



One parking partner. Infinite possibilities.

**G-Cloud 15 (RM1557.15) Parkingeeye
Ltd.**

**Evology Pay
Service Definition**

December 2025

Table of contents

1 Introduction	4
1.1 Document structure	4
1.2 How to use this document	4
2 Service description	4
2.1 About our service	5
2.2 Delivery framework.....	6
2.3 Service features / benefits.....	6
2.4 Service scope	7
2.4.1 Add-ons and extensions	7
2.4.2 Cloud deployment model	7
2.4.3 Service constraints.....	7
2.4.4 System requirements.....	8
2.5 User support	8
2.5.1 Support details.....	8
2.5.2 Accessibility and usability	8
2.6 How users work with our service	9
2.6.1 Browsers.....	9
2.6.2 Desktop application	9
2.6.3 Mobile	9
2.6.4 Service interface	10
2.6.5 API	10
2.6.6 Accessibility and usability	10
2.6.7 Customisation	10
2.6.8 Service levels and availability.....	11
3 G-Cloud alignment information	12
3.1 Section introduction	12
3.2 Onboarding and offboarding processes	12
3.2.1 Onboarding.....	12
3.2.2 Offboarding.....	12
3.3 Data	14
3.3.1 Data importing and exporting	14
3.3.2 Analytics.....	14
3.3.3 Independence of resource	15
3.3.4 Public sector networks	15
3.3.5 Data-in-transit protection	15
3.3.6 Asset protection	15
3.4 Availability and resilience.....	15
3.4.1 Guaranteed availability	15
3.5 Governance	16
3.6 Security	16

3.6.1 Operational security	17
3.6.2 Staff security.....	17
3.6.3 Secure development	17
3.6.4 Identity and authentication	17
3.7 Auditing	17
3.7.1 Performance monitoring and metrics.....	17
3.7.2 Compliance and quality management	18
3.8 Backup, restore & disaster recovery	18
3.9 Training.....	19
3.10 Service pricing.....	19
3.11 Invoicing process.....	19
3.12 Termination terms	19
4 Security and data governance	19
4.1 Data protection and encryption	19
4.2 Data at rest, storage locations, and physical security.....	20
4.3 Data sanitisation and disposal	20
4.4 Security testing and assurance	20
4.5 Incident and protective monitoring management	20
4.6 Configuration and change management	20
4.7 Information security management and certifications	20
4.8 Secure development and cryptography.....	21
4.9 Identity and access management	21
5 Supplier information	21
5.1 About us	21
5.2 Relevant experience and testimonials	21
5.3 How to buy.....	22

1 Introduction

1.1 Document structure

This Service Definition document provides information about the services we offer under the G-Cloud 15 Framework. Providing information on the functionality, security, pricing and management of our services, as well as how to engage with us through the framework, the document is divided into the following sections:

- ✓ **Service description:** Provides an overview of our services, outlining key features, benefits, delivery methodology and assurance measures
- ✓ **Operational delivery and framework alignment:** Details how our services are delivered under and in alignment with the G-Cloud 15 framework
- ✓ **Supplier information:** Summarises our company background, mission, relevant experience and how to procure our services through G-Cloud

1.2 How to use this document

This document is intended to support buyers at every stage of their G-Cloud procurement journey, from initial service evaluation through to contract award and delivery management.

- ✓ To help determine alignment with organisational needs for early-stage evaluation, Section 2 (Service description) outlines our service scope, methodology and core benefits
- ✓ For due diligence and contract preparation, Section 3 (G-Cloud alignment information) provides the required detail on onboarding, service levels, data management, support and exit procedures
- ✓ To assure data protection and compliance, Section 4 (Security and data governance) outlines our information-security framework, data-handling standards and business-continuity measures
- ✓ For supplier verification, Section 5 (Supplier Information) includes background information on us, our experience and procurement routes

2 Service description

2.1 About our service

As the leading Automatic Number Plate Recognition (ANPR) provider for **21+** years, we currently manage over **4500** ANPR car parks across the UK and Europe. Demonstrating our industry-leading position for delivering ANPR solutions, we have worked with over **700** private and public clients to create bespoke car park management solutions. Our service **Evology Pay** is an in-house developed, cloud-hosted SaaS platform for digital cashless parking.

Built and enhanced entirely in-house, the platform evolves rapidly to buyer needs and reduces contact-centre demand through self-service features. It is designed to remove cash handling, minimise manual reconciliation, and improve user satisfaction through convenient payment touchpoints. Available through app and browser, Evology Pay offers optional ANPR integration for automated enforcement. Streamlining parking journeys and reducing operational overheads, Evology provides flexible payment pathways including:

- ✓ **Pay to Park:** User arrives in the car park and pays for parking using a location code. To streamline their payment, we will use the user's location services to identify which car park they are in
- ✓ **Pre booking:** Evology has pre-booking and pre-payment options. Users can search, find and pay for parking in advance with email confirmation and receipts available if required. Adding value, our pre-booking feature includes opt-in SMS reminder notifications
- ✓ **Autopay:** User sets up an account and registers their Vehicle Registration Number (VRN) and debit/credit card within the app. Simplifying the payment process, the user will park as normal, and on exit, we automatically debit their account with the correct duration tariff
- ✓ **Pay After:** For flexibility on payment timings, the user can pay up to 24 hours after leaving the car park

