Data Protection Impact Assessment

Overseas Electors – Public Beta / Go Live

PROVIDED BY DLUCH AND ADOPTED BY CAMDEN ELECTORAL REGISTRATION OFFICER (A SEPARATE DATA CONTROLLER TO CAMDEN COUNCIL)

NAME OF PROJECT/ACTIVITY:	**Overseas Electors**
DATE:	Nov 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?	Gordon Woods. Acting Director, Elections Directorate (DLUHC) Jeanette Pegler Electoral Registration Manager Camden
Who is the Information Asset Owner?	Gordon Woods. Acting Director, Elections Directorate (DLUHC) Jeanette Pegler Electoral Registration Manager Camden
What is the controller/processor relationship	**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** • **collecting data from the citizen space form**

	Data Processor 2: Electoral Management System (EMS) provider to the ERO. **Data Processor 3: Signature verification software provider to the ERO** Sub-processors to DLUHC: 1. Amazon Web Services (data hosting and storage) 2. Risual/Node4(Cyber Security monitoring) 3. Softcat (service development and maintenance) a. Softwire (sub-contractor of Softcat who provide development, support and maintenance on behalf of DLUHC) 4. Google analytics 4 (for measuring site performance and how the site was used and navigated) The purpose of the ERO Portal is for EROs 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. There is no obligation on each data controller to use the service provided by DLUHC [i.e. they could source or build an alternative service if it could meet their needs].** 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?	The processes set out here concern Register to Vote applications for Overseas Electors – British citizens who are resident overseas. At the point of application for an overseas elector registration, the following data items will be processed: 1. Applicant's full name, and any previous names. If the previous name is the name they claim they were known by when last registered/resident, they must provide an explanation as to why they are no longer known by that name. 2. Date of Birth (though an applicant can choose not to provide this, in which case they would need to provide an indication of if they were under 18 in England, Wales or Scotland, and if they were over 76 in England or Wales). (The DoB will be used as part of the check against DWP data along with the NINO. If no DoB is provided, the exceptions process would be used.) 3. Applicant's current (overseas) address 4. Applicant's previous address – their last place of registration (and how they were last registered) or, in some cases, residence in the UK 5. National Insurance number ("NINO") or an explanation as to why they could not be able to provide one 6. Nationality [closed questions relating to British citizenship] 7. Passport number, date and place of issue, or alternative statement illustrating how they qualify as a British citizen (e.g. naturalisation certificate) 8. Phone Number (optional) 9. Email address (optional) 10. Cookie / behavioural tracking data where the data subject uses our online service(s) to register 11. Required technical data - IP addresses 12. The applicant's reference. This is autogenerated by the service using the following process: o The first character is a prefix o * "A" - Register to Vote digital submissions o * "P" - Postal Vote digital submissions o * "R" - Proxy Vote digital submissions o * "V" - Voter Card digital submissions (it looks like V is being used for overseas as well at the moment) o the remaining 9 characters are chosen at random from this set "123456789BCDFGHJKLMNPQRSTVWXYZ"

	If an applicant was previously registered under a Declaration of Local Connection (DOLC) – i.e. if they were of no fixed abode – they would be expected to communicate this during the application process.
	
	If applicants are not able to establish their connection to a previous registration or residence, or if their identity cannot be confirmed via automated checks, they may be required to provide further evidence, including documentary evidence. If they cannot provide adequate documentary evidence, they may be required to provide an attestation. This is set out in the nature of processing section.
	
	<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

Does the project/policy/initiative involve the use of personal data we currently process, or will this be new data?	The majority of applicants will previously have been registered to vote, so may have had their data processed as part of a previous application, but this would not have been processed through the ERO Portal, and only their name and registered address would have been retained on the electoral register. The introduction of the ERO Portal for processing OE applications means that new data will be processed

	whenever an overseas applicant registers to vote. Applicants will be required, to provide personal information such as their date of birth (DOB), national insurance number (NINO) and we will request an address at which they can be contacted. OEs are also asked if they hold a British passport and to provide passport number, place and date of issue. Expired passports are also acceptable. Passport details are not checked but EROs do have the power to request further evidence relating to citizenship or nationality. As a result of changes to the registration journey we may also collect, at the point of application, documentary evidence pertaining either to an overseas applicant's identity or their connection to an address in the UK. This would be new data collected as part of the policy and, by virtue of its function, it will most likely be personal data. A high level summary of the changes is below: 1. addition of proof of identity document upload if applicant cannot provide DoB or NINO in existing (previous registration) OE route 2. addition of 'previous residency' route to provide their date they last lived in the UK, that they were over 18 when they last left, provide their last UK address, and upload proof of residency documents 3. addition of 'left the UK under 18' route, which is a subset of 'previous residency' route. Optional provision of parent/guardian details to prove residency through their parent/guardian Applicants would be required to provide this whenever they register to vote, either for the first time as an Overseas Elector, or if they were previously an Overseas Elector but let their registration lapse.
How many individuals' data will be involved?	Registrations per year can fluctuate for overseas electors, largely because they can only register to vote in respect of certain elections and because of the (current) requirement for them to re- register annually. At the 2019 Election, overseas electors registrations in England and Wales peaked at 192,482 registrations. In December 2021 there were 98,351 overseas elector registrations in England and Wales representing a decrease of 44% since December 2020.

