Master Service Agreement

2025/26

map16 | Asset Management

The smart solution to complete asset management.

Master Service Agreement: map16 Asset Management

Effective Date: January 05, 2026
Data Residency: United Kingdom

Governing Law:

This agreement and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed in accordance with the law of [England and Wales OR Scotland OR Northern Ireland]

1. The Service & Access

We provide a secure, web-based platform designed for physical asset and operations management. Enabling holistic, collaborative management of infrastructure assets across owners, contractors, and partners. A modern, platform-based software, with native web and mobile modules, designed to address complex client and contractor challenges. Delivering strategic solutions for asset maintenance and management, supporting the achievement of objectives/outcomes, regulatory compliance, and optimal, whole-life asset performance.

Your subscription includes:

- **Web Interface:** Access to map16 Web dashboards, data visualisation, scheduling and reporting tools. Our mobile application, map16 Mobile, is provided with seamless integration to the map16 Web system.
- **Integration:** Access via API or Web Feature Service (WFS) for GIS and external asset management tools.
- **Security:** All sessions are protected via HTTPS encryption and require valid user credentials.

2. Infrastructure & Performance

We believe in total transparency regarding how your data is handled. Our service is built on professional-grade architecture to ensure your operations never skip a beat.

Hardware & Virtualisation

- **High Performance:** We utilise Intel hardware with SSD RAID 10 configurations for superior data integrity and speed.

- **Isolation:** Using VMware ESXi, we isolate service layers to ensure that a localised issue doesn't impact the broader system.

- **High Availability (HA):** We deploy a VMware HA cluster with mirrored servers. If a primary server fails, your virtual machines will automatically restart on secondary hardware within minutes, ensuring zero data loss.

Service Level Agreement (SLA)

We aim for excellence, not just "good enough."

- **Target Uptime:** We guarantee a 99.9% monthly uptime target.

- **Remedies:** If we fail to meet this target due to a material interruption, we provide a transparent review process. You may be eligible for 'Service Credits' applied to your next billing cycle to ensure our incentives stay aligned with your operational needs.

3. Security & Maintenance

Your data's safety is our primary objective. Our infrastructure partner, Webnetism, helps us maintain a fortress-like environment.

Proactive Protection

- **Perimeter Security:** Managed via industry-standard Juniper firewalls.
- **Backups:** Encrypted backups are performed daily to ensure long-term data longevity.
- **Monitoring:** Our team conducts 24/7 health monitoring to catch and proactively resolve issues before they become system issues for our customers.

Maintenance Protocol

To keep the system optimised, we perform occasional updates:

- **Scheduled Maintenance:** Conducted during low-usage periods (typically weekends or late-night UK time). We will provide a minimum of 3 business days' notice for any planned downtime.
- **Emergency Maintenance:** In the rare event of a critical security threat, we may perform immediate updates. We will notify you as soon as humanly possible.

5. Mutual Responsibilities

For this partnership to work, we both have roles to play:

What we do:	What You do:
Maintain the infrastructure and API uptime.	Maintain the confidentiality of user credentials.
Protect data with encryption and firewalls.	Ensure your third-party integrations (GIS/Tools) are configured correctly.
Provide advance notice for scheduled work.	Notify us promptly of any suspected security breaches on your end.

6. Termination & Fair Exit

We want you to stay because you value the service, not because you're locked in.

- **Termination for Cause:** Either party may terminate this agreement if the other materially breaches these terms and fails to fix the issue within 30 days.

- **Data Return:** Upon termination, we will provide a window of 30 days for you to perform a final export of your data before it is securely purged from our active systems.

7. Service Credits

This **Service Credit Schedule** is designed to provide clear financial accountability. It ensures that if we fall below our 99.9% uptime target, you are automatically entitled to a “make-good” on your subscription costs.

- Service credits are calculated as a percentage of your monthly service fee (or the monthly equivalent of your annual fee) and applied to your next billing cycle.

