

getyournec.scot
Data Privacy Impact Assessment

Version 2.0

improvement service

Authors

This document was prepared by:

Strategic Business & Delivery Lead – Digital Public Services Improvement Service	

Version History

Date	Document Version	Document Revision History	Document Author/Reviser
01/06/2020	1 Draft	Initial draft of DPIA for getyournec.scot	Programme Manager
06/07/2020	1 FINAL	Finalised	Programme Manager
20/09/2020	1.1 FINAL	Update 27001 Accreditation	Programme Manager
30/11/2021	2.0 FINAL	Updated for Young Persons Free Bus	SB & D Lead

Approvals

Date	Document Version	Approver Name and Title	Approver Signature
06/07/2020	1 FINAL	Finalised	CHANGE BOARD
30/11/2021	2.0 FINAL	Updated for Young Persons Free Bus	CHANGE BOARD

Contents

getyournec.scot Data Privacy Impact Assessment (DPIA) 5
The Need for a DPIA 5
The Processing 6
What is getyournec.scot used for 6
Context of the Processing 7
Processing Responsibilities 8
Purposes of Processing 9
Scope of the Processing 10
Account Registration 11
Apply for a National Entitlement Card 12
Verifying Identity 13
Manage Your Card 15
Data Sources to Help Prove a User is Who They Claim to be 15
Raising a Query 16
Personal Data generated when a user uses the service 17
Personal Data we collect from your device 18
Data Retention 19
Proportionality and Necessity 20
Legal Bases for Processing 20
Standards Applicable to the Processing 22
Data Minimisation 23
Keeping Data Accurate and up to Date 23
Supporting the Personal Rights of Data Subjects 24
Keeping Data Subjects Informed 24
If Applicable, how is the Consent of Data Subjects Obtained? 24
Rights of Access and Data Portability 24
Rights to Rectification and Deregistration 24
Rights to Restriction and to Object 24
Processor Obligations 24
International Transfers 24
Consultation 25
Risks 26
Confidentiality 26
Integrity 27
Availability 28
Existing and Planned Measures 29

Sign-Off and Record Outcomes 32
Action plan 32
Sign-Off 33
Updates 34
Version 2.0 34
Previous Versions 34
Definitions 35

getyournec.scot Data Privacy Impact Assessment (DPIA)

Effective 14th July 2020. **Download PDF**

This DPIA was prepared in advance of the getyournec.scot going live. If you have any questions about the DPIA, please contact the Improvement Service.

The Need for a DPIA

Getyournec.scot will provide Scottish residents (users) the ability to apply for a National Entitlement Card online. Users will also be able to request updates and replacements.

The National Entitlement Card (NEC) Scheme has two primary purposes:

- To provide and administer a personalised smartcard that may be used to allow efficient and customer-friendly access to various Scottish public sector services;
- To provide a means that an individual may use to assist in confirming who they are when accessing Scottish public sector services both in person and online.

The scope of this DPIA, just covers the processing of data on the getyournec.scot platform. This DPIA should be read in conjunction with the DPIA covering the full NEC Scheme.

A DPIA covering the full National Entitlement Card Scheme is available online.

getyournec.scot provides a broad range of services that are made available to users and service providers, including:

- **An online account –** featuring a growing range of options, including apply for and request updates for a NEC.
- **Identity verification –** a service that enables users to prove who they are during the application process.
- **Helpdesk –** an online helpdesk to help users resolve any queries which they may have.

This DPIA has been created in line with the Information Commissioner's Office (ICO) guidelines. Guidelines can be found at the ICO's website.

A DPIA is necessary as the getyournec.scot service:

- Processes special category data;
- Combines, compares or matches data from multiple sources, to establish that users are who they say there are;
- Processes personal data that could result in a risk of physical harm in the event of a security breach;
- Uses technologies to make online identity proofing easier for users.

Improvement Service policy, (the company who operate getyournec.scot), also dictates that major systems that process personal data will always be subject to a DPIA before implementation or following a significant change.

The use of mygovscot myaccount for authentication and identity verification is mandatory for the getyournec.scot service. A separate DPIA covering the scope of the myaccount service is available online.

The Processing

What is getyournec.scot used for

getyournec.scot allows users to apply for a National Entitlement Card online. Although not all services may be available initially; users will also be able to:

- Update their details;
- Update the photograph on their card;
- Request a replacement for a lost or stolen or damaged card;
- Renew an expiring or expired card.

Users will be able to apply for the following National Entitlement Cards via getyournec.scot:

- Free concessionary travel for people over 60
- Free concessionary travel for people with a disability
- Young Scot Card
- Young Persons' Free Bus Travel (Scottish residents aged 5 – 21 years old)

Users will be required to login to getyournec.scot using the mygovscot myaccount service.

While using getyournec.scot, users will be required to provide information and present documents to verify their identity and eligibility. The requested information is in accordance with the NEC application process, to apply for a NEC, request an update, request a replacement, or request a renewal.

getyournec.scot transfers application information submitted by a user to the NEC CMS (Card Management System), to prompt a card to be printed by the card supplier and sent to a user.