	Changes which will be implemented following the passing of the Elections Act 2022 will move registration periods from 1 to 3 years and will remove the 15 year limit. We estimate that at a maximum in 2024/25 there could be up to 3,251,000 registrations. However, our modelling estimates that there will be 527,000 new registrations in 2024/25, as not all those enfranchised will actually register. Accordingly, we estimate there will be 612,000 total registered OEs in 2024/25 (including existing registrations carried over from the previous FY). We assume that 8.75% of applicants (Source: IERDS) will fail the DWP NINo check, corresponding to 49,000 applicants in 2024/25. However, there will also be applicants who will require the exceptions process for address verification. We estimate that 84,000 applicants in total will require the exceptions process (request documentary evidence) for identity and/or address verification in 2024/25.
How much data will you be collecting?	We will be collecting all the necessary data described above for an application to be processed on behalf of the ERO from the citizen. We anticipate that most applications will successfully pass the DWP NINO match but, based on current Register to Vote precedents, we assume that 8.75% of applicants will fail the DWP NINo check, corresponding to 49,000 applicants in 2024/25. However, there will also be applicants who will require the exceptions process for address verification. We estimate that 84,000 applicants in total will require the exceptions process (request documentary evidence) for identity and/or address verification in 2024/25. Any individuals who are applying to register as an OE will be asked if they hold a British passport (expired or current) and to provide passport number, place and date of issue. This will not be checked against government records as standard.

	If the applicant requires the exceptions process due to not having a NINo or the match not succeeding, they will typically be asked to provide 1-4 pieces of identifying information, as set out above
Describe the nature of the processing	'Overseas electors' have been eligible to vote in some form as part of UK General elections since 1985. UKG collecting and processing the application data on behalf of EROs is therefore not new and we have an existing legal responsibility for the IERDS. However, some of our legal changes to the Overseas Electors registration journey have implications around personal data in the form of collection, use, processing, and retention. If an applicant was previous registered under a Declaration of Local Connection (DOLC), the applicant must provide an explanation as to which category of DOLC applied when they were last registered. These categories are set out in Representation of the People Act 1983 Section 7B, and include: - A person who would not be entitled to be registered by virtue of residence at any place other than a mental hospital at which they were a patient - A person who was not resident at any address (for example, if they were homeless) - A person who was permanently resident on a houseboat. Applications in respect of a DOLC can only be made offline, but will still be processed via the ERO Portal. OEs can also register as an anonymous elector. Anonymous applications are available to electors whose safety would be at risk if their name or address were listed on the electoral register. These applications can also only be made offline, and would require an applicant to complete a standard OE application plus an anonymous registration application. Anonymous applications must additionally contain the reason for

	anonymous application and evidence to support that application, which could be a court document or an attestation from a qualifying officer, such as a police officer. If an applicant is unable to provide a NiNo to enable an identity check, they will be processed through a new 'exceptions' route and will be asked to provide documentary evidence pertaining to their identity. For overseas electors the list of acceptable evidence is as follows. **List 1: Primary ID Documents** • applicant's passport • applicant's identity card issued in the European Economic Area • applicant's biometric immigration document issued in the United Kingdom in accordance with regulations made under section 5 of the Borders Act 2007 • applicant's electoral identity card issued in Northern Ireland • 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. **List 2: Trusted Government Documents** *With the exception of Non-UK/Crown Dependencies issued driving licences, these must be issued in the UK or Crown Dependencies* • Birth certificate • Marriage or civil partnership certificate • Adoption certificate • Firearms certificate • UK-issued Driving licence (not in photocard form) • Driving licence granted other than in UK or Crown Dependencies, which has a photograph and is valid for at least 12 months from the date the applicant entered the UK