Highlighting the safety, efficiency and quality of our services, we hold the following accreditations and memberships:



Figure 2.1.1: Our industry accreditations and memberships

2.2 Delivery framework



Figure 2.2.1: Our delivery framework

Evology Pay is delivered as a managed SaaS service hosted on Microsoft Azure in UK regions. Prioritising user-centred enhancements and operational reliability, our in-house product and engineering teams use Agile/Scrum to iterate quickly and safely. Aligning with buyers' requirements and site-specific rules for car parks, our Account Management Team gather the following information at mobilisation:

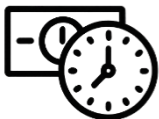
- ✓ Tariffs
- ✓ Grace periods
- ✓ Site rules
- ✓ Optional ANPR integration for automated Parking Charge Notice (PCN) enforcement
- ✓ Exemptions, whitelists and permits
- ✓ Identity options
- ✓ Integrations including Azure AD B2C Single Sign-On (SSO)

Our technical team then integrate these criteria into our back-office proprietary system, Cayenne, enabling Evology Pay to function as desired.

2.3 Service features / benefits



Autopay with VRN and card on exit: This option delivers frictionless parking and eliminates manual payment steps, enhancing customer satisfaction.



Pay After up to 48 hours post-visit: This reduces enforcement pressure and complaints, reducing reputational risk to buyers, by allowing flexible post-visit payments.



Parking session extension from the Evology app: Improving user experience and encouraging parking compliance, this option allows users to stay longer without returning to their vehicle.



Booking overview of past and upcoming sessions: Providing transparency and easy record access for users and administrators, this option supports confidence in car park use, planning and easy reference when needed.



Receipt download for expenses and records: Supporting simple and compliant expense management, this option allows users to easily download receipts for their parking sessions when needed.



SMS confirmations and reminders: Supporting compliance, SMS confirmations and reminders improve simple transparent communication and reduce users' missed payments.



Seamless optional ANPR integration: Reducing the need for manual checks, Evology Pay's ability to integrate with ANPR allows for automated enforcement through accurate entry/exit validation.



Fully paperless cashless parking solution: Evology Pay eliminates the need for paper tickets, reducing cash handling and manual reconciliation, streamlining operations and keeping costs down.

2.4 Service scope

Evology Pay operates as a standalone service that can integrate with ANPR systems through our back-office proprietary system, Cayenne. Providing a unified digital parking experience across mixed site architectures without reliance on third party dependencies for core payment functions, ANPR integration enables Evology Pay to automate:

- ✓ Entry/exit validation
- ✓ Payment accuracy
- ✓ Enforcement workflows

2.4.2 Cloud deployment model

We provide our service entirely through a public cloud hosting model on Microsoft Azure, using secure UK-based data centres that meet established industry compliance standards. The solution supports scalable, multi-tenant environments and is designed for high availability, resilience, and rapid provisioning.

While the core service runs entirely in Azure, the system can integrate with on-premise or third-party applications via secure APIs, allowing organisations to align with local governance, data residency, or interoperability requirements without compromising performance or security.

2.4.3 Service constraints

Evology Pay is designed for flexibility across diverse parking environments. We deliver our services within the following standard constraints:

- ✓ The service operates in a cloud-hosted environment and is accessible via all modern web browsers

- ✓ Planned maintenance is conducted outside core UK business hours in the evening (daily device patching and weekly server patching), so as not to affect app users or result in app downtime
- ✓ Performance may vary when used in non-UK regions due to data residency and latency differences

2.4.4 System requirements

To ensure optimal performance, the service requires the following minimum system configuration:

- ✓ **Supported browsers:** Latest versions of Chrome, Edge, Safari, Firefox and Opera
- ✓ **Operating systems:** Windows 10+, macOS 12+, iOS/Android (latest two versions)
- ✓ **Connectivity:** Stable broadband connection (recommended minimum 10 Mbps)
- ✓ **User permissions:** Standard user account. Administrative rights required only for optional local integrations
- ✓ **Optional Interactive Voice Recognition (IVR):** For telephone payments
- ✓ **Third-party prerequisites (if applicable):**
 - Valid Microsoft 365/Google Workspace licence for productivity integrations
 - API keys for approved external systems

Any additional requirements specific to a buyer engagement will be confirmed within the Statement of Work.

2.5 User support

To ensure buyers can access help quickly, resolve issues efficiently and maintain continuity of operations, we provide a dedicated Account Manager for every contract, as well as the below structured, responsive support service:

2.5.1 Support details

Support channel	Availability/response times
Dedicated Account Manager	Available Monday – Friday, 9am – 5pm throughout the contract, with defined points of escalation/contingency for absence. Our Account Managers respond to all queries/issues within 24 working hours, and will respond to high priority issues within 4 working hours
Evology App, email and WhatsApp chat bot/human agents	Our WhatsApp chat bot will respond 24/7 and our other channels will respond during office hours, Monday–Friday, 8am–6pm. Outside of working hours, we will respond the next working day
Out-of-hours call service	Responses in emergencies, by the next working day

Figure 2.5.1.1: Support channels and response times

2.5.2 Accessibility and usability

Prioritising accessibility and usability, in line with WCAG guidelines, Evology Pay is designed to enable all users, including those with assistive needs, to access and manage parking easily, leveraging system-level accessibility features such as:

- ✓ Screen readers
- ✓ Text scaling

- ✓ High-contrast modes

Reducing cognitive load and speeding up user interactions, the Evology has simple, task-focused flows for pre-booking, paying, extending sessions and downloading receipts.