Context of the Processing

All 32 Local Authorities in Scotland use the National Entitlement Card. getyournec.scot is offered as an application route (in addition to other channels) to all Local Authorities; however, it is a decision for each Authority to onboard the service to make it available to its citizens.

The NEC Scheme requires a user to prove who they claim to be before being issued with a NEC. Depending on the card type, the user may also have to provide proof of entitlement to receive a certain card e.g. proof of disability.

Users can currently apply for a NEC in person by attending a validation point (typically Local Authority offices or Post Offices) and present proofs. Not all users however can attend or want to attend an office in person and would prefer to apply for a NEC online. That is where getyournec.scot comes in.

getyournec.scot enables users to apply for a NEC online at a time that is convenient to them. For Local Authorities, they can offer getyournec.scot as a new channel to their citizens to apply for a NEC. By opening the new channel, they can achieve efficiencies and free up staff (who would otherwise be needed to verify and process applications in person) to support other areas of the business or support users who need additional assistance.

getyournec.scot uses tools from the myaccount services to enable users to prove who they are by verifying their details.

The process to validate and verify a user via getyournec.scot meets or exceeds the criteria noted in the NEC Scheme requirements for verifying applications.

This model is in line with Government Standards to verify identities of users accessing online services.

Processing Responsibilities

getyournec.scot services are provided by:

The Improvement Service
A company limited by guarantee and registered in Scotland (Company No. SC287978)

iHub
Quarrywood Court
Livingston
EH54 6AX

You can read more about the Improvement Service and what we do on our website.

Any reference to Data Protection Law we make in this document refers to the EU General Data Protection Regulation ((EU) 2016/679) and the UK Data Protection Act 2018, which came into effect in the UK on 25th May 2018.

Registration

The Improvement Service is the Data Controller for all account registrations.

When a user signs in to getyournec.scot, they will be prompted to consent to share their myaccount data with the service. At that point an account will be created on getyournec.scot for the user. The user will be able to apply for and manage their NEC through the account dashboard

Processing of applications

The Improvement Service is a Data Processer for all types of NEC applications via getyournec.scot.

The Improvement Service acts as a data processer on behalf of the appropriate Local Authorities to gather data, verify the identity of users and process NEC applications.

Local Authorities are the Data Controllers for all application data generated via getyournec.scot.

When a user applies for a NEC or requests an update or renewal, Local Authorities are the data controller of that data including copies of any documents uploaded during the application process.

Local Authorities are Joint Data Controllers for all data related to a cardholder within the NEC CMS.

Other Data Processors

The Improvement Service has contracts with a managed service company (Tata Consultancy Services), a hosting company (brightsolid UK) and an identity provider (Yoti for the purposes of Doc Scan). All companies are Data Processors for the Improvement Service. The contracts with these companies reflect the GDPR obligations of both the Improvement Service and the contractors.

Purposes of Processing

getyournec.scot processes a user's personal data for the following purposes:

- To allow users to register for an account on getyournec.scot.
- To allow users to apply for a NEC.
- To allow users manage their card.
    - request a change of photograph on their NEC.
    - To allow users to update their details.
    - To allow users to report a lost, stolen or damaged card and request a replacement.
    - To allow users to renew a NEC that is expired or due to expire.
- To allow users to verify their identity as part of the application processes. User may have to provide information that can be checked against other sources to prove their identity/eligibility/entitlement.
- To allow parents/guardians to apply on behalf of their child aged 5 – 15 years and provide approval for a free concessionary travel product to be added to their child's card.
- To provide Service Providers with information to decide whether a user should be granted access to a service.
- To enable the myaccount Helpdesk resolve any queries raised by a user.
- To develop and improve the getyournec.scot service.
- To protect both users and the getyournec.scot service from possible fraudulent or malicious use.

Scope of the Processing

In theory, every resident of Scotland could apply for their own NEC. There are currently over 2 million National Entitlement Cardholders.

To apply for a card, all users must supply their name, date of birth and address. A user can also supply their gender and contact details. The user must also supply a verified photograph if they are over the age of 11 years old or if they require access to national concessionary travel.

User must be a minimum of 12 years old to access getyournec.scot to apply for a card WITHOUT free concessionary travel.
User must be a minimum of 16 years old to access getyournec.scot to apply for a card WITH free concessionary travel.
Parent/guardian must apply on behalf of their child aged 5 – 15 years for a card WITH free concessionary travel. Approval for a free concessionary travel product to be added to their child's card is required.

A significant number of cardholders (around 10%) will also submit basic information about their disability to receive a travel concession. Whilst this data is not detailed, it is classified as a special category of personal data. In the event of a security breach special category data could be mis-used to target certain users e.g. by criminals targeting individuals with impaired vision.

Basic personal information is collected from anyone who wants to set up an account. Users can verify their information by providing additional information that can be checked to prove who they claim to be to apply for or manage their NEC. Some information or documents may be checked against trusted identity stores if required. No special categories of data are processed.

Information is collected on getyournec.scot in one of more of the following ways:

- directly from user registering for an account
- directly from user when applying for a NEC
- directly from user verifying identity
- directly from user when managing their card (requesting a change/renewal/replacement)
- from data sources to help prove that someone is who they claim to be
- directly from user when they raise a query
- generated when a user uses the service
- from the devices used to access myaccount

Account Registration

Information Users Consent to Share

When a user signs-in to getyournec.scot for the first time, they will be prompted to consent to share their myaccount data with the getyournec.scot service.