	• Police bail sheet **<u>List 3: Financial and Social History Documents</u>** *For Overseas Applicants, these must be issued in the UK or its Crown Dependencies.* • A financial statement, including, but not limited to: i. Mortgage statement ii. Bank or Building Society statement iii. Bank or Building Society account opening confirmation letter iv. Credit card statement v. Pension or endowment statement • Council Tax statement • Utility Bill • P45 or P60 • Benefit statement EROs will be able to accept: a. Any one document from List 1; b. One document from List 2 and two additional documents from either List 2 or List 3; or c. Four documents from List 3. If the applicant is registering under the previous residence condition, then they will be asked to provide documentary evidence connecting them to that address, either at the point of application or at the request of the administrator. There is a prescribed list permissible evidence for address verification,

	though EROs will have discretion to accept other evidence as long as it contains the applicant's name and the address they are applying in respect of: • letter from His Majesty's Revenue and Customs • council tax demand letter or statement • rent book issued local authority • statement of benefits or entitlement to benefits • letter from DWP confirming entitlement to state pension • letter from a school, college, university or other educational institution confirming attendance or offer of a place • letter from Student Loans Company • official copy of land register entry or other proof of title • solicitor's letter confirming purchase of, or confirmation of, land registry registration • P45, P60, reference or payslip issued by employer • bank or building society passbook or statement, or letter from bank or building society confirming opening of account • credit card statement • utility or mobile telephone bill • letter from insurance provider Documentary evidence from the list above can be accepted as copies of the originals which can be submitted electronically or by post, or the originals can be posted to and returned by the ERO. If an applicant stated that they were known by a different name when they were last resident and their documentary evidence showed that previous name, EROs may request evidence relating to a name change. The Digital application will also gather data from Cookies to enable analytic information to be gathered and analysed by Google Analytics 4. 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 both UK and non-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 for GA, our application and security logs capture client IPs and store them for up to 14 days. This info is only used where necessary for system security or maintenance and is not routinely accessed. We use Google Analytics to measure how you use the service, so we can improve it based on user needs. Google stores anonymised information about: • how you got to the service • the service pages you visit, and how long you spend on each • what you click on while you use the service Google does not share or use this data Applicants are asked if they consent to cookies however there are 'strictly necessary' cookies which remember application form progress, and are always on. The following link, https://registertovote.service.gov.uk/cookies, offers a comprehensive list of cookies, distinguishing between those that are optional and essential. There is a non-optional cookie which we store to record responses for a limited period to recall application progress. The business team utilises this information to gain insights into how the service is utilised, aiding in the prioritization of future updates. It's important to note that the data collected does not directly impact individual user's journey. **Address Verification** If the applicant is registering under the previous residence condition, or if a register check was not successful, there are a number of address verification processes an ERO can use to connect an applicant

	to their qualifying address. Primarily, this will be done via another DWP check, checking the applicant's previous UK address against DWP records to confirm a match. If no match is found through historic register checks, or if there are any concerns about the accuracy of DWP data, the applicant will be asked to provide documentary evidence connecting them to that address, either at the point of application or at the request of the administrator. There is a prescribed list permissible evidence for address verification, though EROs will have discretion to accept other evidence as long as it contains the applicant's name and the address they are applying in respect of: • letter from His Majesty's Revenue and Customs • council tax demand letter or statement • rent book issued local authority • statement of benefits or entitlement to benefits • letter from DWP confirming entitlement to state pension • letter from a school, college, university or other educational institution confirming attendance or offer of a place • letter from Student Loans Company • official copy of land register entry or other proof of title • solicitor's letter confirming purchase of, or confirmation of, land registry registration • P45, P60, reference or payslip issued by employer • bank or building society passbook or statement, or letter from bank or building society confirming opening of account • credit card statement • utility or mobile telephone bill • letter from insurance provider

	Documentary evidence from the list above can be accepted as copies of the originals which can be submitted electronically or by post, or the originals can be posted to and returned by the ERO. If an applicant stated that they were known by a different name when they were last resident and their documentary evidence showed that previous name, EROs may request evidence relating to a name change. Should no satisfactory documentary evidence be provided, EROs could check the application against locally held data, such as council tax information. If all other routes are unsuccessful, an applicant can provide an address attestation, in which another registered elector can provide details of that individual's previous address. **<u>Attestations</u>** Attestations can be used for both identity and address verification. They are an existing process currently in use in electoral registration, but they are being introduced as a process for address verification for the first time. Attestations will require the attestor to provide personal information to verify the validity of the attestation. The identity attestation will: • Confirm that the applicant is the person named in the application; • [If the attestor is an overseas elector] include the attestor's British passport number together with its date and place of issue • [If the attestor is a domestic elector or service voter registered in GB] include the attestor's electoral number