For ongoing accessibility, we perform testing at every major release using automated tools such as axe-core and WAVE, combined with manual audits using assistive technologies like VoiceOver and NVDA. This enables users to reliably navigate and complete tasks. Our support channels, including WhatsApp and in-app ticketing, provide accessible assistance, helping users resolve issues quickly through keyboard navigation and screen readers. Giving buyers and administrators flexible, inclusive access, documentation is available in HTML and PDF formats that meet accessibility guidelines, with alternative formats available on request. Enhancing usability, confidence and adoption for all users, we continually review accessibility feedback through our user-centred design process, integrating improvements into each release.

2.6 How users work with our service

2.6.1 Browsers

Evology Pay is accessible through any modern standards-compliant web browser. We support the latest versions of:

- ✓ Google Chrome
- ✓ Microsoft Edge
- ✓ Mozilla Firefox
- ✓ Apple Safari
- ✓ Opera

We recommend enabling JavaScript and cookies for full functionality. Buyers are notified in advance of any changes to browser support.

2.6.2 Desktop application

No dedicated desktop application is required as Evology Pay operates via all modern web browsers.

2.6.3 Mobile

Our Evology Pay app is designed for mobile and is available on iOS/Android with location services, notifications and native flows.

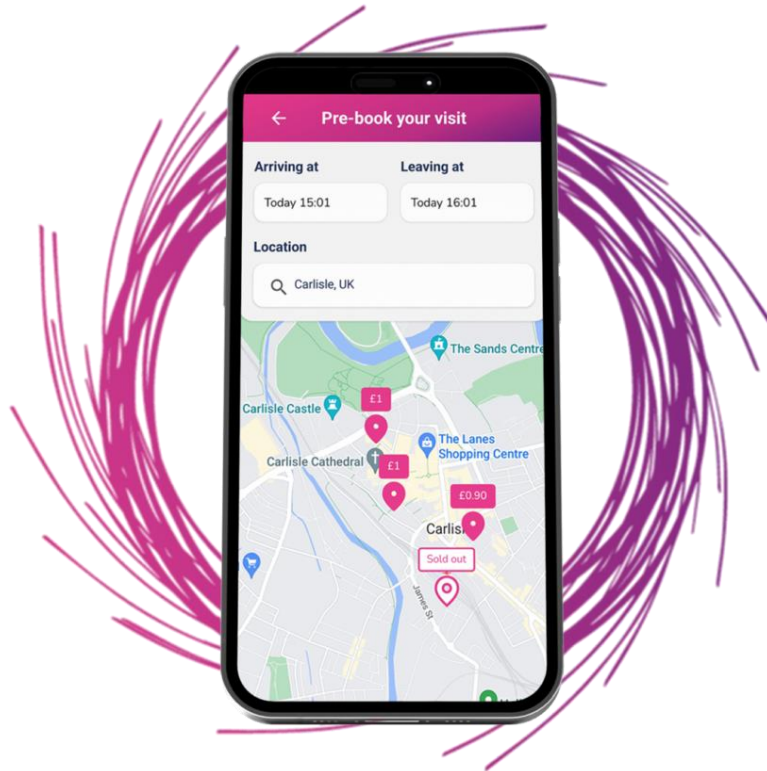


Figure 2.6.3.1: The Evology Pay app's easy-to-use interface

2.6.4 Service interface

The mobile app provides native experiences such as location services for car park identification and push/SMS notifications. The web experience provides equivalent core functions (payment, booking overview, receipt download, Pay After and session extension) via responsive interfaces. Both support cashless workflows, but the app offers convenience for on-the-go actions while desktop suits admin review.

2.6.5 API

Identity and payment integrations are supported, including Azure AD B2C, Apple Pay and Google Pay. Buyers can enable SSO and bulk upload concessions data. Full public API specifications/sandbox details are available on request.

2.6.6 Accessibility and usability

All interfaces are designed in accordance with WCAG 2.2 AA standards. Interfaces use clear journeys and benefit from native/mobile and accessible web patterns. We regularly test usability with diverse user groups, including users with assistive technologies. Features include keyboard navigation, screen-reader compatibility, high-contrast modes and scalable text.

2.6.7 Customisation

Buyers can tailor payment pathways through:

- ✓ Our Pay After window
- ✓ SMS notifications
- ✓ Identity options (Azure AD B2C/Apple/Google)
- ✓ Tariffs and site parameters (location codes)

To preserve user states, concessions data can also be bulk uploaded. For buyers requiring automated enforcement, Evology Pay can also be customised to integrate with ANPR. Ensuring buyers receive a tailored

service, we assign a dedicated Account Manager to all contracts, from mobilisation for the entire duration of the contract.

2.6.8 Service levels and availability

Assuring buyers of our high service performance and availability, we maintain a system uptime of **99.9%**. In the unlikely event of an outage, buyers' dedicated Account Managers will report this and resolution timescales, as well as remedial actions, within 2 working hours of being aware of a problem.

Any breaches of agreed service levels targets trigger internal escalation and, where applicable, corrective actions or service credits in line with the contract.