This data is called core myaccount identity data and includes:

- First Name;
- Surname;
- Gender (Male, Female, Prefer Not to Say or Prefer to Self-Describe);
- Address;
- Date of Birth;
- E-mail Address; and
- Level of Assurance.

The user will then be able to apply for a NEC. If they already have a NEC, users will be able to link and manage their NEC; such as update photograph, report lost/stolen/damaged or renew.

Optional Information That May Be Helpful

Myaccount gives users the option to add optional information to their account profile. The information may be helpful to personalise services e.g. call a user by a preferred name or contact a user if there is a problem. Users will be given the option to share this information in addition to the core identity data.

Optional information includes:

- Mobile telephone number;
- Landline telephone number;
- Preferred First Name; and
- Preferred Surname.

Apply for a National Entitlement Card

Users who apply for a NEC are required to provide getyournec.scot certain information. That information is then processed on behalf of their Local Authority.

User applies for a card for themselves

The information which is gathered during the application process includes:

- First name
- Surname
- Date of birth
- Gender (Male, Female, Prefer-Not to Say, Prefer to Self-Describe)
- Postal address
- Contact details
- Photograph (which meets photograph guidelines)

The user is required to verify the above information before they can submit their application.

For some applications, the verified information above is enough to allow the user to be provided with a NEC; e.g. over 60s concessionary travel.

Other types of applications, however, may require additional information/proofs (which may include special category data) to be supplied by the user, and verified, before an application can be submitted. One example is where a user will be required to supply proof of disability to apply for a disabled concessionary travel NEC.

User (parents/guardian) applies for a card on behalf of their child (aged 5 – 15)

The information of the user which is gathered during the application process includes:

- First name
- Surname
- Date of birth
- Gender (Male, Female, Prefer-Not to Say, Prefer to Self-Describe)
- Postal address
- Contact details

The user is required to verify the above information before they can submit their application.

The information of the child (applicant) which is gathered during the application process includes:

- First name
- Surname
- Date of birth
- Postal address (if different from parent)
- Photograph (which meets photograph guidelines if aged 11+)

The user is required to verify the above information before they can submit their application.

Other types of applications, however, may require additional information/proofs (which may include special category data) to be supplied by the user, and verified, before an application can be submitted. One example is where a user will be required to supply proof of disability to apply for a disabled concessionary travel NEC, or proof of parent approval for Young Persons' Free Bus Travel.

Verifying Identity

Users are required to verify their myaccount details as well as submit a verified photograph. getyournec.scot provides users with two options from myaccount's identity verification services, to choose from, to verify their information:

- Yoti app - Verify identify using a smartphone and the Yoti app; or
- Doc Scan - Scan and upload evidence using a device which has a camera (laptop, webcam, smartphone, tablet).

More information about the Yoti app and Doc Scan is available on the Yoti website.

Yoti app

Users who have a verified Yoti account, can use that same account to verify their myaccount data. Yoti users will have already gone through the identity verification process with Yoti. The Yoti process verifies a user:

- Liveness detection to prove the user is a real person;
- Combination of OCR scanning, NFC chip reading and an expert security team to extract data and check document authenticity (document being a passport or driving licence);
- Biometric face match. A hybrid approach uses technology and expert super recognisers to match the scan of the user's face captured during the liveness test to their ID document photo.

Users who select the Yoti app option will be asked to authenticate with getyournec.scot using their Yoti app. They will be prompted to share their verified data, which is checked against the users account data for a match. Users will be required to share their verified Yoti photograph with getyournec.scot; this photograph will be used on their NEC. Before the Yoti photograph is shared, the user will be asked to authenticate again, this time using Yoti's biometric face match functionality, to match the user to the verified photograph.

Users will be prompted to accept terms and conditions of the NEC Scheme before submitting the application.

The application will be reviewed by an authorised getyournec.scot agent. The role of that agent is to confirm whether the verified photograph meets NEC guidelines. If the photograph does, the agent will approve the application. If the photograph does not meet guidelines, the application will be rejected, and the user will be invited to resubmit a new application with new photograph.

Only approved applications are sent to the NEC CMS to produce a NEC. Once the application data has been transferred by secure APIs into the NEC CMS, the card application data, including photograph will be deleted from getyournec.scot after 28 days. Approved Young Scot applications will be held for 2 years for audit purposes, in accordance with PASS Scheme compliance.

Doc Scan

The Doc Scan process enables a user to verify their details without needing to use a separate application. Users who select this route, will be prompted to confirm what identity document they will upload as proof of identity; a passport or a photo driving licence.
User who select the passport option will be required to submit a proof of residence document from the following list, before starting the Doc Scan process.

The Doc Scan process verifies a user by:

- Extract data from scanned documents (passport or photo driving licence);
- Manual and automatic processes to check the authenticity of the document;
- Liveness detection to prove the user is a real person;
- Biometric face match to confirm the ID document belongs to the user.

On completion of the biometric face match process, the user will be asked to upload a photograph which meets the NEC guidelines, to be printed on their NEC.