	• [If the attestor is a domestic elector or service voter registered in NI, where electoral numbers are not used] include the applicant's Digital Registration Number (DRN) • Include the date on which it is made; • Include the qualifying attestor's full name, date of birth, occupation, residential address and (if different) the address in respect of which the qualified attestor is registered as an elector • Include an explanation as to the qualifying attestor's ability to confirm that the applicant is the person named in the application, including (but not limited to) the qualifying attestor's connection to the applicant and the length of time that that connection has existed • Include confirmation that the attestor is aware of the criminal penalty for providing false information to a registration officer. • Include a declaration by the qualifying attestor that all the information provided in the attestation is true • Be signed and in writing The process for address attestations is similar, with some small changes. All address attestations will: • [If the attestor is an overseas elector] include the attestor's British passport number together with its date and place of issue • [If the attestor is a domestic elector or service voter registered in GB] include the attestor's electoral number • [If the attestor is a domestic elector or service voter registered in NI, where electoral numbers are not used] include the applicant's Digital Registration Number (DRN) • Include the date on which it is made • Include the qualifying attestor's full name, date of birth, occupation, residential address and (if different) the address in respect of which the qualified attestor is registered as an elector • Include an explanation as to the attestor's ability to confirm that the applicant met the relevant requirement (in most cases, that the applicant was resident at their qualifying address), including

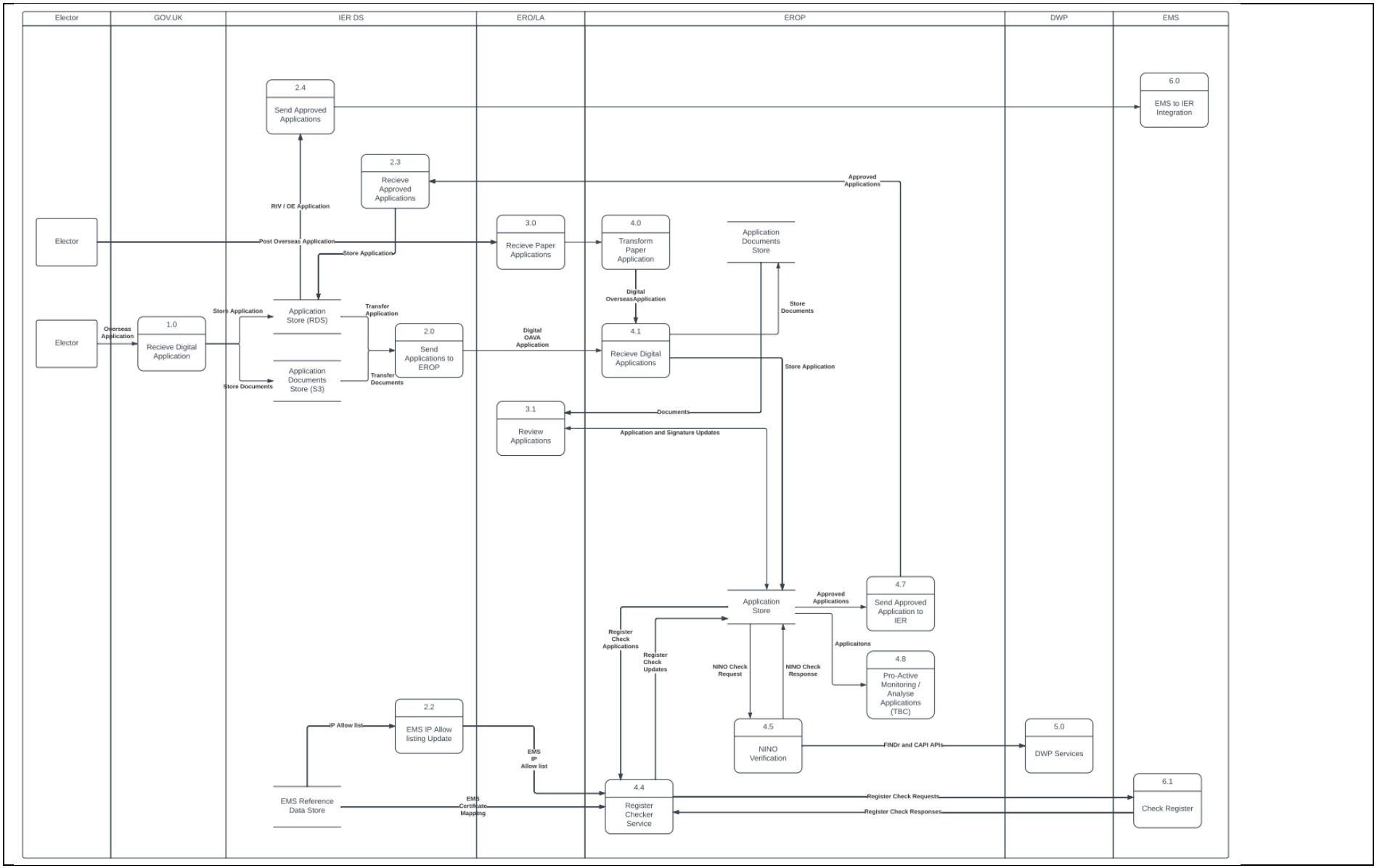
	(but not limited to) the attestor's connection to the applicant and the length of time that that connection has existed • Include confirmation that the attestor is aware of the criminal penalty for providing false information to a registration officer. • Include a declaration by the qualifying attestor that all the information provided in the attestation is true • Be signed and in writing **<u>Renewals</u>** OEs will be entitled to remain on the register for up to 3 years. If they wish to remain on the register past that point, they will be required to submit a renewal declaration. The renewal declaration is a lighter-touch version of the declaration they submit when they first register to vote, so will mostly be confirming details currently held by the ERO. However, they will be permitted to change correspondence details through the renewal declaration, including correspondence address, email address, and telephone number. The list of personal information required at renewal is: • Their full name and date of birth; • A statement to confirm the declarant is a British citizen; • A statement to confirm they are not resident in the United Kingdom on the date of the declaration; • Their registered address; • Their current (overseas) address; At the point of commencement, this will not be an online process. The SI permits an online renewal journey to be developed in future, however. Future digital development of an online renewal journey will include measures to mitigate against risk of fraud.

