Scottish Dog Control Database

Data Privacy Impact Assessment

Version 2.0

Authors

This document was prepared by:

Project Manager – Digital Public Services Improvement Service	

Version History

Date	Document Version	Document Revision History	Document Author/Reviser
09/11/2021	1.0 Draft		Project Manager
11/1/2022	2.0	Remove reference to whitelisting	Project Manager

Approvals

Date	Document Version	Approver Name and Title	Approver Signature
25/11/2021	1.0	Strategic Business & Delivery Lead	
11/1/2022	2.0	Strategic Business & Delivery Lead	

Contents

Scottish Dog Control Database Data Privacy Impact Assessment (DPIA)

Effective 11th January 2022.

The Need for a DPIA

The database (dcn.scot) will hold information from all local authorities relating to dog control notices (DCN) served in Scotland.

Section 8 of the Control of Dogs (Scotland) Act 2010 ("the 2010 Act") provides an enabling power for Scottish Ministers to make regulations to establish a "Scottish dog control database": The 2010 Act introduced the DCN regime. The DCN is a civil notice, for use against dog owners who do not keep their dogs under proper control. A DCN can contain a number of conditions such as requiring a dog to be on a lead when in public. The 2010 Act came into force on 26 February 2011.

Local authority 'authorised officers' (i.e. dog wardens), have therefore been issuing DCNs, to dog owners who do not keep their dogs under proper control, for over a decade. Under the 2010 Act each local authority has a statutory responsibility to monitor the effectiveness of every DCN they have issued. All 32 local authorities have their own internal record systems in place for monitoring and enforcing DCNs. However, concerns have been raised about difficulties that occur when the person who has been issued with a DCN moves from one local authority area to another.

We are now looking to use the powers available under section 8 of the 2010 Act to establish a national database. The national database will bring together the records of all 32 local authorities into a centralised database that is accessible by local authorities and Police Scotland. Local authorities and the Improvement Service will be 'joint controllers' of the database. The creation of a national database will be a valuable tool in helping to enforce DCNs where a person subject to a DCN moves to another local authority area. The database will not hold any information relating to breaches of DCN, investigations undertaken by local authorities nor will it hold any information relating to compliance and enforcement of conditions imposed as part of the DCN. No criminal information is held on the database.

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 Scottish Dog Control Database:

- Processes personal data that could result in a risk of physical harm in the event of a security breach

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

The Processing
What is the Scottish Dog Control Database used for

The national database will bring together the records of all 32 local authorities into a centralised database that is accessible by local authorities and Police Scotland.

Local authorities and the Improvement Service will be 'joint controllers' of the database.

The creation of a national database will be a valuable tool in helping to enforce DCNs where a person subject to a DCN moves to another local authority area. The database will not hold any information relating to breaches of DCN investigations undertaken by local authorities nor will it hold any information relating to compliance and enforcement of conditions imposed as part of the DCN. No criminal information is held on the database.

Context of the Processing

The proposed database was widely supported in the public consultation held between September 2019 and January 2020, 'Steps to Improve the Operational Effectiveness of the Control of Dogs (Scotland) Act 2010.'

Further, during the last session of Parliament the Public Audit and Post-legislative Scrutiny (PAPLS) Committee undertook Post-legislative scrutiny of the 2010 Act. In July 2019 the Committee published their Post-legislative scrutiny report on the 2010 Act. One of recommendations contained in the report was that the Scottish Government should establish a national database as a matter of urgency.

When the Minister for Community Safety appeared before the PAPLS Committee on 18 February 2021, the Minister gave a commitment that a national DCN database would be delivered and up and running by the end of 2021.

The personal date to be processed will be:

- The name of the person to whom the DCN applies.
- The date of birth, address and postcode of person to whom the DCN applies.

The database will also record:

- If the DCN has been discharged.
- If the DCN has been varied.
- If the DCN has been transferred from one council to another council.
- Any steps that person was required to take for the purposes of bringing and keeping the dog in question under proper control In addition, the DCN will also record information about the dog, for example, the microchip number and name of the animal.

The Scottish Dog Control Database is run in line with best practice and has external accreditation for ISO27001.

Processing Responsibilities

The Scottish Dog Control Database is 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 Bill 2018, which came into effect in the UK on 25th May 2018.

The Improvement Service and all 32 Scottish Councils are the joint Data Controllers for the database.

Users of the database are strictly limited to authorised officers from Scottish local authorities, Police Scotland authorised officers, and authorised staff from the Improvement Service.

Other Data Processors

The Improvement Service has contracts with a managed service company (Tata Consultancy Services) and a hosting company (brightsolid UK). Both companies are Data Processors for the Improvement Service.

The contracts with all these companies reflect the GDPR obligations of both the Improvement Service and the contractors.

