary for reasons of substantial public interest' UK GDPR, based on domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. The processing of this data is also necessary for statutory or government purposes under Sch 1, Part 2, Paragraph 6 of the Data

		Protection Act 2018 to ensure that the data subject can successfully vote in elections by successfully applying for an absent vote. The vires for the processing of personal data is found in the Representation of the People (Postal and Proxy Voting) Regulations 2023.
Criminal Convictions & Offences **UK-GDPR Article.10**	**Criminal Convictions:** • Will the information include personal data about offences/convictions? • If yes, what information will be processed? why is this needed? • Do you have a legal reason to process it and use it?	Criminal convictions or offences data may also be handled. For instance, applicants may choose to submit a police bail sheet in order to confirm their identity. Similarly to the above, this is the only intended use for processing of the data- thus it would not DPA Part 3 (Law enforcement) processing. In such cases the following lawful basis will be applied to that processing: Article 9(2) (g) 'necessary for reasons of substantial public interest' UK GDPR, based on domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject; It will in fact be necessary to process this data to ensure that eligible electors can receive an absent vote, and thus cast their vote in elections. The vires for the processing of personal data is found in the Representation of the People (Postal and Proxy Voting) Regulations 2023.
Right to Erasure **UK-GDPR Article.17**	**Erasure:** • What processes will be in place to manage requests for erasure?	Deleting of personal data within the EROP will be the responsibility of individual EROs.

		Responsibility for the management of the Electoral register and deletion processes lays with the ERO is managed within their EMSs.
Right to Restriction **UK-GDPR Article.18**	**Restriction:** • What processes will be in place to manage requests to restrict processing?	The data will only be processed in the manner described and there will not be a process to restrict that as this is the purpose for which it was collected
Data Portability* **UK-GDPR Article.20**	**Portability:** • Will the data be extractable in a machine-readable format? • What processes will be in place to manage requests to port the data? *NB: This will not apply to most government (legislation based) processing.	n/a
Automated Decision Making **UK-GDPR Article.22**	**Automated Decision Making:** • Will the processing involve automated decision making affecting a person? • If yes, please explain the circumstances. • What processes will be in place to manage objections to automated decision-making?	The ERO will reject or approve an application in its entirety. There will be no decision without human involvement.
Joint Controllers & Processors **UK- GDPR Articles.26 to 30**	**Data Sharing / Contracts:**	The Controller will have appropriate agreements signed and in place with its Data Processors or others:

	• Will the data be shared with other business units/teams/parts of the Department/ Organisation? • If yes how will the data be shared/disclosed? • Will the personal data be shared with an external organisation? • OGD? • Supplier? • Third party? • What kind of arrangement will be in place to covers this? • Contract? • Data Sharing Agreement? • Memorandum of Understanding? • Other? • How will the data be shared/disclosed with the other organisations?	1. DLUHC to DWP – Independent Controller to Controller Memorandum of Understanding (as between two public bodies) 2. ERO to DLUHC – Controller to Processor Memorandum of Understanding (as between two public bodies) 3. DLUHC to sub-processors –contracts between: a. Amazon Web Services (data hosting and storage) b. Cabinet Office (Cyber Security monitoring) c. Softcat (development, support and maintenance provider DLUHC for EROP)
Security **UK-GDPR Article.32**	**Security:** • Will the data be encrypted? • Will the data be pseudonymised? If so how? • How will the data be protected against risk of loss, confidentiality, availability and integrity? • Will back-ups be taken?	All digital applications originating from the online absent vote application service citizen-facing website are first stored on a secure SQL database in encrypted format and will be pulled down into the portal by a secure API interface into AWS Aurora database. All data held in databases are backed up on a regular basis and can be recovered from backups if required Consultation by the data processor with **Cabinet Office Digital and Cyber security teams** and DLUHC Digital and cybersecurity teams informally and via Architecture working Group meetings have provided

