

G-Cloud 15

Service Definition

**ENTERPRISE DATA SECURITY AND DATA
MANAGEMENT PLATFORM FOR SALESFORCE
ODASEVA UK LTD**

Lot 2a Infrastructure Software (I-SaaS)

1. Introduction	4
Company Overview	4
Value Proposition	4
What the Service Provides	5
Social Value	6
Overview of the G-Cloud Service	13
Associated Services	14
2. Data Protection	16
Information Assurance	16
Data Back-Up and Restoration	19
Business continuity statement/plan	20
Privacy by Design	21
3. Using the service	23
Ordering and Invoicing	23
Availability of Trial Service	23
On-Boarding, Off-Boarding, Service Migration, Scope etc.	24
Training	26
Implementation Plan	27
Service Management	28
Service Procedures	28
Service Levels	30
Outage and Maintenance Management	31
Financial Recompense Model for not Meeting Service Levels	32
4. Provision of the service	32
Customer Responsibilities	32
Technical Requirements and Client-Side Requirements	33
Outcomes/Deliverables	33
Development life cycle of the solution	34
After-sales Account Management	34
Termination Process	36

5. Our experience	36
Case Studies	36
Clients	38
Contact Details	38

1. Introduction

Company Overview

Odaseva is an Enterprise Data Security Platform company providing data security and data management solutions for organisations using Salesforce. Odaseva is headquartered in Paris, France and operates in 8 countries including the United Kingdom, United States, Canada and Australia. Odaseva was founded in 2012 by Sovan Bin to address the most challenging Salesforce data security use case which was to restore Salesforce data without altering its integrity. Today, Odaseva offers a full suite of solutions which as well as Backup & Restore cover a wide range of use cases including Archiving, Sandbox Seeding, Data Privacy, Encryption and more.

The biggest differentiator of Odaseva is its Zero-Trust approach which is built into the platform. Odaseva has been a No View Provider since its inception ensuring customer data is completely encrypted and protected from risks such as data breaches. Odaseva partners with some of the largest organisations worldwide from the most highly regulated industries like financial services and healthcare as well as non-profit organisations. In the UK, Odaseva is working with customers like Oxfam International and NHS Professionals for whom data security is paramount.

Value Proposition

Odaseva is an enterprise data platform focussed on Salesforce data: securing, managing, archiving, replicating, restoring and ensuring compliance.

Key capabilities include backup and recovery (even decoupled from Salesforce to avoid lock-in) so data is restorable in disasters; data privacy (helping meet GDPR, CCPA, etc.); data management (archiving, housekeeping, dealing with large data volumes) to keep orgs performant; data automation; data seeding & replication across orgs.

Security features: zero-trust architecture, “no-view” provider (even Odaseva cannot see the data in the backups), strong encryption, data residency options.

Odaseva solves challenges around data resilience, governance & compliance, performance of large Salesforce deployments, and reduction of risk (both operational risk from data loss or corruption, and legal/regulatory risk from privacy or security breaches).

- Security, resilience & risk mitigation; Zero-trust architecture, strong encryption, no-view provider, backups that are immutable, etc. Also options to host backup data in specific geographies or bring your own storage (so the public sector can maintain more control). This helps reduce risk of breach, leakage, and non-compliance.
- Compliance pressures (GDPR, data privacy, audits) – Odaseva’s Data Privacy module helps implement policies, ensure sensitive data is handled properly, enforce deletion / retention rules, and auditability. Also features like data residency and BYO-storage help public entities comply with local server / data location requirements.

What the Service Provides

Odaseva technology enables customers to secure and manage their Salesforce data. The platform provides solutions such as Backup & Restore, Archiving, Sandbox Seeding, Data Encryption and Privacy. All solutions provided follow Odaseva’s No View Provider approach to ensure complete protection of all data migrated via Odaseva solutions.

Backup & Restore ensures Salesforce data is stored as an immutable copy that can be restored in the event of data corruption or data loss. Archiving is a cost-effective way to remain within Salesforce data limits by removing data off Salesforce and archiving a copy on the Odaseva platform. Sandbox Seeding enables users to test anonymised production data in a non-production environment for development. Additional tools allow you to encrypt data, audit data, comply with GDPR requests such as the “right to be forgotten” and manage multiple orgs through one platform.