Users will be prompted to accept terms and conditions of the NEC Scheme before submitting the application.

The application will be reviewed by an authorised getyournec.scot agent. The role of that agent will include two steps:

- Confirm the image taken during the Doc Scan liveness detection process is the same person in the uploaded photograph.
- Confirm whether the uploaded photograph meets NEC guidelines.

If the photograph does, the agent will approve the application. If the photograph does not meet guidelines, the application will be rejected, and the user will be invited to resubmit a new application with new photograph.

Data Transfer to NEC Card Management System (Operated by NECPO)

Only approved applications are sent to the NEC CMS to produce a NEC. Once the application data has been transferred by secure APIs into the NEC CMS, the card application data, including photograph will be deleted from getyournec.scot after 28 days to allow time for the application to be processed and the NEC to be received by the applicant. Approved Young Scot applications will be held for 2 years for audit purposes, in accordance with PASS Scheme compliance.

The Improvement Service transfer the application data under strict instruction from Local Authorities. Photographs along with the application data is transferred via APIs.

Special category data which is transferred:
Disability card type – The Improvement Service will not pass any document used as proof of disability. Only an application type indicator is transferred to NECPO to confirm what type of card needs to be printed e.g. a disabled concessionary travel card rather than an over 60s concessionary travel card or Young Scot card. All identity and entitlement proof documents are encrypted at rest.

Manage Your Card

Current cardholders will be able to sign-in to getyournec.scot and manage their card. Current cardholders will be able to login to the "Your NEC" option and will be asked to link their card.

The user will enter their 16-digit card number. The card number along with the user's myaccount data will be looked-up against the NEC CMS Extract for a match, to confirm the card exists and the user's details are a match to the cardholder details.

Once a card has been linked, the user will have the options to:

- Update their photograph
- Report a lost, stolen and damaged card for a replacement
- Renew an expiring or expired card

Users who select any of these options will be required to verify their identity through the same process as a user who is applying for a NEC. Users will be given the option to verify their identity and apply for the update/replacement/renewal via the Yoti app or the Doc Scan route.
Please read the section above for details of the verify identity process.

Data Sources to Help Prove a User is Who They Claim to be

Update Photograph

Users who request an updated photograph will have their current NEC photograph compared against the requested updated photograph (verified Yoti photograph or uploaded photograph) for fraud prevention purposes by authorised getyournec.scot agents. A user's NEC photograph is stored separately to the users account data. The photograph is retrieved via APIs in real time when a user requests to update their photograph.

Verify a Cardholder via National Entitlement Card CMS Extract

Getyournec.scot through the myaccount service, uses a limited extract from the National Entitlement Card (NEC) system to help verify the user is a genuine card holder. The extract may also be used to confirm a user's eligibility to access a service from a Service Provider.

When myaccount use the extract, The Improvement Service are acting as Data Processors under written instruction of NECPO as the Data Controller. When myaccount checks a user's information against the NEC extract, it must follow rules laid down by NECPO, acting as the Data Controller on behalf of all 32 Scottish Local Authorities.

The NEC extract is a list of everyone who has a National Entitlement Card. The extract contains basic information such as a user's name, address and their card number. The extract does not contain any information about transactions carried out with the card. It contains the following information only:

- Forename;
- Surname;
- Date of Birth;
- Address;
- Applicant ID;
- Gender;
- Local Authority;
- Entitlement Indicator;
- Photograph; and
- NEC Number.

Raising a Query

If a user wants to contact us or report a problem, they can do so via the getyournec.scot Helpdesk. Both registered and unregistered users can contact the Helpdesk. A user must supply a valid email address to enable the Helpdesk to reply to the query. A user can also supply a contact telephone number if they would prefer this.

If a query relates to a user proving their identity, the Helpdesk may ask the user to provide more information to help resolve the query.

Some queries may need to be answered by Service Providers. In these circumstances, the Helpdesk will forward the query to that Service Provider to respond.

Personal Data generated when a user uses the service

The data helps to identify individual users.

When a user signs-in to getyournec.scot, myaccount generates a unique, anonymous identifier for that user. The identifier is called a Secure Visitor Token (SVT) and is sent to getyournec.scot along with the attribute's a user has agreed to share.

The SVT is only shared between a user and getyournec.scot and is only used when a user logs in. It helps getyournec.scot know that the user is the same person that logged in previously.

User can withdraw consent to share their data with getyournec.scot at any time by visiting the myaccount website and remove consent.

Personal Data we collect from your device

The data helps understand how getyournec.scot is used. This helps provide information to keep improving getyournec.scot.

The information collected includes:

- the type of device being used by a user;
- the unique device identifier that the manufacturer embeds into the device (e.g. the IMEI number of a mobile phone);
- a user's operating system and browser versions; and
- the IP address used.

Every device that connects to the internet has an IP address and getyournec.scot uses it to identify the geographic locations people access the service from. getyournec.scot stores this information securely in what are called logfiles on its servers.

The Improvement Service has an interest in understanding how people are using the getyournec.scot service so that the service can keep improving; for example do users prefer to use the Yoti App or the Document Scanner option to verify their identity and how can we improve this part of the process.

Another interest is ensuring that the service is protected from malicious use and protect users from potential identity theft or account compromise.