	• Will the security of the system/premises be trialled regularly? • Will the security of the system be required to have any formal accreditation or independent certification (e.g. ISO27001)? • What processes will be in place to determine who will have access to the data/system? • What level of security clearance will be required to access the system/data? • What data protection/security training will users of the data/system be required to have? • How will access to the system be granted? • What information asset register and/or risk register will the data be recorded on?	assurance on the solution design, security and integrity as the build has progressed. The delivery teams from **Valtech and Softwire** are experienced in the technology being used (AWS) and how to build a service with security controls in place. This has been demonstrated by the external IT Health Check undertaken by CyberFort. Both the Cabinet Office Cybersecurity team and DLUHC Cyber security team have been involved in the project from an early stage and through the Architecture Working Group meetings and TDA forums they have provided consultation and assurance on the solution being built. The DLUHC cybersecurity team arranged and managed the external ITHC and will continue to do so until the service goes live. ITHCs are completed annually thereafter. Security monitoring – alert monitoring, protective monitoring is provided by Cabinet Office cybersecurity team for the service Access to system data is managed through AWS access controls and only SC cleared approved staff will be provided access to it. The data is recorded on the Information Asset Registers of each Local Authority (around 360). **Cyber Assurance Statement** All Systems and Suppliers involved in the Electoral Integrity Programme have been subject to the DLUHC Cyber Security Assurance Framework. This includes the Voter Authority Certificate Service, OAVA and OE

		websites and the ERO Portal (AWS hosted), Softcat, Softwire, Valtech, HH Global (VAC only), Integrity and A1. The DLUHC Cyber Security Assurance processes include various tools and techniques ranging from Threat Modelling, Supplier Questionnaires, System Defence in Depth reviews for control review and Information Technology Health Checks (ITHC). The specific tools and techniques for each system and supplier are tailored depending on the risk profile, however all aligned with industry best practice, NCSC Guidance and HMG publications such as Government Functional Standard GovS 007: Security. For further clarity, DLUHC Cyber Security have confirmed that all suppliers have been reviewed in relation to their governance structures and frameworks to determine their suitability to design and develop DLUHC systems and/or store, process and manage DLUHC data. Further to this, the control reviews in relation to the citizen facing application services, middle tier and ERO Portal include a defence in depth methodology across the Data, Application, Infrastructure and Network tiers. Control categories across these tiers include a full holistic approach to assessment, including but not limited to: encryption of data at rest, encryption of data in transit, backups, patching and vulnerability management, secure configuration, authentication and authorisation, secure administration architecture, anti-malware, separation of networks and environments, secure boundary services and logging and monitoring.

Other privacy legislation and policies -		Comments
Privacy & Electronic Communications Regulations 2003	**Technology** Does the project/policy/initiative involve new or inherently privacy-invasive electronic communications technologies? For the avoidance of any doubt, 'communication' means any information exchanged or conveyed between finite parties by means of a public electronic communications service, but does not include information conveyed as part of a programme service, except to the extent that such information can be related to the identifiable subscriber or user receiving the information.	No
	Communication providers Does the project/policy/initiative involve new or existing communication providers? For the avoidance of doubt, 'communication providers' means a person or organisation that provides an electronic communications network or an electronic communications service.[1]	No
	Communication subscribers / users Does the project/policy/initiative involve new or existing communication subscribers / users? For the avoidance of doubt, 'communication subscriber' means a person who is a party to a contract with a provider of public electronic communication services for the supply of such services. 'User' means an individual using a public electronic communications service.	No

Human Rights Act 1998	**Article 2: Right to Life** Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to life, subject to any limitations as may be defined in Article 2(2)? For the avoidance of any doubt, the limited circumstances are that in peacetime, a public authority may not cause death unless the death results from force used as follows: • Self defence or defence of another person from unlawful violence; • Arresting of someone or the prevention of escape from lawful detention; and A lawful act to quell a riot or insurrection	N/A
	Article 3: Prohibition of Torture Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to be not subjected to torture or inhuman or degrading treatment? For the avoidance of doubt, this is an absolute right.	N/A
	Article 4: Prohibition of Slavery or Forced Labour Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to be not held in servitude or forced to perform compulsory labour? For the avoidance of doubt, this is an absolute right; the following are excluded from being defined as forced or compulsory labour: • Work done in ordinary course of a prison or community sentence; • Military service; Community service in a public emergency; and normal civic obligations.	N/A

Article 5: Right to Liberty and Security Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to be not deprived of their liberty subject to certain limitations? For the avoidance of doubt, the following limitations apply when a person is: • Held in lawful detention after conviction by a competent court; • Lawfully arrested or detained for non-compliance with a lawful court order or the fulfilment of any lawful obligation; • Lawfully arrested or detained to effect the appearance of the person before a competent legal authority; • Lawfully detained to prevent the spreading of infectious diseases; • Lawfully detained for personal safety (applies to persons of unsound mind, drug addicts etc.); and Lawfully detained to prevent unlawful entry into the country or lawful deportation from the country.	N/A
Article 6: Right to a Fair Trial Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to have a public hearing within a reasonable time by an independent and impartial tribunal established by law? For the avoidance of doubt, the hearings included are both civil and criminal proceedings that are not specifically classified as hearings that must be heard 'in camera', i.e. closed to the public	N/A
Article 7: Right to no Punishment without Law Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to not be prosecuted for a crime that was not, at the alleged time of commission, constitute a criminal offence under national or international law? For the avoidance of doubt, this is an absolute right	N/A