Monthly Uptime Percentage	**Service Credit Ammount**	**Impact Description**
99.9% – 100%	0%	Standard Service Level Met.
95.0% – < 99.8%	5%	Minor interruption beyond the target.
90.0% – < 94.9%	10%	Significant service degradation.
Below 90.0%	25%	Major service interruption.

Definitions & Terms

- **Monthly Uptime:** Calculated by taking the total minutes in a calendar month, subtracting any "Excused Downtime," and dividing by the total minutes.

- **Excused Downtime:** This includes:

    - **Scheduled Maintenance:** Planned work communicated at least 3 business days in advance.
    - **External Factors:** Issues with the client's local internet connection, internal GIS systems, or third-party API providers not managed by us.
    - **Force Majeure**: Extraordinary events outside of reasonable human control.

The Claim Process

We aim for a **"No Hassle" transparency policy**.

1. **Automated Logging**: Our 24/7 monitoring systems log all outages.

2. **Request:** If you believe we have missed our 99.9% target, simply contact your Account Manager within 30 days of the end of the month in question.

3. **Review:** We will provide a transparent report from our infrastructure logs. If the target was missed, the credit is applied automatically to your next invoice.

4. **Cap**: The maximum total credit for any month is capped at 25% of that month's service fee to ensure we can maintain the resources necessary to fix the underlying issue.

8. Data Privacy & GDPR Compliance

We treat your data with the same level of care we treat our own. As a UK-based provider, we adhere to the highest global standards of data protection.

Our Roles

- **You (The Client):** Are the Data Controller. You decide what data is collected and how it is used.
- **Us (The Provider):** Are the Data Processor. We only act on your documented instructions to provide the service.

Lawful Basis & Transparency

- We process personal data (such as user login info and audit logs) under the lawful basis of Contractual Necessity. For certain security and system-health monitoring, we operate under Recognised Legitimate Interest, as defined by the UK Data (Use and Access) Act 2025.

Key Privacy Commitments

- **Data Residency:** Your data never leaves the UK. All primary storage, backups, and failover systems are located within UK borders to ensure total sovereignty and ease of audit.
- **Minimalism:** We only collect the data necessary to provide the service. We do not engage in “shadow profiling” or sell your data to third parties.
- **User Rights:** We provide built-in tools for you to fulfill Subject Access Requests (SARs), data corrections, or “Right to be Forgotten” requests. Under 2026 UK law, we ensure these processes are “Reasonable and Proportionate” to avoid administrative bloat for your team.

Sub-processors

We only use high-tier infrastructure partners (like Webnetism).

- **Transparency:** A full list of our sub-processors is available upon request.
- **Notification:** We will provide 30 days' notice before adding any new sub-processor. You have the right to object on reasonable data-security grounds.

Data Breach Protocol

In the highly unlikely event of a security incident:

- **Notification:** We will notify you without undue delay (and no later than 48 hours) after confirming a personal data breach.
- **Transparency:** We will provide a detailed report including the nature of the data involved and the steps we are taking to mitigate the impact.
- **Support:** We will assist your Data Protection Officer (DPO) in fulfilling any required notifications to the Information Commissioner's Office (ICO).

9. Data Processing Agreement (DPA)

By using the service, both parties agree to our Standard DPA (Appendix B), which is incorporated by reference. This document provides the detailed “legal plumbing” required by UK GDPR Article 28, ensuring our technical and organisational measures (TOMs) are legally binding.

Personal Data Processing Record

As of January 2026, the following table outlines the specific categories ofpersonal data processed by the service.

Data Category	Specific Elements	Purpose of Processing	Lawful Basis (UK GDPR)	Retention Period
Account Information	Name, Professional Email, Job Title.	To create user profiles and manage platform access.	**Contractual Necessity**	For the duration of the active subscription + 30 days.
Authentication Data	Hashed Passwords, MFA Tokens, Session IDs.	To ensure secure login and prevent unauthorized access.	**Contractual Necessity**	Deleted immediately upon account termination.
System & Audit Logs	IP Address, Browser Type, Timestamps, Actions performed.	To maintain security, provide audit trails for physical asset changes, and troubleshoot.	**Legitimate Interest** (Security & Integrity)	12 months (standard for security audits), then purged.
Asset Metadata	Names of staff assigned to specific physical assets or inspections.	To track accountability and history of physical asset management.	**Contractual Necessity**	Controlled by the Client (can be deleted/anonymized by you).
Support Records	Support tickets, email correspondence, screen captures.	To resolve technical issues and improve service quality.	**Contractual Necessity / Legitimate Interest**	2 years after ticket closure to assist with recurring issues.