Data Retention

The table below notes the data retention rules:

Entity	Type	State	Retention Period	Data Deleted
Account	User	Inactivity (not logged in)	450 days then deleted after further 30 days	Account Data, Account History, Support Requests, Authentication Logs,
Account	Agent	Inactivity (not logged in)	45 days	Account Data, Account History, Support Requests, Authentication Logs, Credentials
Account	Agent	Never activated	45 days	Account Data, Account History, Support Requests, Authentication Logs, Credentials
Account	Agent	disabled	450 days	Account Data, Account History, Support Requests, Authentication Logs, Credentials
Application	User	Submitted	28 days after data exported to NECPO/CMS	Application data, application proof documents, application photograph
Special Category Data	User	Submitted	28 days after data exported to NECPO/CMS	Proof of disability
Support Request	getyournec.scot	Closed	450 days then deleted after further 30 days	Support request and audit trail
Support Request	Service Provider	closed	450 days then deleted after further 30 days. Sanitised after 30 days (see Support Request section below)	Support request and audit trail
Authentication Log	Successful	Known user	750 days	All log data
Authentication Log	Unsuccessful	Known user	750 days	All log data
Young Scot Application Audit Data	User	Submitted	2 years	In accordance PASS Scheme

Proportionality and Necessity

Legal Bases for Processing

Data protection law means that we can only use data for certain reasons and where we have a legal basis to do so. Here are the reasons for which we process data:

Creating accounts and asserting the identity of a user

The Improvement Service are funded to supply a digital identity service to users and Service Providers. By maximising myaccount adoption and its identity verification services across Scotland, further demonstrates value for money for the public purse.

Legal basis for this data usage: Legitimate interest

Processing Application Data

The principal legal basis for the processing is that it is necessary for the performance of a task carried out in the public interest and in the exercise of official authority vested in the controller (Article 6(1)(e)), i.e. the Local Authorities. It is carried out in line with the Local Authorities' duty to secure best value, and their power to advance well-being as outlined in Local Government in Scotland Act 2003, ss 1, 2; ibid., pt3.

Legal basis for this data usage: Public Task

Pass additional information to getyournec.scot

Optional information can be passed to getyournec.scot when a user logs-in to myaccount with consent from the user.

Legal basis for this data usage: Consent

Processing of special category data

Application for a disabled concessionary travel National Entitlement Card. Users are requested to submit a document as proof of disability. That document will be one of the following:

- a photograph of a blue badge;
- a letter from the DWP noting the applicant is in receipt of middle or higher rate component of Disability Living Allowance, or receive Attendance Allowance or Personal Independence Payment;
- a letter from the DWP or SSS which may include details about your health;
- a letter from a Health Consultant or GP detailing relevant disability;
- a copy of Certificate of Vision (CVI) Scotland form;
- a letter from DVLA confirming driving licence has been removed for medical grounds;
- a letter from Ministry of Defence or Veterans UK stating the applicant is in receipt of War Pensioner Mobility Supplement;
- a copy of a NCT002a form noting the applicant has a learning disability;
- a copy of a DS1500 report or hospice admittance letter confirming the applicant has a terminal illness.

The full list of up to date accepted proofs can be found on Transport Scotland's website.

Legal basis for this data usage: Public Task

Article 9 condition of processing for this data usage: Explicit Consent (for getyournec.scot only)

Customer Support

Notifying users of any changes to our service, solving issues via our Helpdesk, phone or email including any bug fixing.

Legal basis for this data usage: Legitimate Interest

Improve getyournec.scot
Test features, interact and review feedback, manage landing pages, heat mapping our site, traffic optimisation and data analysis and research, including profiling and the use of machine learning and other techniques over your data and in some cases using third parties to do this.
Legal basis for this data usage: Legitimate Interest

Asserting the identity of a user
Look up Scottish users in the NEC Extract.
Legal basis for this data usage: Legitimate Interest

Where Legitimate Interest has been cited, a Legitimate Interest Assessment is conducted.

Further explanations of legal basis for processing can be found on the Information Commissioners Office's website.

Standards Applicable to the Processing

The Improvement Service follows several standards to operate the getyournec.scot service.

The getyournec.scot services processes application in accordance with the National Entitlement Card Guidelines.

The getyournec.scot service (including myaccount) follows and adheres to industry best practice.

For authentication, SAML network federation standards are used.

An Information Exchange Protocol outlines the agreed technical controls for securing data in transit between the myaccount service and Service Providers.

The Information Exchange Protocol is part of a wider Framework Services Agreement between the Improvement Service and individual Service Providers.

The Improvement Service has internal governance to assesses changes, risk, impact, supportability, privacy and alignment with architecture principles, standards, relevant legislation and Scottish Government policy guidance.

Authentication traffic is signed and encrypted using strong cipher suites and uses SAML protocols. Strong digital certificates against fully qualified domain names are used to encrypt and sign all web services traffic including authentication.

Both the sender and the receiver require signature of encrypted traffic.

Any bulk traffic is transmitted using secure file transfer to named users and whitelisted IP addresses.