3 G-Cloud alignment information

3.1 Section introduction

We deliver Evology Pay under a collaborative service model that incorporates structured onboarding, secure operation, transparent, consistent support and controlled offboarding. The account-led framework aligns to G-Cloud requirements and public-sector governance, with security embedded through:

- ✓ Azure hosting
- ✓ Multi-Factor Authentication (MFA)
- ✓ Monitoring through our Security Information and Event Management (SIEM) and external Security Operations Centre (SOC)
- ✓ Regular testing

3.2 Onboarding and offboarding processes

3.2.1 Onboarding

For smooth onboarding and alignment with buyers' requirements and expectations, upon contract award we execute our implementation plan and schedule a launch meeting with key stakeholders. The meeting agenda typically includes:

- ✓ **Introductions and governance:** Confirmation of attendees, project roles, escalation routes and key contacts
- ✓ **Implementation timelines:** Agreement of key milestones, including configuration, testing and go-live dates and confirmation of any changes to the delivery plan
- ✓ **Commercial and financial set-up:** Confirmation of agreed commercial terms, payment flows, banking and settlement arrangements and finance contacts for onboarding
- ✓ **Contract and procurement coordination:** Confirmation of legal and procurement contacts and contract finalisation timelines (led by buyers)
- ✓ **Site and service scope:** Confirmation of car parks and locations to be enabled within Evology Pay, including any optional ANPR integrations
- ✓ **Communications and user engagement:** Agreement of customer communications for launch, including approval processes and any digital or on-site messaging required to support adoption
- ✓ **System access and training:** Confirmation of user roles, back-office access and delivery of appropriate system training to ensure all users are competent prior to go-live

In the finalised implementation plan, agreed at the launch meeting, the buyers' Account Manager will confirm key milestones for the delivery of Evology Pay, including:

- ✓ Platform configuration and tenant set-up
- ✓ Integration and configuration of optional ANPR services (where selected)
- ✓ User account, payment and notification set-up
- ✓ Testing and validation of live environments
- ✓ Go-live dates for agreed sites
- ✓ Completion of system set-up and handover to business-as-usual support

3.2.2 Offboarding

To support easy exit/offboarding, full data portability and a secure transition, we operate a clear, documented Exit Plan for Evology Pay. Ensuring buyers can leave the service without disruption, hidden costs or dependency on proprietary systems, we have outlined our Exit Plan below:

1. Early engagement and communication

Upon written notice of contract expiry or early termination, we will initiate an exit process focused on transparency, cooperation and continuity.

Initial transition meeting (within month 1): We will hold an initial meeting with the buyer and, where applicable, an incoming supplier or internal team to agree the scope of exit, confirm responsibilities and outline the transition approach. A mutually agreed exit timetable will be confirmed, typically covering up to six months depending on buyer requirements.

Appointment of a demobilisation lead: Coordinating technical, commercial and data-related activities and ensuring accountability, a dedicated Account Manager will act as the single point of contact throughout the exit process.

2. Documentation and data portability

To enable a smooth handover and avoid vendor lock-in, we will provide clear documentation and portable data formats.

Transition documentation: We will provide an exit and transition pack setting out:

- ✓ Evology Pay system configuration and service scope
- ✓ User roles and permissions
- ✓ Payment, reporting and notification workflows
- ✓ Integration details (including optional ANPR, where used)

Documentation will be kept up to date and reissued if required up to one month prior to service cessation.

Data compilation and export: All buyer-owned data will be made available in commonly used, non-proprietary formats such as CSV or Excel, including:

- ✓ Transaction and payment records
- ✓ Parking session data
- ✓ User account data
- ✓ Audit logs and reports

Data exports will be agreed in advance to ensure they meet the buyer's governance, audit and retention requirements.

3. Joint meetings and handover support

Operational walkthroughs: Where required, we will host walkthrough sessions to explain system functionality, reporting, and data structures, enabling the buyer or incoming provider to understand and reuse the data effectively. Sessions can be delivered remotely and supported with written guides.

Ongoing communications during transition: The Account Manager will hold regular progress meetings throughout the agreed exit period to track milestones, resolve issues and confirm readiness for service closure.

4. Secure service closure

Account closure and access removal: Once data handover is complete and confirmed, user access will be securely revoked, administrative accounts closed and integrations disabled in line with agreed timelines.

Data deletion and confirmation: Following buyer confirmation, remaining buyer data will be securely deleted in accordance with contractual obligations and data protection requirements, with written confirmation provided.

5. Post-exit support

To reduce transition risk, we offer a defined post-exit support or “grace period”, such as 30 days, during which the buyer or incoming provider can raise clarification queries relating to exported data or documentation, at no additional cost.

3.3 Data

3.3.1 Data importing and exporting

By using open, widely adopted data formats and clear governance processes, Evology Pay enables buyers to move data into, within and out of the service easily and without restriction. Enabling flexibility throughout the contract and providing confidence that data remains fully under the buyer’s control, our approach ensures buyers are not locked into the service.

Buyers can bring data into the service easily using standard, non-proprietary formats such as CSV, with additional formats (including XML where required) supported depending on client preference. This allows straightforward onboarding of parking records, whitelists and related configuration data without the need for bespoke tooling or specialist development.

Ensuring ongoing transparency and operational independence, buyers can export all their data at any time. Allowing data to be reused, analysed or transferred to alternative systems with minimal effort, data is made available in open formats such as CSV, PDF or XML. Exports are provided securely and in a structure that is easy to interpret by internal teams or incoming suppliers.