Key Data Handling Principles

- **Encryption at Rest & in Transit:** All data listed above is encrypted using HTTPS/TLS while moving across the web and AES-256 encryption while stored on our Intel SSD RAID 10 arrays.

- **No Automated Decision-Making:** We do not use your personal data for profiling or automated “black-box” d ecisions that have legal effects on your users.

- **The “Right to be Forgotten”:** If a user leaves your organisation, you can delete their profile through the admin dashboard. This will immediately obscure their name from active dashboards, though their actions will remain in the encrypted audit logs for 12 months for security and accountability purposes.

- **Hardware Disposal:** In line with our partnership with Webnetism, any retired Intel hardware or SSDs that previously held data are physically shredded or degaussed according to NCSC (National Cyber Security Centre) standards.

10. Acceptable Use Policy (AUP)

To ensure the security, reliability, and integrity of our asset management platform, all users must adhere to this policy.

10.1. Protecting the System

We provide high-performance hardware, and we expect users to respect those resources. You agree **not** to:

- **Stress Test:** Perform unauthorised load testing or penetration testing without prior written consent.
- **Abuse APIs:** Use the API or WFS in a way that exceeds reasonable usage patterns or bypasses our rate-limiting systems.
- **Automated Scraping:** Use “bots” or automated scripts to scrape data from the web interface outside of the provided API/WFS tools.
- **Malicious Code:** Upload any files containing viruses, Trojan horses, or any other software designed to disrupt or damage system functionality.

10.2. Respecting Intellectual Property

Our platform is the result of significant investment in Intel and VMware-based innovation. You agree **not** to:

- **Reverse Engineer:** Attempt to decompile, disassemble, or derive the source code of the web interface or API.
- **Resell:** Rent, lease, or sub-license the service to third parties without an enterprise partner agreement.
- **Copycat:** Build a competitive product or service using similar “look and feel” or proprietary workflows extracted from our platform.

10.3. Account Security & Integrity

The security of our Juniper-protected perimeter depends on user discipline. You agree to:

- **Keep Logins Private:** Never share user credentials between multiple individuals. Each authorised user must have their own unique login.
- **No Impersonation:** Do not attempt to access data you do not have permission to view or pretend to be another user.
- **Reporting:** Notify your internal IT team or our support desk immediately if you suspect a password has been compromised.

10.4. Professional Conduct & Content

As a physical asset management tool, the data stored should be professional in nature. You agree **not** to:

- **Illegal Content:** Store data that is unlawful, defamatory, or infringes on the intellectual property rights of others.
- **Privacy Violations:** Use the platform to store highly sensitive “Special Category” personal data (e.g., medical records) that is not relevant to physical asset management.

10.5. Enforcement & “Fair Warning”

We believe in a transparent and equitable approach to enforcement:

- **Minor Breaches:** If we notice unusual activity (e.g., an API integration is poorly coded and “spamming” our servers), we will reach out to your technical contact to help resolve it before taking any restrictive action.
- **Serious Breaches:** In cases of clear malicious intent, data theft, or a direct threat to system stability, we reserve the right to suspend access immediately to protect the wider environment.

11. Fees, Billing, and Payment Terms

11.1 Subscription Model

The Service is provided on a **per-User, per-week** basis. A “User License” is required for every unique individual authorised to access the web interface or utilise the API/WFS credentials.

11.2 Billing Cycle & Invoicing

- **Advance Billing:** Fees are billed in advance on a monthly cycle, starting from the Effective Date.
- **Payment Terms:** Invoices are due and payable within 30 days of the invoice date.
- **Currency & Taxes:** All fees are quoted in GBP (£) and are exclusive of VAT, which will be added at the prevailing rate.