Data Minimisation

getyournec.scot is built with data minimisation principles. getyournec.scot only asks a user for the minimum amount of data required. The minimum data required to sign in to getyournec.scot is:

- Name
- Address
- Date of birth
- Gender
- Email Address

Users can add optional data from their myaccount profile and consent to share that data if they choose to do so.

A Secure Visitor Token (SVT) is shared with the data a user consents to share. The SVT is an anonymous unique persistent identifier. The SVT that helps getyournec.scot identify a unique user.

If a user has linked their NEC to manage their card, getyournec.scot will store the card number to avoid the user having to enter it every time they log in.

A user's NEC photograph is stored separately to the users account data. The photograph is retrieved via APIs in real time when a user requests to update their photograph.

Keeping Data Accurate and up to Date

All users can keep their own details up to date via self-service on their myaccount. The details will be updated in getyournec.scot when the user next signs in.

Supporting the Personal Rights of Data Subjects

Keeping Data Subjects Informed

Many documents are made available to users to inform them of their rights and how data is used.

These documents include:
Privacy Notice
Terms and Conditions
DPIA (this document)

These documents are available on the getyournec.scot website.

Any changes to these documents are communicated with users on the getyournec.scot website. Users are prompted to read and accept the changes on screen. Acceptance of changes is logged in audit files. Refusal to accept terms and conditions will result in in the service being withdrawn.

If Applicable, how is the Consent of Data Subjects Obtained?

Consent is captured at service enrolment and recorded in the getyournec.scot database.

Users can withdraw their consent at any time via their myaccount profile. Any withdrawal or consent is logged for an audit trail.

Getyournec.scot is informed of any consent changes so that they may take the appropriate action. Any withdrawal of consent will not affect the data held by the NEC Scheme itself.

Rights of Access and Data Portability

Users can contact the getyournec.scot Helpdesk to request information about their data. Users can also request information in a machine-readable format. Users may be asked to prove who they are before information is provided.

Rights to Rectification and Deregistration

Users can log into their account and change their personal information. This may require users to re-verify their identity.

Users can withdraw their consent at any time via their myaccount profile. At which point getyournec.scot will delete the users account in line with its Data Retention Policy.

Users can contact the getyournec.scot Helpdesk and ask for their data to be updated, amended or account closed. If the request is made by a user who has not logged in, they will be asked to prove who they are.

Rights to Restriction and to Object

Users can raise a complaint with the getyournec.scot Helpdesk if they feel their rights have been breached. Instructions are noted within the Privacy Notice and help section on the website.

Processor Obligations

The Improvement Service has contracts with TCS and Brightsolid. They have explicit GDPR-compliant schedules. Both companies are Data Processors for the Improvement Service.

International Transfers

No data is transferred outside the EEA/European Union

Consultation

This DPIA has been drafted in preparation for getyournec.scot launching. The design, development, testing and deployment of getyournec.scot was carried out in consultation with many stakeholders including:

- Scottish Local Authorities
- Transport Scotland,
- Young Scot,
- National Entitlement Card Programme Office,
- Strathclyde Partnership for Transport,
- Scottish Government, and
- Members of the public (via user testing).

Getyournec.scot is likely to be updated throughout 2022 with new features and functionality to meet customer requirements. Consultations will be carried out for new developments where required. Invitations to participate in future consultations will include the organisations listed above. Further consultation will be carried out with myaccount User Groups and other key stakeholders.

Risks

Confidentiality

Source and nature of potential impact on users	Likelihood	Severity or Harm	Mitigating controls	Overall Risk
Nature of Impact: • Human error, • Misconfiguration. Source: • Internal or • External human sources.	Possible Username and password are used to access most accounts. Accounts could be compromised if there is a data breach on a different site a user uses the same credentials on. Service Providers also carry out a degree of assurance before any transaction is carried out or finalised.	Distress or inconvenience to user. Potential for minor financial loss. Reputation damage to the system and service provider.	• Digital certificates for encryption and client signing, • Logical and physical controls, • Network security, and • Continuous network monitoring. Service Providers carry out additional checks before any transaction is carried out or finalised. We have controls within the data centres to monitor for potential data loss and anomalous behaviour. 2FA has been implemented for Agent access.	Low

Action plan / corrective actions

Two-Factor-Authentication would provide protection against account compromise due to data breaches elsewhere. The myaccount Authenticator App is available for users to voluntarily download.

Emails are sent to users to notify them if their myaccount has been accessed from a new device and at what time to make sure it is them who are accessing their account and not someone who should not be.

Continue to develop network monitoring so that a more active approach to looking for threats can be developed. Alerts need to be real time or near real time.

Integrity

Source and nature of potential impact on users	Likelihood	Severity or Harm	Mitigating controls	Overall Risk
Nature of Impact: • Human error, • Misconfiguration. Source: • Internal or • External human sources.	Possible	Minor inconvenience to one or more users.	Network security, continuous network monitoring including file integrity monitoring. Data at rest is protected by defence in depth infrastructure and a range of technical and procedural controls. Data in transit is encrypted using strong encryption and requires digital signature by both the sender and receiver before transmission. NEC Application data (including special category data) is held for a maximum of 28 days after application is exported to NECPO/CMS. Approved Young Scot applications will be held for 2 years for audit purposes, in accordance with PASS Scheme compliance. All identity and entitlement proof documents are encrypted at rest.	Low

Action plan / corrective actions

Encrypt all data items within the system so that no meaningful access to personal data could be possible without the relevant keys. This would require a significant redesign and requires an impact assessment.