	<u>Application Reference</u> When an application is submitted, a reference is autogenerated by the service. It is stored in the ERO Portal along with all the other application data that is sent from IERDS. It is retained only as long as the other application data is. This is shown on the page to the applicant after submitting an application online, and is also sent to the applicant's email once the application is created in the ERO Portal. Its only purpose is for communication to/from the ERO during the process of determining an application (and potentially for a short while post-determination e.g. during the objections period). It is not used when applying to vote or to vote. **Data source:** 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. Alternatively, an applicant can submit a paper application form to the ERO, this will then be manually entered into the EROP. Other methods will continue to available to the applicant including the ability to apply by phone or in person however any application information collected by the ERO will need to be manually entered into the EROP to be processed. The EROP will perform an automated historic register check. When an applicant enters their previous address, this function will search for a match to historic addresses drawn from OS Places.

	Controller and Processors: The ERO will be the data controller, with DLUHC and the EMS provider processing on their behalf. DWP will be data controller for the data processed as part of the NINO check. Other processors/sub-processors involved include: 1. Amazon Web Services (data hosting and storage) 2. Risual (Cyber Security monitoring) 3. Softcat (service development and maintenance) a. Softwire (subcontractor of Softcat) 4. Google analytics (for measuring site performance) **Paper application storage:** Applications which utilise the exceptions route we will provide a facility to store the full applications, including the documentary evidence uploaded, in the EROP. **Digital application storage:** All digital applications originating from DLUHC '**Get ready to Vote service'** 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. Once the application and any associated documents have been considered, EROs will make a determination on that application and the outcome and information relating to that application needed for that electors record will automatically flow through to the ERO's EMS, where information will be stored. **Data access:** DLUHC has responsibility for the technical management of the EROP but does not have day to day access to applications, unless dealing with a technical fault/issue/bug. In such cases, EROs would

	notify DLUHC of the occurrence and permission is granted for DLUHC and Softwire to rectify the specific issue only. Otherwise, DLUHC would not access any applications. All ERO access is via the EMS platform 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:** EROs will be responsible for compliance with storage and deletion processes under the law. For applications which went down the exceptions route and supplied additional documentation, DLUHC remains a data processor only and does not manage the ongoing storage or deletion of documents. ***[To support EROs in complying with the law – the archive function within the EROP will issue reminders about data where it has been stored for over 12 months, however this can be overridden by the ERO as the data controller who may choose to retain the data for longer].***

Data Flow analysis


Elector
GOV.UK
IER DS
ERO/LA
EROP
DWP
EMS
2.4
Send Approved Applications
6.0
EMS to IER Integration
2.3
Recieve Approved Applications
Approved Applications
RtV / OE Application
Elector
Post Overseas Application
Store Application
3.0
Recieve Paper Applications
4.0
Transform Paper Application
Application Documents Store
Digital OverseasApplication
Store Documents
Elector
Overseas Application
1.0
Recieve Digital Application
Store Application
Application Store (RDS)
Transfer Application
2.0
Send Applications to EROP
Digital OAVA Application
4.1
Recieve Digital Applications
Store Application
Store Documents
Application Documents Store (S3)
Transfer Documents
3.1
Review Applications
Documents
Application and Signature Updates
Application Store
Approved Applications
4.7
Send Approved Application to IER
Register Check Applications
Register Check Updates
Applicaitons
NINO Check Request
NINO Check Response
4.8
Pro-Active Monitoring / Analyse Applications (TBC)
IP Allow list
2.2
EMS IP Allow listing Update
EMS IP Allow list
4.5
NINO Verification
FINDr and CAPI APIs
5.0
DWP Services
EMS Reference Data Store
EMS Certificate Mapping
4.4
Register Checker Service
Register Check Requests
Register Check Responses
6.1
Check Register