11.3 Adjusting User Licenses (Scaling)

We believe software should grow with your business.

- **Adding Users:** You may add User Licences at any time through the administrative dashboard. New users added mid-cycle will be charged a pro-rata fee for the remainder of the current billing period and thereafter at the full monthly rate.
- **Reducing Users:** You may reduce the number of licences for the following billing cycle by providing notice via the Customer Service Portal. No refunds or credits are provided for “partial months” or unused licences within a cycle already billed.

11.4 Late Payments & Service Continuity

To ensure the stability of our high-performance Intel/VMware infrastructure, timely payment is essential.

- **Interest:** Fees not paid when due shall accrue interest at a rate of 4% above the Bank of England base rate, or the maximum rate permitted by the Late Payment of Commercial Debts (Interest) Act 1998, whichever is higher.

- **Suspension Grace Period:** If an account is more than **14 days overdue**, we reserve the right to suspend access to the web interface and API. We will provide at least **two (2) email warnings** before suspension occurs to ensure your operational continuity isn't inadvertently disrupted.

- **Reactivation:** A reasonable administrative fee may be charged to reactivate a service that has been suspended for non-payment.

11.5 Fee Adjustments

We commit to price transparency. We will not increase your per-license rate during an active subscription term. We provide at least 90 days' notice of any price changes affecting future renewal periods, allowing you ample time to budget or adjust your requirements.

11.6 Payment Disputes

If you believe there is an error in an invoice, you must notify us in writing within **15 days** of the invoice date. Both parties agree to act in good faith to resolve the discrepancy. While a specific line item is in dispute, you agree to pay all undisputed portions of the invoice on time.

Appendix A: Technical Onboarding Checklist: API & GIS Integration

Phase 1: Connection & Authentication

Before making your first call to our API or WFS, ensure your environment meets these security baselines:

- **[ ] TLS Protocol:** Verify your systems support TLS 1.2 or 1.3 (Standard HTTP is blocked by our Juniper firewalls).
- **[ ] IP Whitelisting:** Provide your static egress IP addresses to our support team for perimeter authorisation.
- **[ ] Credential Management:** Ensure API keys or WFS credentials are stored in a secure vault (e.g., Azure Key Vault, AWS Secrets Manager) and never hard-coded.
- **[ ] MFA Setup:** Confirm all administrative users have enabled Multi-Factor Authentication for the web dashboard.

Phase 2: GIS & Data Standards

To ensure your spatial data renders correctly and remains interoperable with other asset management tools:

- **[ ] Coordinate System:** Standardise on EPSG:27700 (British National Grid) for UK-based projects to ensure sub-meter accuracy.
- **[ ] Format Compatibility:** Confirm your GIS software (e.g., ArcGIS, QGIS) is configured to consume WFS 2.0.0 or GeoJSON for live feature updates.
- **[ ] Attribute Mapping:** Review our “Asset Schema” guide to ensure your local field names (e.g., Install_Date) align with our database parameters.

Phase 3: Performance & Reliability

To maintain our **99.9% uptime** and prevent service degradation during large data syncs:

- **[ ] Batching Strategy:** Configure your scripts to batch POST/PUT requests (e.g., 50–100 records per call) rather than individual requests.
- **[ ] Error Handling:** Implement Exponential Backoff logic for handling 429 (Too Many Requests) or temporary 503 responses.
- **[ ] Rate Limit Awareness:** Check your specific tier's burst and daily limits (typically 1,000 calls per minute).

Phase 4: Security & UK Compliance

As part of our mutual responsibility for UK GDPR and the Data Act 2026:

- **[ ] Data Minimisation: A**udit your integration to ensure only necessary asset fields are being synchronised.
- **[ ] Audit Logs:** Ensure your local systems log the specific user ID associated with every API action for internal traceability.
- **[ ] Breach Protocol:** Update your internal "Incident Response Plan" to include our 48-hour notification window for any detected security events.