At the end of the contract, our Demobilisation Team works collaboratively with the buyer and any incoming provider’s IT team to ensure a GDPR-compliant handover of all relevant data.

To further support trust and auditability, we operate annually reviewed data retention and disposal policies within our Information Security Management System (ISMS). Non-contravening data is retained for up to 6 months, images for 90 days, and contravening data for up to 6 years, after which data is securely wiped. We provide formal data deletion certificates where required, giving buyers assurance that data is handled responsibly beyond contract end.

3.3.2 Analytics

Evology Pay provides meaningful usage and operational data through bespoke dashboards and reporting tools, accessible to buyers through secure logins to our Client Portal. Buyers can access booking overviews, receipts and session details, with internal availability metrics tracked and reports provided on request or at agreed intervals. Supporting informed decision-making, governance and proactive management of the service, data can be exported for use in external BI platforms.

3.3.3 Independence of resource

Providing stable, reliable performance for all users, Evology Pay is hosted on Azure, leveraging its built-in scalability, proactive patching and continuous monitoring. Workloads are fully isolated and multi-tenant resources are carefully managed so that activity from other customers does not impact performance. Giving buyers confidence that their operations remain uninterrupted and consistent regardless of broader system usage, availability targets are maintained according to server type. Load balancing ensures that multi-tenant demands are distributed efficiently.

3.3.4 Public sector networks

Where necessary, Evology Pay can support secure integration with authorised public sector networks, including PSN, HSCN, JANET, PNN and SWAN. All connections are implemented in accordance with the applicable governance, accreditation, and security frameworks, ensuring that data exchanged across these networks is appropriately safeguarded. Any requirement for connectivity to a specific public sector network will be identified during onboarding and implemented in line with the relevant technical and compliance standards.

3.3.5 Data-in-transit protection

Our infrastructure is entirely cloud-based, with storage hosted by Microsoft Azure. All data in transit is encrypted using Advanced Encryption Standard (AES) 256 as a minimum standard. This level of encryption ensures that even if physical or logical access to data storage were compromised, the data would remain unreadable without access to the appropriate decryption keys.

3.3.6 Asset protection

As our infrastructure is fully hosted on Microsoft Azure, we do not maintain physical data centre access. Ensuring data sovereignty, Azure uses UK-based data storage facilities.

In line with the General Data Protection Regulations (GDPR) and Data Protection Act, information captured is processed securely with strict access controls. All data is securely stored within Cayenne, which is hosted on a cloud-based infrastructure. This ensures scalability, high availability, and resilience, with real-time access for authorised personnel. Data is encrypted in transit and at rest and is stored in compliance with GDPR. Our cloud hosting includes redundant backups to protect against data loss, ensuring business continuity and operational reliability. We store data on Cayenne for 6 months, before anonymising it for up to 6 years, after which data is securely wiped to MC Infosec Level 5 Enhanced (CESG) via Green IT prior to destruction. Giving buyers assurance that data is handled responsibly beyond contract end, we provide formal data deletion certificates where required.

3.4 Availability and resilience

3.4.1 Guaranteed availability

We maintain **99.9%** availability for web, IVR and SMS servers. Embedding resilience, we ensure:

- ✓ Near-real-time Disaster Recovery replication
- ✓ Nightly off-site backups
- ✓ Bi-annual recovery tests
- ✓ Proactive patching
- ✓ Weekly vulnerability scans
- ✓ Annual penetration testing

Maintaining transparency, outages are communicated through dedicated Account Managers and the wider support channels outlined in Figure 2.5.1.1.

3.5 Governance

To proactively maintain data protection and cyber security, in line with our Cyber Essentials Plus accreditation and ISO 27001-aligned ISMS, we manage the following risks:

- ✓ Unauthorised system access
- ✓ Malware infection
- ✓ Internal user data misuse

To mitigate these risks and maintain robust security governance, we implement:

- ✓ **Antivirus software:** To protect against cyber threats, we use Microsoft Defender. This offers automatic updates and patching to address known vulnerabilities across our systems. Supporting this, NinjaOne, our Remote Monitoring and Management solution, scans and updates end-user devices automatically
- ✓ **MFA:** We maintain mandatory MFA for accessing all systems. This includes password and verification combinations on user devices/apps holding sensitive data
- ✓ **Firewall:** Preventing unauthorised access, we use our firewall, Palo Alto, which monitors traffic to block unauthorised access in real time. Palo Alto has intrusion detection and prevention (IDS and IPS) enabled
- ✓ **Data encryption:** Making sensitive data unreadable to unauthorised users, we encrypt all data, both in transit and at rest, using Advanced Encryption Standard (AES) 256 encryption
- ✓ **Internal training:** We provide annual training on phishing prevention, safe data handling, maintaining secure passwords and our GDPR and Data Protection Policies. Supporting this, users cannot install unauthorised software on their devices

3.6 Security

We have developed our Information ISMS in line with ISO 27001. This covers our Data Protection legal obligations. Our policies are reviewed by Alban Tramard, our Information Security Manager at least annually to reflect changes in regulations and best practices. All policy changes are signed off by a company executive and made available to all staff. This includes but not limited to the following policies:

- | | |
|------------------------|------------------------|
| ✓ Information Security | ✓ Business continuity |
| ✓ Data Protection | ✓ Access control |
| ✓ Acceptable Use | ✓ Operational Security |
| ✓ Asset management | |

Our Information Security Team conduct annual internal audits to review compliance with our Information Security and Data Protection policies. These audits cover:

- ✓ Joiner, mover and leaver processes
- ✓ Access control
- ✓ Data handling practices
- ✓ Risk management

To ensure that our automated patching is effective, our systems are scanned annually for known vulnerabilities. We employ an independent party, RM Information Security, to conduct penetration tests and assess the strength of our websites.