Availability

Source and nature of potential impact on users	Likelihood	Severity or Harm	Mitigating controls	Overall Risk
Nature of Impact: • Data breach, • Ransomware, • DDoS, • Another cyber incident. Source: • Internal or • External human sources, • Non-human sources.	Likely	Minor inconvenience to many users. getyournec.scot is used by many Local Authorities with usage increasing. Lack of service could cause inconvenience to users. Other channels (face to face, telephone) are generally still offered by Service Providers.	• DDoS protection in data centres, • Failover to warm standby site, • Contract/SLA with supplier.	Medium

Action plan / corrective actions

Consider enhancement to DDoS service if cost effective,

Existing and Planned Measures

Accreditation

Getyournec.scot is operated in line with security best practice. The Improvement Service holds ISO27001:2017 certification with the following scope:

'The provision of consultancy and facilitation products and services, and research, data and intelligence to support all Scottish councils to help them manage their own performance and improvement, deliver digital services, enhance the learning and skills of officers and elected members and improve outcomes for communities.'

The certification period runs from 14/09/2020 to 13/09/2023.

You can view the certificate here https://cvs.babcert.com/babcert.asp?c=225737&v=1rosr95c52

You can check the validity of the certificate on the British Assessment Bureau website here https://clients.britishassessment.com/verify.asp (client reference number is 225737)

You can read the Improvement Service ISMS policy on its website at https://www.improvementservice.org.uk/home/iso27001

Encryption

All authentication transactions are signed and encrypted using strong digital certificates and delivered over TLS. Transactions must be signed by valid digital certificates by both sender and receiver. All bulk data transfer uses secure file transfer over TLS with IP whitelisting.

Logical access control

VLANs are used to separate different environments. IP whitelisting and shared metadata in conjunction with digital certificates ensure that partner organisations are trusted.

Strong password controls in password policy.

No generic accounts are permitted so that all actions within the system are traceable to an individual. This is monitored and reported on as part of routine service management.

Use of captcha and failed login account lockout is used to mitigate brute force attacks.

Remote access for support personnel is via VPN and 2FA to named users only.

All privileges and access are reviewed monthly. Any elevation of privileges is monitored and reviewed.

Operating security

Comprehensive System Security Policy covering all elements of operational security. Adopted/signed by all contractors and sub-contractors.

Website security

Real time monitoring from industry-leading specialist products includes both external and internal anomalies. Annual IT Health Check is carried out by an accredited security company. Formal change and release management policies require vulnerability assessment prior to any upgrade or deployment.

Monitoring network activity
GPG13 compliant network monitoring including anomaly detection, malware and virus scanning.

Protecting against non-human sources of risks
Secure resilient UK data centres (primary data centre with warm standby failover to secondary).

Policy
Security policy framework includes a range of procedural controls including extensive system security policy adopted by contractors and sub-contractors.

Managing privacy risks
Fortnightly risk and change boards within Improvement Service look at all risks to the services with clear escalation paths to senior stakeholders. SIRO signs off residual risk.

Integrating privacy protection in projects
Threat modelling as standard in new developments. DPIA screening using ICO guidance. Staff awareness sessions and supporting documentation.

Traceability (logging)
Audit logs are stored and encrypted to prevent tampering. Logs are aggregated into SIEM. Logs are analysed for near real-time threats and longer-term trends analysis.

Clamping down on malicious software
Up to date anti-virus/anti-malware on all connected system machines. Anti-virus/anti-malware scanning on network boundary for all inbound and outbound traffic.

Maintenance
Routine patching policy with machines updates every 6 months or immediately if emergency arises. Industry-leading specialist software used to block any unpatched vulnerabilities through routine application of IDS rules. This gives breathing space to manage patching.

Physical access control
Data Centres are ISO27001 accredited. Strong perimeter controls, mantraps, turnstiles. Visitors escorted on premises, wearing of visible badges is mandatory. Improvement Service premises protected by electronic door entry.

Hardware security
All builds created from golden images, cabinets locked, storage deletion using CESG-approved software accredited up to OFFICIAL. Controls over management ports, firewall rules tested and reviewed regularly by independent security company.

Processing contracts
Contracts include specific instructions on what data to be processed, and how, in line with GDPR et al requirements. Solution design signed off by security architect prior to go live.

Network security
Host based firewalls with deny all by default and specific entries to limit traffic only to what is required between machines. IDS/IPS monitoring. Regular internal scans using industry-leading specialist software. Solution being extended in 2018-19 to include user behaviour analytics.

DDoS Protection

Data Centre provides DDoS protection service that can be switched on if a spike in traffic is detected. Possibility of having DDoS protection switched on permanently under investigation.

Sign-Off and Record Outcomes

Action plan

Promote 2FA for users. Consider turning on 2FA as mandatory for all users. Solution would require all users to have a verified mobile number in myaccount.