Purposes of Processing

The personal data which is to be processed and held is limited to:

- The name of the person to whom the DCN applies.
- The date of birth, address and postcode of person to whom the DCN applies.

The purpose of this processing is to provide a service to Scottish local authorities, in the interest of public safety. The lawful basis for processing is Public task/ Legitimate interests.

The database will also record:

- If the DCN has been discharged.
- If the DCN has been varied.
- If the DCN has been suspended.
- If the DCN has been transferred from one council to another council.
- Any steps that person was required to take for the purposes of bringing and keeping the dog in question under proper control In addition, the DCN will also record information about the dog, for example, the microchip number and name of the animal.

The database will also hold basic information for registered users of the system, to include:

- An authorised officer's name
- E-mail address

The purpose of this is to ensure that access is only permitted to authorised individuals and that all access is logged and traceable to individual users.

Finally, system access and use will be timestamped and recorded in log files along with the user ID of the person using the service. This is done to ensure we can trace suspicious activity to individuals and to prevent system misuse. Examples of behaviour which we would seek to capture for this purpose includes:

- Users remaining logged in for extended periods of time (e.g. Several hours at a time)
- Users lacking proper cause to make use of the service (e.g. checking if your neighbour has a DCN)

Scope of the Processing

Access to the database is strictly controlled. Each local authority will be provided with no more than two super-agent accounts on the system. Those provided with super-agent access will then be permitted to grant and authorise access to other members of their team, for the purposes of uploading new DCNs, adding a variation to a DCN, discharging a DCN, suspending a DCN, or viewing DCN data on the database.
Police Scotland also be provided with no more than two super-agent accounts, but with read-only access. The super-agent will be permitted to grant and authorise access to other colleagues who require access to the system, for the purposes of searching for DCN data but will be unable to edit / suspend / discharge or add a variation to a DCN.

Raising a Query

If a user wants to contact us or report a problem, they can do so via the dcn.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.

Data Retention

The dcn.scot Data Retention Policy is in line with the GOV.UK Verify: IPV Operations Manual. The manual is a set of instructions for identity providers on how to provide identity proofing services in line with Good Practice Guides (GPGs 44 and 45).

The table below notes the data retention rules:

Entity	Type	State	Retention Period	Data Deleted
DCN	DCN record	Discharged	24 months after the date of discharge.	All data recorded in the DCN, including pdf of DCN and Service of Notice.
Support Request	Dcn.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	5 years.	All log data
Authentication Log	Unsuccessful	Unknown user	5 years.	All log data

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:

Processing DCN data on behalf of councils

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

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 dcn.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

Where Legitimate Interest has been sighted, 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 dcn.scot service.

The dcn.scot service follows standards and guidelines for identity proofing set by Government including; GOV:UK Verify IPV Operations Manual, GPG 44 and GPG 45.

For authentication, SAML and OpenID Connect network federation standards are used. The OpenID Connect solution has self-certification through the OpenID website.

An Information Exchange Protocol outlines the agreed technical controls for securing data in transit between the DCN.scot 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 either SAML or OpenID Connect protocols. Strong digital certificates against fully qualified domain names are used to encrypt and sign all web services traffic including authentication.

Signature of encrypted traffic is required by both the sender and the receiver.

Data Minimisation

Dcn.scot is built with data minimisation principles. Dcn.scot holds the minimum amount of data required for each DCN as laid out in 'The Scottish Dog Control Database Order 2021'

Dcn.scot aligns its data policy with agreed standards set out by Government. These standards include the GOV.UK Verify: IPV Operations Manual which provides instructions for identity providers on how to provide identity proofing services in line with Good Practice Guides (GPGs) 44 and 45.

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 dcn.scot website. The privacy notice and terms and conditions are emailed to an authorised agent (council / Police Scotland) when they activate their agent account.

Any changes to these documents are communicated with users on the dcn.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.

Rights to Restriction and to Object

Users can raise a complaint with the dcn.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

Risks

Confidentiality

Source and nature of potential impact on users	Likelihood	Severity or Harm	Mitigating controls	Overall Risk
Nature of Impact: Identity theft due to: • Spoofing, • Impersonation, • Human error. Source: • External, or • Internal human sources.	Possible Username and password are used to access agent accounts. Accounts could be compromised if there is a data breach on a different site a user uses the same credentials on.	Distress or inconvenience to user. 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. We have controls within the data centres to monitor for potential data loss and anomalous behaviour.	Medium

Action plan / corrective actions

Two-Factor-Authentication would provide protection against account compromise due to data breaches elsewhere.

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.	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. Lack of service could cause inconvenience to users.	• 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

Dcn.scot is operated in line with security best practice. Accreditation to ISO27001 already in place.

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.

Logical access control

VLANs are used to separate different environments.

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. IS 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 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

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:		
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:		

Definitions

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

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.

Identity
Any reference to identity in dcn.scot 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.

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.

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.

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

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.