1.0 The citizen (elector) can register to vote via the citizen facing front-end (Gov.uk). The application and associated documentation provided by the citizen is stored in IERDS application store and document store (hosted in AWS).

2.0 The relevant application data is transferred to EROP (the Portal).

3.0Alternatively, the citizen may choose to submit a paper application. The citizen would submit their application to their local Electoral Registration Office. Upon the LA (Local Authority) receiving the application, the application would be timestamped.

4.0The application and any supporting documentation would be manually uploaded and stored in EROP, by an administrator. Once application is in EROP, this enables the LA administrator(s) to review and process the application including any documentation that has been provided.

4.4 A register check service would be carried out on an application to identify that it is a valid application i.e. not an application for an individual who is already registered as an Overseas elector. If this is the case, the application would be rejected at determination stage.

5.0 In order to determine the outcome of an application, the administrator would be required to process the identity and qualifying address for that citizen. For example, where a NINO has been provided and the DWP check (NINO verification) returns an exact match, this would complete the identity aspect for the application.

6.0 The outcome determination of an application (acceptance / rejection) and the relearnt data is sent from the EROP to IERDS and then to the LA's EMS.

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 processing personal data is the below: 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 lawful basis for processing cookie data is Article 6(1)(a) - the data subject has given consent to the processing of his or her personal data for one or more specific purposes. Where cookies are necessary, an exemption is applied where consent is not required to provide an online service at someone's request, in accordance with PECR and UK GDPR. The necessary cookies track application progress are auto-deleted when the application is completed. An example of this are cookies that remember what's in an online basket, or to ensure security in online banking. 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.
	Purpose: • What is the business use/purpose for processing the data?	Processing of the data is undertaken on behalf of the EROs who have a legal duty to register overseas electors and maintain the accuracy of the electoral register in their area. New UKG processing, including conducting checks of UKG data for previous residence at an address, are designed to support applicants who may struggle to prove they were registered at an address prior to leaving the UK. By submitting to the check they increase the chances of being successful in their applications. The benefit to the ERO as data controller is reduced administrative burden having to manually request and review physical documentation which could hinder their ability register eligible applicants.
	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 overseas elector to register to vote by demonstrating their connect to their previous registration/residence 2. enable the ERO to communicate with the elector via email / phone if required. All the data gathered by the system (summarised above) is being collected and processed to enable eligible electors to register to vote in elections through the

		successful identity verification and processing of their applications. Accordingly, the only data being processed is data stipulated by the legislation as being necessary and nothing more. This is also the case for necessary cookies which include personal data. Please note that cookies containing this data are deleted once the application journey is complete.
	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 the validation of aspects of the elector's registration status and NINO are 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. If data such as the NiNo is considered inaccurate, for example if the ID check fails, then the ERO will contact the applicant to verify corrections. Alternatively, applications can be rejected prior to corrections to the data being made, this is at the EROs discretion. The approach for correcting data would apply to all data collected and would be managed through the ERO Portal. It is the responsibility of the controller to manage any requests for rectification. Accuracy of passport information: EROs have a power to request additional information related to the applicant's citizenship if they deem it necessary. This could include circumstances where the passport details are clearly not correct. However, EROs will not be expected to routinely check passport information. Accuracy of NiNo :

		If an applicant's identity cannot be checked via the check of their National Insurance Number, EROs will have an expanded range of options available to them. OE applicants will now be able to provide documentary evidence, by providing one or more documents from a prescribed list. If that is not possible, EROs will be able to consult local data sources if they have them available, or request an attestation from a qualified elector.
	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?	*Sub-processors will be required to provide destruction certificates to DLUHC to evidence erasure of personal data from systems containing data for the trial, and which meet UK National Cyber Security Centre (NCSC) media sanitisation guidance.* Once an application has been determined, application data may be held by the EROP as long as necessary, though they must retain the application until it is determined. If they choose to retain the application data longer, they must remove the NINO from the application within 13 months of receipt. It is for EROs to consider whether they have need of application data for longer than the period up until determination. This is in accordance with existing legislation and there are no changes to existing legislation with regards to retention. Outside of the EROP, in the ERO's chosen EMS, data will be held for the extent of the elector's registration – a maximum of three years, unless the elector renews their declaration. Once an application has been determined, data retention processes will be automated.
	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?	Data Sharing Agreements will make clear the responsibilities with regards to data. There will be a data protection guide from the EC to EROs. There will be a review point in diaries to remind processors of deletion points in the future. Applicants will be presented with a privacy notice prior to accessing the service. Once an application has been determined, data retention processes will be automated. All sub-processor relationships will be governed by contracts satisfying UK GDPR article 28.