3.6.1 Operational security

Evology Pay ensures changes are carefully controlled through formal configuration and change management processes, with all updates assessed for security impact before deployment. Vulnerabilities are addressed proactively, with daily patches to end-user devices, weekly server updates, and staged rollouts to minimise disruption. Continuous monitoring is provided via a SIEM system with 24/7/365 SOC oversight, complemented by firewalls, intrusion detection and regular vulnerability scans. Ensuring secure, reliable and well-managed service delivery, we manage incidents using ISO/IEC 27035-aligned workflows. These include rapid triage, clear escalation paths and transparent reporting to buyers through agreed communication channels.

3.6.2 Staff security

All personnel with access to systems or customer data undergo thorough background screening in line with BS7858:2019, conducted through **Verifile**. Access is granted following a strict least-privilege principle, secured with MFA and monitored via activity logging. For roles that require higher-level security, Security Check clearance can be sponsored and obtained as necessary to meet regulatory or operational requirements.

3.6.3 Secure development

Evology Pay is developed in-house following secure and controlled development practices that allow rapid enhancements while maintaining security. Policies and procedures are aligned with ISO 27001, and software undergoes annual penetration testing to validate security controls.

3.6.4 Identity and authentication

User access is managed through secure authentication options, including Azure AD B2C SSO and Apple/Google logins, with MFA enforced for employees. Access is granted on a least-privilege basis, and all administrative actions are captured in the SIEM for auditing and review, ensuring that only authorised users can perform privileged functions and all activity is traceable.

3.7 Auditing

Ensuring continual compliance, our ISMS has been developed in line with GDPR/DPA 2018 principles and undergoes annual third-party security audits covering all IT systems and processes. These include:

- ✓ National Cyber Security Centre (NCC) for Cyber Essential Plus
- ✓ DVLA for access to motorist data
- ✓ British Parking Association to maintain membership, as per DVLA requirements

Our Security Team use our security systems, including DataDog and Microsoft Azure, to conduct internal audits to manage compliance as systems update. This includes detecting anomalies and ensuring effective patch implementation.

3.7.1 Performance monitoring and metrics

To effectively measure performance, we record all performance information and Key Performance Indicator (KPI) adherence on Cayenne and review these monthly. Promoting collaboration, we will discuss these with buyers at monthly contract review meetings. Providing accountability, Account Managers will be responsible for embedding remedial actions if required. Operational reports can also be provided to buyers on request.

Embedding continuous improvement principles from the start of each contract, we will review our progress against agreed milestones at review meetings. Continuing to gather feedback throughout contracts, we will also discuss improvements at monthly review meetings/post-project review stage. Where improvements are identified, we will implement these immediately, cascading lessons learned through:

- ✓ 1-2-1s
- ✓ Refresher training
- ✓ Weekly team meetings
- ✓ Toolbox talks
- ✓ Email bulletins
- ✓ Policy updates

3.7.2 Compliance and quality management

Our services are delivered under our ISMS, aligned to **ISO 9001**, **ISO 20000-1**, **ISO 27001** and **ITIL v4** to ensure consistent quality and continual improvement. We hold **Cyber Essentials Plus** certification and undergo annual third-party audits including DVLA and BPA, as well as internal audits through DataDog and Azure.

For robust operational security, staff receive regular training on phishing awareness, safe data handling, and GDPR/DPA compliance. Performance data, customer feedback and audit outcomes are reviewed monthly to identify improvement opportunities and track corrective actions. Governance of all management systems is overseen by Alban, who reports to the Board.

3.8 Backup, restore & disaster recovery

To safeguard all client and corporate information assets, we maintain comprehensive Data Protection, Business Continuity, and Information Governance policies. Ensuring service continuity, data integrity, and minimal disruption to client operations, our approach is aligned with recognised standards including ISO 22301 (Business Continuity Management) and G-Cloud 15 Call-Off Terms.

Our Business Continuity Management (BCM) framework identifies potential threats, evaluates their impact, and defines structured response procedures. A dedicated Operations and Recovery Team activates recovery protocols, coordinates communications, and oversees service restoration. We conduct full risk reviews bi-annually, verify readiness, test technical resilience and evidence compliance through continuity and disaster recovery exercises, including:

Cloud replication: Critical data and servers are synchronised in near real-time to a secure disaster recovery (DR) site within Microsoft Azure, ensuring high availability and resilience.

Nightly backups: All essential datasets are backed up nightly to an offsite location, with bi-annual testing to verify integrity.

Geo-redundancy and recovery vaults: Azure Recovery Vaults with geo-redundant storage provide additional resilience, and managed failover ensures rapid continuity if required.

Incremental and full backups: Both are scheduled to preserve complete operational datasets and audit trails.

Secure retention: Backup data is encrypted at rest and stored in controlled facilities to prevent loss from environmental hazards or unauthorized access.