Final Verification

- [ ] **Sandbox Test:** Perform a “Dry Run” in the staging environment to verify data mapping without affecting live production assets.
- [ ] **Technical Contact:** Assign a primary “Integration Lead” who will receive notifications regarding planned maintenance or API version updates.

Appendix B: Data Processing Agreement (DPA)

Last Updated: January 05, 2026 **Between:** The “Client” (Data Controller) and the “Provider” (Data Processor).

1. Scope and Purpose

This DPA applies to all personal data processed by the Provider on behalf of the Client while providing physical asset management services. This agreement ensures both parties comply with UK Data Protection Laws, including the UK GDPR and the Data (Use and Access) Act 2025/2026.

2. Processing Instructions

- **Role of Provider:** We process personal data only on your documented instructions. The “Master Service Agreement” serves as your primary instruction.
- **Compliance:** If we believe an instruction violates UK data protection law, we will inform you immediately.
- **Confidentiality:** We ensure that all personnel authorised to process data are committed to confidentiality through binding employment contracts.

3. Technical and Organisational Measures (TOMs)

We agree to implement industry-standard security measures to protect your data against unauthorised access, loss, or destruction. Per our infrastructure specification, these include:

- **Infrastructure Isolation:** Use of VMware ESXi to isolate service layers.
- **Physical Integrity:** SSD RAID 10 configurations for data redundancy.
- **Network Security:** Perimeter protection via Juniper firewalls and HTTPS encryption for all data in transit.
- **Encryption:** All data is encrypted at rest using AES-256 standards.
- **Maintenance:** Daily encrypted backups and 24/7 proactive health monitoring.

4. Sub-processors

- **Authorised Sub-processors:** You grant us a general authorisation to engage sub-processors. Our primary infrastructure sub-processor is Webnetism.
- **Standard of Care:** We impose the same data protection obligations on our sub-processors as set out in this DPA.
- **Right to Object:** We will notify you of any changes to our sub-processors at least 30 days in advance. You may object to such changes on reasonable grounds related to data protection.

5. Data Subject Rights

We will provide you with the technical tools (via the dashboard or API) necessary to fulfil your obligations to respond to requests from individuals exercising their rights, including:

- Right of access (Subject Access Requests).
- Right to rectification or erasure ("Right to be Forgotten").
- Right to data portability.

6. Personal Data Breaches

- **Notification:** We will notify you within **48 hours** of becoming aware of a personal data breach.
- **Documentation:** Our notice will describe the nature of the breach, the categories of data affected, and the remediation steps taken.
- **Assistance:** We will provide reasonable assistance to help you meet your notification obligations to the Information Commissioner's Office (ICO).

7. Data Residency & International Transfers

- **UK Sovereignty:** All personal data is stored and processed on physical servers located within the United Kingdom.
- **No Unauthorised Transfers:** We will not transfer personal data outside of the UK unless specifically instructed by you in writing and only if such transfer complies with UK GDPR adequacy regulations or standard contractual clauses.

8. Audit Rights

- **Information Provision:** We will make available all information necessary to demonstrate compliance with this DPA.

- **Inspections:** We allow for and contribute to audits, including inspections, conducted by you or an independent auditor. Such audits shall occur no more than once per year, with at least 30 days' notice, and must be conducted during business hours to minimise operational disruption.

9. Termination and Deletion

- **Data Return:** Upon termination of the Service, we will provide a 30-day window for you to export your data.