Article 8: Right to Respect for Private and Family Life Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to respect for privacy in terms of their private and family life subject to certain qualifications? For the avoidance of doubt, the qualifications are: • Legal compliance; • National security; • Public safety; • National economy; • Prevention of crime and disorder; • Protection of public health and morals; Protection of rights and freedom of others.	N/A
Article 9: Right to Freedom of Thought, Conscience & Religion Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to freedom of thought, conscience and religion subject to certain qualifications? For the avoidance of doubt, the qualifications are: • Unless prescribed by law; • In interest of public safety; • Protection of public order, rights or morals; Protection of rights and freedoms of others.	N/A

Article 10: Right to Free Expression Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to hold opinions and express their views singly or in dialogue subject to certain qualifications? For the avoidance of doubt, the qualifications are as set out in Article 9 above.	N/A
Article 11: Right to Freedom of Assembly & Association Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to freedom of peaceful assembly and association with others subject to certain qualifications/ For the avoidance of doubt, the qualifications are as set out in Article 9 above.	N/A
Article 12: Right to Marry Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to marry and found a family subject to certain restrictions? For the avoidance of doubt, the restrictions are regulated by law so long as they do not effectively take away the right, e.g. age restrictions apply	N/A

Article 14: Right to Freedom from Discrimination Does the project/policy/initiative involve new or existing data processing that adversely impacts an individual's right to be treated in a manner that does not discriminate the individual from others subject to certain restrictions? For the avoidance of doubt, this right is restricted to the conventions as set out in the European Convention of Human Rights 1950; the grounds for discrimination can be based on: • Sex • Race • Colour • Language • Religion • Political persuasion • Nationality or social origin • Birth • Other status.	N/A
Articles: 16 / 17 / 18 Not relevant for the purpose of this questionnaire	

Regulation of Investigatory Powers Act (RIPA) 2000	Does the project/policy/initiative involve new or inherently privacy invasive electronic technologies to intercept communications? (For the avoidance of doubt, 'communications' is defined in RIPA Part V, section 81(1)). Does the project/policy/initiative involve new or inherently privacy invasive electronic technologies pertaining to the acquisition and disclosure of data relating to communications? Does the project/policy/initiative involve new or inherently privacy invasive electronic technologies pertaining to the carrying out of surveillance? Does the project/policy/initiative involve new or inherently privacy invasive electronic technologies pertaining to the provision of the means by which electronic data protected by encryption or passwords may be decrypted or accessed? Does the project/policy/initiative undertake any of the functions of the Security Service, the Secret Intelligence Service or the Government Communications Headquarters?	N/A

RISK ASSESSMENT

Risk Event, Cause & Impact	Risk Owner	Inherent Rating	Proximity	Mitigation	Target Rating	Risk has been recorded
(e.g. there is a risk that x, caused by y, will have the effect of z)	*(the individual accountable for the risk)*	*(assessment of risk with no mitigation or control in place. Use matrix in appendix 2)*	*(when do you expect the risk to occur?)*	*(actions to be taken to treat the risk)*	*(the rating to which the risk should be reduced if mitigations are actioned)*	*(Yes/No)*
There is a risk that the creation of the new digital services (citizen facing and administrator sides) opens up a potential new route for cyber attack which would result in the loss/release of significant amounts of personal data.	DLUHC	10	ongoing	DLUHC cyber risk assessment / IT health checks completed and passed. A Private Beta will be completed on the service before it goes live, and the service will have passed a CDDO service assessment. Vendor due diligence completed via the DLUHC assured supplier process. Data Sharing Agreements will be in place with Local Authorities. We have existing protections in place through our cloud hosting provider AWS which will be expanded to cover the new OAVA service. This includes advanced DDoS protection through AWS Advanced Shield and threat monitoring through GuardDuty, alongside a dedicated Technical Account Manager (TAM) for rapid response. Live	4	yes