Our Disaster Recovery Plan defines recovery priorities, escalation paths, and structured procedures to restore services. Key objectives include:

- ✓ Restoring critical systems with minimal downtime
- ✓ Limiting potential data loss to less than 1 working day
- ✓ Maintaining continuous communication with client contacts throughout recovery
- ✓ Prompting users to back up local data where required to ensure all operational information is preserved

Following any exercise or live incident, we complete a post-event review and integrate lessons learned into updated procedures. This ensures a cyclical improvement model that strengthens resilience, maintains compliance, and aligns with ISO 22301 and DSPT requirements.

3.9 Training

Included in our onboarding support, we provide training for relevant staff, including but not limited to the following:

- ✓ Troubleshooting
- ✓ Fault reporting
- ✓ Usage
- ✓ Onboarding and handover documentation
- ✓ System user guides

All staff receive mandatory training for all products relating to the job. Depending on the tender requirements we offer the options to complete this in person, online or on-site. Jan Luxford, our Head of Learning and Development arranges training and ensures this is regularly updated so that all staff have the skills and tools to complete their job roles effectively. A launch meeting sets milestones for go-live dates and set up completion. Account Management oversees timelines and coordinates marketing communications, site surveys and back-office training. Repeat training sessions are available free of charge throughout the contract.

3.10 Service pricing

We operate a fixed pricing model for Evology Pay, which we have detailed in our separate Pricing Document. This is a standard package composed of elements payable by the customer and elements payable by the motorist. We recognise that circumstances and outcomes can vary, so we will handle formal pricing tiers/rates are at call-off.

3.11 Invoicing process

Our standard invoicing cycle is monthly in advance and our payment terms comply with standard government terms of 30 days. Accepted payment methods include BACS and PO.

3.12 Termination terms

Termination is governed by the Crown Commercial Service G-Cloud 15 Call-Off Terms and Conditions. Our standard contracts have a **minimum term of 3 years**, followed by rolling 12-month extensions. Longer terms (for example, 5 years) can be agreed depending on commercial arrangements. Buyers may terminate at the end of the minimum term or any subsequent rolling term by providing **at least 3 months' written notice**.

Early termination may incur costs where upfront investments have been made (for example, optional ANPR hardware), typically calculated to recover amounts committed over the minimum term. In some cases, a **fixed repayment amount** may be agreed, which can reduce progressively over the contract duration. We may terminate only in cases of material breach or non-payment. Upon termination, all data will be handled in line with our offboarding and data-deletion process described in Section 3.3.1.

4 Security and data governance

4.1 Data protection and encryption

Ensuring confidentiality and safeguarding against interception, all data in transit is encrypted using TLS 1.2 or higher, with sensitive information additionally protected using AES-256 encryption. Internal network traffic is

secured through MFA, least-privilege access controls and network segmentation, with a Palo Alto firewall and IDS/IPS providing perimeter protection.

Maintaining robust internal security and operational oversight, a SIEM system monitored by an external SOC ensures continuous detection and escalation of anomalous activity.

4.2 Data at rest, storage locations, and physical security

All data at rest is encrypted using AES-256, providing strong protection against unauthorised access. Data is stored exclusively in UK-based Azure data centres, which adhere to recognised security and resilience standards. Physical security is managed entirely by Microsoft Azure, with no supplier access to the data centres, and includes 24/7 monitoring, biometric access controls, CCTV, perimeter protection and environmental safeguards. Logical and physical separation ensures buyer data remains fully isolated, and storage regions can be specified where required to meet data-sovereignty or compliance obligations.

4.3 Data sanitisation and disposal

Data is securely sanitised in line with **NCSC** and industry best practice. Personally identifiable information (PII) is automatically removed at the end of its retention period, and deleted data is rendered irrecoverable using cryptographic erasure or secure overwrite methods.

When hardware reaches end-of-life, equipment is disposed of through third-party destruction services with certificates of destruction, or via in-house processes. Providing assurance that all data is fully irrecoverable, devices are wiped to **MC Infosec Level 5 Enhanced (CESG) standards** using Green IT prior to destruction.

4.4 Security testing and assurance

Regularly testing systems for vulnerabilities, we ensure the security of the service through regular, independent penetration testing conducted annually. We also conduct weekly automated vulnerability scans to identify emerging risks. For rapid detection, escalation, and remediation of any security incidents, continuous monitoring is provided via a SIEM system overseen by an external 24/7/365 SOC.

4.5 Incident and protective monitoring management

The service follows an ISO/IEC 27035-aligned incident management framework, allowing users to report issues via the app, webform or through their dedicated Account Manager. All events are logged in the SIEM and monitored by the 24/7/365 external SOC, with updates communicated through agreed channels. Continuous protective monitoring is provided via the SIEM/SOC, supported by firewalls with IDS/IPS, regular vulnerability scanning, and patch audits. Maintaining system integrity, this ensures that potential threats are detected and addressed promptly.

4.6 Configuration and change management

For controlled, auditable updates, Evology Pay follows strict configuration and change management processes aligned to recognised standards. All components are tracked throughout their lifecycle, with changes assessed for potential security impact before implementation. Updates and patches are deployed proactively (daily for end user devices and weekly for servers) using automated tools such as NinjaOne. Staged deployments minimise service disruption and post deployment validation ensures integrity. Logs are reviewed regularly and audits confirm compliance with internal ISMS and industry best practice.