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 decline to disclose or share their information?	Data subjects will be made aware of what is happening to their data, including data sharing with Data Processors, by way of a Privacy Notice that will be made available to them at time of the application. Applicants can choose not to submit their application at any stage of the digital journey and this is not stored.
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?	Applicants' data will not be shared with any other individual or organisation outside the UK.

Lawfulness **UK-GDPR Article.6**	**Lawfulness:** 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 lawful basis for processing personal data is the below: 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") 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 the Representation of the People (Overseas Electors) Regulations 2023. The lawful basis for processing cookie data is Article 6(1)(a) - the data subject has given consent to the processing of his or her personal data for one or more specific purposes. Where cookies are necessary, an exemption is applied where consent is not required to provide an online service at someone's request, in accordance with PECR and UK GDPR. These cookies are auto-deleted when the application is completed.

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 **UK-GDPR Article.9**	**Special Categories:** • 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)?	The processing of special category data is in fact aimed at ensuring to data subject can successfully vote in elections by successfully registering to vote. EROs already process special category data (SCD) for elections administration purposes. EROs, under this SI, will have the discretionary power to ask for evidence of an individual's nationality. Nationality is not SCD as such under UK data protection law, however DLUHC understands that Electoral Commission policy is to treat it as SCD and it is Home Office policy to treat nationality as SCD, which DLUHC will also follow. The list of permissible documentary evidence for identity verification purposes also includes a police bail sheet, which may reveal details of criminal convictions. No data subject would be required to provide such documentation – there are other options available, especially as we anticipate the majority of applicants holding a passport given their status as British citizens overseas. Furthermore, this is the same as the existing process for domestic electors. If an applicant provided a biometric immigration document as proof of identity under the exceptions process, that document may also reveal protected characteristics, such as previous immigration status, along with

	j) Archiving in the public interest or for historical/scientific research?	biometric data such as photograph and fingerprints. Limited special category data may be processed, though this would be indirectly. 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 verification. No other processing is intended. 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 vires for the processing of personal data is found in the Representation of the People (Overseas Electors etc) Regulations 2023. Additionally, the Substantial Public Interest Condition in Schedule 1 of the DPA 2018 is likely to be:

		6. Statutory and government purposes
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 be necessary to process this data to ensure that eligible electors register successfully. The vires for the processing of personal data is found in the Representation of the People (Overseas Electors etc) Regulations 2023. However, EROs will be responsible for determining the lawful basis for processing and using data under this category. Additionally, the Substantial Public Interest Condition in Schedule 1 of the DPA 2018 is likely to be: 6. Statutory and government purposes

Right to Erasure **UK-GDPR Article.17**	**Erasure:** • What processes will be in place to manage requests for erasure?	Erasure processes are the responsibility of the controller. 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?	Restriction processes are the responsibility of the controller. There is no specific mechanism to restrict processing. The system offers an "on hold" status so an ERO could use that to tag the individuals application - it wouldn't prevent anyone from further processing the data as a technical control but could be used when filtering the list of applications.
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 under Public Task basis
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?	No, there will be no decisions taken without involvement of an electoral administrator.

Joint Controllers & Processors **UK- GDPR Articles.26 to 30**	**Data Sharing / Contracts:** • 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?	The Controller will have appropriate agreements signed and in place with its Data Processors or others: 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. ERO to Electoral Management Systems provider - Controller to Processor DSA DLUHC to sub-processors – Processor contracts
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? • Will the security of the system/premises be trialled regularly?	All digital applications originating from '**Get Ready to Vote service'** 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 **Risual and Cyber security teams** and DLUHC Digital and cybersecurity teams informally and via Architecture working

	• 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?	Group meetings have provided assurance on the solution design, security and integrity as the build has progressed. The delivery teams from **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 Risual 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 Security monitoring – alert monitoring, protective monitoring is provided by Risual 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