				SOC cyber monitoring, alerting and response is in place and is being expanded to cover the OAVA service.		
There is a risk with the involvement of sub processors to maintain and continue to develop the new front/back end system that personal data could be accessed and individual's data is misused.	DLUHC	4	ongoing	All contracted suppliers to DLUHC are subject to an in-depth assurance process (details contained in assurance statement.) All contracted staff go through extensive security clearance at SC level, which includes a comprehensive background check. All activity on personal data within the EROP including technical work/maintenance is auditable. System access can be traced, and any suspicious activity flagged. Technical development work carried out requiring system level access has an audit trail, whilst access is actively monitored by continuous event-based alerts and COD cyber SOC analysts. Staff accessing the system are required to report their access to the Cabinet Office Digital (cyber security) and DLUHC staff team every time they connect to a database.	2	yes

Data subject is unclear on purposes of data processing and inadequate transparency leads to missing or incomplete data being given limiting successful outcomes/access to service.	DLUHC	4	ongoing	User testing of journeys will maximise user understanding of the purpose of the data processing. Users will have the ability to contact their local ERO to clarify issues of data purposes. They can also provide feedback to the digital service team via the front-end journey. A privacy statement will be accessible at all points throughout the user journey in the foot of the website.	1	yes
In processing data within the identity checking element, there is a risk that inaccurate data compromises subject's ability to successfully apply (Identity checking tool).	DLUHC/ DWP	3	ongoing	Data sources used in processing include DWP data and ERO's own electoral roll data both are kept up to date routinely and are as accurate as possible. If data subject believes the UKG held data is inaccurate there is a NINO call centre to which they can be referred. This would not interfere with their ability to continue with journey and data subject will be able to avail themselves of the exceptions process. EROs can re-run an identity check in the EROP with a different NINO if the data held	1	yes

				on the EROP is confirmed to be inaccurate by an applicant. Identity can be manually checked by requesting further documentation.		
There is a failure of some aspect of the Online Absent Vote Application service infrastructure after launch/during live running preventing EROs accessing applications.	DLUHC	4	ongoing	The service will be able to handle large volumes of applications and has been through significant load testing and ITHCs. Our hosting provider, AWS, has a range of mitigations including the ability to rapidly scale up infrastructure if required. An enhanced support period is put in place during the election period particularly around deadline days in order to identify and resolve any issues with the operation of the service as quickly as possible, minimising disruption. This is accompanied by a 'change freeze' where development work is paused for the lead up to the election period and for the elections themselves. The enhanced support includes an increase to our digital processing to handle increased application volumes and loads on the systems. Our technical support resource is increased to enable rapid responses as set out in the service's incident management playbook.	1	yes

				In the event an outage was to occur, electors needing an absent vote will be able to apply for a bespoke emergency proxy arrangement and still manage to vote.		
There is a risk that in event of unauthorised access on ERO side (users and accounts) a lack of clarity/ inadequate procedures could lead to personal data being misused.	ERO	6	ongoing	Unauthorised access to EROP via the ERO is a risk held by the ERO alone. DLUHC has in place an Acceptable Use Policy for the ERO Portal which is renewed annually and signed by the ERO. The ERO nominates individuals to receive admin privileges for their ERO Portal account. EROs acknowledge that access should only be given to permitted staff, and who require access to fulfil their role. DLUHC will provide any necessary technical support where necessary via the IER service desk, where an ERO identifies an issue/breach with individual accounts or access.	2	yes
Inadequate data retention policies and functionality lead to personal excessive retention of personal data, or the data subject's right to deletion compromised.	DLUHC and EROs	3	ongoing	Electoral law is clear on data retention requirements (it provides that application data must be retained for 12 months and then deleted unless subject to criminal investigation). Data stored in the main ERO Portal database will be retained for 28 working	1	yes

				days, at which point it will be automatically moved to an archive. After 12 months, EROs will be prompted to delete the data from the archive, which will be accessed via the ERO Portal.		
There is a risk 'data controllers are not given sufficient assurance and/or details of processing from data processor, for example not setting out the ways in which data is transferred, stored, or accessed. This could lead to confusion as to responsibilities which could lead to an unintended data protection breach.	ERO and DLUHC	8	ongoing	An MOU will be signed between individual EROs and DLUHC with clear obligations and details of the processor controller relationship and DLUHC will provide explanatory companion to support understanding from the outset. DLUHC will also provide a copy of this DPIA and data flows for full transparency of processing and risk management. DLUHC will continue to provide ongoing technical support and can answer queries from individual EROs through Zen desk support.	3	yes