4.7 Information security management and certifications

Our service is delivered under a robust governance framework, with policies aligned to ISO 27001, ISO 20000-1 and ISO 9001, and accredited to Cyber Essentials Plus. Compliance and controls are validated through ongoing third-party audits, including annual assessments and surveillance by organisations such as the DVLA and the

BPA. We also conduct internal audits via DataDog and Azure. Security is continuously monitored by an external SOC, and oversight is provided by Alban, ensuring accountability and effective management of information security risks.

4.8 Secure development and cryptography

Demonstrating secure coding and cryptographic controls, Evology Pay is developed in-house following secure development practices and stores all data using AES-256 encryption. Operations adhere to UK data protection principles and are comply with cryptography and NCSC guidance.

4.9 Identity and access management

To effectively control user and admin access, Evology Pay leverages Azure AD B2C SSO, Apple/Google login options, and MFA for employees, ensuring only authorised users can access the system. Access is granted on a least-privilege basis, and all privileged administrative actions are logged in the SIEM for auditing and review. providing flexible yet secure access controls while maintaining full oversight of user activity, where additional security is required, management access can be routed through VPN connections or certificate-based authentication.

5 Supplier information

This section provides background information, relevant experience and practical details on how buyers can procure our services through the G-Cloud 15 framework.

5.1 About us

As the leading ANPR provider for **21+** years, we currently manage over **4500** ANPR car parks across the UK and Europe. Throughout our estate, we maintain a **97%** client retention rate and **99%** system uptime, capturing **1.6 billion** vehicle reads annually and representing **35%** of the market. Using technology-driven, innovative solutions to meet the demands of a multi-sector client base, we operate a diverse team of 360 people. Our history includes several key milestones:

- ✓ **2004:** Founded
- ✓ **2005:** Launched a nationwide ANPR network
- ✓ **2007:** 1 of the first ANPR adopters
- ✓ **2011:** Became a British Parking Association (BPA) member
- ✓ **2015:** Supreme Court decision in Parkingeye v Beavis. Judgement delivered clarity to motorists, landowners and the parking industry
- ✓ **2017:** Developed technology-based payment solutions like autopay/virtual permits
- ✓ **2020:** Developed ParkIQ, our data insights tool
- ✓ **2022:** Launched Evology, our externally facing B2C brand, and ParEV, our EV charging solution
- ✓ **2025:** Became the BPA's first Platinum member

Our **21 years' experience** gives us unparalleled expertise in mobilising, implementing and managing bespoke parking solutions. Maximising revenue and occupancy while minimising traffic flow restrictions, we deliver a positive, streamlined experience for clients and car park users.

5.2 Relevant experience and testimonials

Evidencing our experience, we:

- ✓ Provide services for **36+** NHS Trusts covering 897 car parks, including **6 of the 10** Shelford Group Trusts
- ✓ Support over **180** locations in higher and further education, including with universities such as Surrey, Chichester, Portsmouth, Oxford and Westminster

- ✓ Manage **3 of the big 6** supermarkets, plus large national retail chains such as Home Bargains, The Range and Farmfoods
- ✓ Have the largest portfolio of hotels working with brands such as Marriott, Hilton, Radisson and Holiday Inn
- ✓ Support many other household brands such as Euro Garages, Starbucks and Costa Coffee

We have outlined a case study below showcasing our solution for Staffordshire University, which included Evology Pay.

Staffordshire University: Since 2017, we have provided the following minimally disruptive services to support Staffordshire University's staff, visitors and students:

- ✓ ANPR system with automated enforcement
- ✓ Permit system, including free parking for staff/students and multiple cars per user
- ✓ Cashless payment options through our app, Evology

This contract includes 2 separate campuses at Stafford and Stoke-on-Trent.

Challenges: The University was transitioning from free parking to paid and permit parking, which required flexibility and effective customer service to manage the change.

Outcomes: To implement the new service without affecting the University's operations or reputation, we introduced Evology Pay to manage car park access for staff, students, and visitors. The system provided flexibility by allowing users to pay for specific periods, with Pay to Park functionality enabling public access around term times and on weekends to increase revenue generation.

By managing all customer service and appeals through our in-house team, we safeguarded the University's reputation. Adding further value, we implemented immunity windows at key points in the year, ensuring the system adapted to term schedules and the specific needs of staff and students.

The creation of the different exemption lists allows the department to offer free or discounted parking when required, providing great customer service throughout the university. This is an effective and efficient system to use, reducing resources required within the team.

- **Helen Rutherford, Head of Campus Facilities Management**

5.3 How to buy

Evology's services can be procured directly through the Crown Commercial Service (CCS) G-Cloud 15 Digital Marketplace.

Buyers can search for Evology on the Digital Marketplace and select the required service listing.

Once selected, the buyer and Evology will:

1. Agree a Statement of Work detailing scope, deliverables, timescales and pricing
2. Raise a Call-Off Contract under the G-Cloud framework terms
3. Issue a Purchase Order to confirm commencement

Ensuring transparency and compliance with public-sector procurement regulations, all engagements are delivered in line with G-Cloud framework conditions.

Enquiries or pre-contract discussions can be arranged through our central contact point:

- ✓ tenders@evology.co.uk
- ✓ 01772 450 970