Continue to develop network monitoring so that a more active approach to threat hunting can be developed. Alerts need to be real time or near real time.
Expected date of implementation: Ongoing

Encrypt all data items within the system so that no meaningful access to personal data could be possible without the relevant keys. This would require a significant redesign though and an impact assessment
Expected date of implementation: to be assessed 2022.

Sign-Off

Item	Name/date	Notes
Measures approved by:		
Residual risks approved by:	SIRO	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Chief Security Officer	
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		

Updates

Version 2.0

Why did we change the DPIA?

We're improving our DPIA and making them easier for you to understand. These changes reflect an evolving regulatory environment and our ongoing efforts to simplify how we communicate with users.

What are the main changes?

At a glance, here's what this update means for you:

- **Added information related to new concessionary travel scheme (Young Persons Free Bus Travel).**

Previous Versions

We want to be as transparent as possible about the changes we make to our DPIA.
In this archive you can see versions of our DPIA.

Version 1
Version 1.1

Definitions

Authentication
This is the process you go through to sign-in to myaccount.

CAPTCHA
CAPTCHA stands for Completely Automated Public Turing test to tell Computers and Humans Apart. In other words, CAPTCHA determines whether the user is real or a spam robot. CAPTCHAs stretch or manipulate letters and numbers and rely on human ability to determine which symbols they are.

Data
This is information about you that you give us like your name or email address,
or
information we collect while you use our service, like what type of device you are using or browser. Our Privacy Notice explains more about how your information (data) is used.

Federated Identity Assurance Services
A federated identity in information technology is the means of linking a person's electronic identity and attributes, stored across multiple distinct identity management systems.

Getyournec.scot Agents
An agent will either be an Improvement Service member of staff who is authorised to review, verify and process application data on behalf of a Local Authority; or an authorised member of staff from a Local Authorised.

Identity
Any reference to identity in myaccount refers to the identity of the user, which is you. You have an identity and at times, you may be asked to verify your identity to prove who you are. This enables service providers to provide you with the correct service and prevent people from fraudulently gaining access to a service.

IDP
An identity provider (abbreviated IdP or IDP) is a system entity that creates, maintains, and manages identity information for principals while providing authentication services to relying applications within a federation or distributed network. Identity providers offer user authentication as a service.

ISO 27001
ISO/IEC 27001 is widely known, providing requirements for an information security management system (ISMS), though there are more than a dozen standards in the ISO/IEC 27000 family. Using them enables organizations of any kind to manage the security of assets such as financial information, intellectual property, employee details or information entrusted by third parties.

Log Files
A log file is a file that records either events that occur in an operating system or other software runs, or messages between different users of a communication software.

NECPO
The NEC scheme is operated by Dundee City Council (acting as the National Entitlement Programme Office (NECPO)) on behalf of all Scottish Local Authorities.

Open Standard Protocols
Open standard protocols for identity federation define how service providers (SPs) and identity providers (IdPs) exchange identity information. Open standards are critical to enable secure interoperability between unique identity systems, web resources, organisations and vendors.

Service Provider
Is a Local Authority that has made getyournec.scot available to its citizens as an online channel to apply for and update a National Entitlement Card.

Single Sign On (SSO)
Single sign-on is an authentication process that allows a user to access multiple applications with one set of login credentials.

Special Categories of Data
Means any personal data relating to a users' health, genetic or biometric data, criminal convictions, sex life, sexual orientation, racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership.

Applications for a disabled concessionary travel National Entitlement Card require special category data to be submitted. Users are requested to submit a document as proof of disability. That document will be one of the following:

- a photograph of a blue badge;
- a letter from the DWP noting the applicant is in receipt of middle or higher rate component of Disability Living Allowance, or receive Attendance Allowance or Personal Independence Payment;
- a letter from the DWP or SSS which may include details about your health;
- a letter from a Health Consultant or GP detailing relevant disability;
- a copy of Certificate of Vision (CVI) Scotland form;
- a letter from DVLA confirming driving licence has been removed for medical grounds;
- a letter from Ministry of Defence or Veterans UK stating the applicant is in receipt of War Pensioner Mobility Supplement;
- a copy of a NCT002a form noting the applicant has a learning disability;
- a copy of a DS1500 report or hospice admittance letter confirming the applicant has a terminal illness.

The full list of up to date accepted proofs can be found on Transport Scotland's website.

Two Factor Authentication (2FA)
Two-factor authentication (2FA), sometimes referred to as two-step verification or dual-factor authentication, is a security process in which users provide two different authentication factors to verify themselves.

Example: a user can sign-in to an account using a username and password (something they know) and an authentication code is sent to their mobile phone (something they have).
If a user could sign in without the code, there's a risk that someone else could guess or steal their password to access their account. Using an authentication code as another authenticator means that, even with the password, a fraudster would still not be able to access the account.

Users
This is you and other people who use our services.

Verified
This means you have gone through a process to prove you are who you claim to be. You have verified your identity.

VLANS
A VLAN (virtual LAN) is a subnetwork which can group together collections of devices on separate physical local area networks (LANs). A LAN is a group of computers and devices that share a communications line or wireless link to a server within the same geographical area.

Yoti
Yoti is a company which the Improvement Service contracts with to provide us with services. Their services enable you to register, sign-in and verify a myaccount. More info can be found on their website.