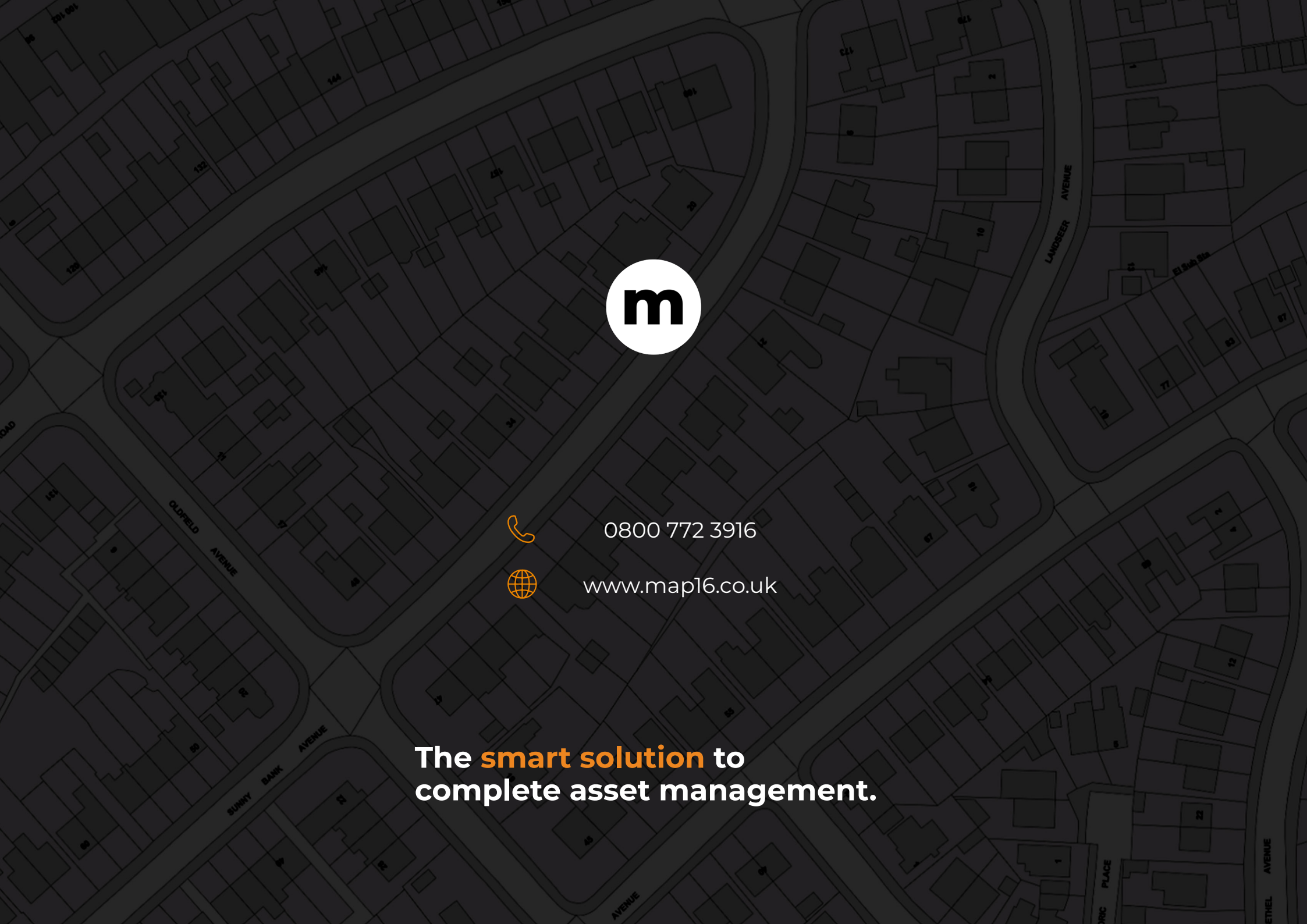
- **Secure Disposal:** Following this window, we will securely delete all personal data from our active systems and backups (unless UK law requires continued storage).

- **Hardware:** Any decommissioned hardware (Intel SSDs) is physically destroyed or degaussed according to NCSC standards.

Annex 1: Details of Processing

- **Subject Matter:** Provision of a web-based physical asset management platform.
- **Duration:** The term of the Master Service Agreement plus 30 days.
- **Nature of Processing:** Collection, storage, retrieval, and visualisation of asset-related data and user logs.
- **Categories of Data Subjects:** Client employees, contractors, and authorised system users.
- **Types of Personal Data:** Names, professional emails, IP addresses, and system activity logs (as detailed in Appendix A of the Terms).

map16 | Asset Management



0800 772 3916

www.map16.co.uk

The smart solution to complete asset management.