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

[1] Source – Communications Act 2003

	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
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. 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 [redacted]	4	yes
There is a risk with the involvement of sub processors to maintain and continue to develop the new front/back	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	2	yes

end system that personal data could be accessed and individual's data is misused.				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, [redacted]		
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	1	yes

				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.		
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 on the EROP is confirmed to be inaccurate by an applicant. Identity can be manually checked by requesting further documentation.	1	yes

There is a failure of some aspect of the Oversees Electors Vote Application service infrastructure after launch/during live running preventing EROs accessing applications.	DLUHC	4 if not during an election period 5 during an election period	ongoing	The service will be able to handle large volumes of applications and has been through significant load testing and ITHCs. [redacted]	1	yes
There is a risk that in event of unauthorised access on ERO	ERO	6	ongoing	Unauthorised access to EROP via the ERO is a risk held by the ERO alone.	2	yes

side (users and accounts) a lack of clarity/ inadequate procedures could lead to personal data being misused.				DLUHC has in place an Acceptable Use Policy for the ERO Portal which is renewed annually and signed by the ERO. [redacted] 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.		
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 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.	1	yes

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
NiNo checks are not adequate for all verification purposes	ERO	No impact as other options available.		If an applicant's identity cannot be checked via the check of their National Insurance Number, EROs will have an expanded range of options available to them. OE applicants will now be able to provide documentary evidence, by providing one or more documents from a prescribed list. If that is not possible, EROs will be able to consult local data sources if they have them available, or request an attestation from a qualified elector.		
Incorrect passport numbers entered	ERO	No impact as EROs can		EROs have a power to request additional information related to the applicant's citizenship if they deem it necessary.		

		request more information.		This could include circumstances where the passport details are clearly not correct. However, EROs will not be expected to routinely check passport information.		
Data subject contact details entered inaccurately	ERO	4		When filling in their online contact details, the applicant is shown a 'check your answers' screen to confirm their responses and change any that are incorrect. The applicant is also asked to share both their email and phone number so if they do then the ERO has multiple ways to contact them.		

Summary of DPO advice if applicable: –

I've reviewed the updated version of this DPIA following my comments on 22/12/2023. I am broadly content with this risk assessment version bar one comment, and two longer-standing risks sitting across all EIP workstreams:
Comment – I'd like to understand further the "back end" of the processing which is new in the public beta and full services stages of Overseas Electors, and how the reference generated is actually used at that stage. My main concerns are around inaccurate processing and voter impersonation.

Inaccurate processing – inability to communicate with the data subject due to e.g. incorrect or obsolete email address, which might affect ability to vote. Mitigations appear to be sound though as long as system design compels the data subject to provide more than one means of communication, a “safety check” is present to ensure the data subject has entered data correctly; and the data subject can subsequently update their contact details via the Portal (with identity assured). If this is the case I am content.
Impersonation – this likely sits outside of the ERO Portal itself, but again what risk exists of someone being able to vote as someone else, after registering? This may or may not include use of the reference generated and I’d like to understand this potential risk better at go live stage.

Longer-term risks

1. Use of NINO data for data subject identity verification – I note the IAO has previously chosen to over-ride DPO advice on this aspect of processing, so I can only reiterate this here with a request for a longer-term plan to provide more assured identity verification
2. Similarly, any use of “AdTech” to market the use or testing of the ERO Portal (if this occurs during public beta and go live phases), for which GDPR compliance cannot be assured – again DPO advice here was previously over-ruled.

DPO advice accepted or overruled by:	[redacted]	If overruled, you must explain your reasons below
Comments:		

Stakeholders/Participants.
What organisations and individuals contributed to this assessment (include their role/function)?

Name	Role	Organisation	Nature of Input
Stephen Mak	DPO	DLUHC	Supporting IG advice on completion of DPIA and IG requirements
[redacted]	Deputy DPO	DLUHC	
[redacted]	Data Protection Compliance lead	DLUHC	Supporting IG advice on completion of DPIA and IG requirements

Sarah Laws, Data Protection Manager and Jeanette Pegler Elections Manager, Camden Council, Camden advice on data protection and elections respectively

APPENDIX 1 – DETERMINING THE RISK LEVEL

Evaluation of likelihood of risk occurring:

Likelihood score	1	2	3	4	5
Description	Very Unlikely	Unlikely	Possible	Likely	Very Likely
Indicative Frequency	Will probably never happen	Not anticipated to happen, but possible	Might happen or recur occasionally	Will probably happen or recur, but not persistently	Almost certain to happen or recur, possibly frequently

Evaluation of impact should risk occur:

Description	Very Low	Low	Medium	High	Very High
Indicative Impact	Unlikely to have any impact	May have an impact	Likely to have an impact	Highly probably it will have a significant impact	Will have a major impact