Odaseva offers Managed Backup Services as well as Managed Archiving Services to ensure Salesforce data is backed up and archived according to the customisations of each Salesforce org. A team of Salesforce experts will create a tailored backup and archiving plan to ensure complete coverage of Salesforce data required to be backed up and archived. Additionally, Odaseva provides Expert Services with each of its solutions to ensure Odaseva users can be trained on testing restore scenarios and supported with the implementation of solutions.

Social Value

Make Britain a Clean Energy Superpower

Odaseva is committed to reducing its carbon footprint and supporting climate-positive growth through measurable, realistic, and transparent actions.

1. Business–Travel Emissions

Target: –3 % in business–travel–related emissions.

A Travel Policy limits travel and promotes low-carbon transport and virtual meetings. A carbon assessment has already been completed; it will be renewed in Q2 2026 with our accredited provider to measure progress. In parallel, we will explore becoming more autonomous in calculating and monitoring our own emissions.

2. Supplier Emissions

Target: –5 % across our 30 main suppliers (excluding Salesforce).

We collect their carbon data through a structured questionnaire and support their reduction efforts. Actions and progress will be monitored through our Sustainable Procurement Policy, co-led with Procurement and updated annually.

3. Partnership with Salesforce

Indicative Target: –20 % reduction in emissions related to Salesforce.

A meeting took place in early September 2025. This target depends largely on Salesforce; monitoring will begin once technical data is available.

4. Green IT Programme

Workshops address digital sustainability — internal tools, data storage, and software eco-design.

Target: ~2 % reduction per initiative. Results will be added to our climate roadmap.

5. Monitoring and Governance

An Environmental Dashboard will track key metrics (business travel, supplier progress, Green IT actions, Salesforce results). It will be reviewed annually by the CSR team and shared with clients to ensure transparency and continuous improvement.

Kickstart Economic Growth

1. Commitment Statement

Odaseva is committed to promoting economic equality by creating fair opportunities across its supply chain, supporting skill development in high-growth sectors, and contributing to a more diverse and inclusive digital ecosystem.

2. Method Statement

a. Supply Chain Diversification

Objective: Integrate more SMEs, start-ups, and social enterprises (e.g. adapted companies) into Odaseva's procurement process.

Actions:

Include supplier diversity and prompt-payment criteria in all tenders.

Introduce a social impact dimension in supplier evaluations through the upcoming Supplier Code of Conduct.

b. Employment and Skills Development

Objective: Enhance access to jobs and professional training in data protection, cloud, and cybersecurity.

Actions:

Deliver continuous internal cybersecurity awareness training.

Build partnerships with universities and training organisations to host interns and apprentices (1–2 in 2025, expansion planned in 2026–2027).

Maintain the Buddy Mentoring Programme, pairing senior employees with juniors and new graduates.

Encourage expert participation in inclusive tech initiatives (e.g. Women in Tech, Salesforce Talent Alliance).

c. Governance and Transparency

Progress will be monitored via Odaseva's CSR dashboard, tracking:

% of SME/social-impact suppliers,

% of employees trained in cybersecurity,

number of interns/mentees supported.

3. Timed Project Plan & Monitoring

Phase	Key Action	Lead	KPI / Target
Q1 2025	Supply-chain audit	Procurement	% of SMEs identified
Q2 2025	Publish Supplier Code of Conduct	CSR & Legal	Code issued to 100 % of suppliers
Q3 2025	Launch mentoring & internship programme	HR	1–2 apprentices onboarded

Q4 2025	Internal communication of first social-impact results	CSR	Results shared company-wide
2026 → 2027	Annual review & continuous improvement	CSR & Procurement	+5 % SME partners / +10 % staff trained

Through these measures, Odaseva will ensure equitable access to opportunities, transparent reporting, and measurable social impact throughout contract delivery.

Break Down Barriers to Opportunity

1. Commitment Statement

Odaseva is committed to promoting equal opportunity in employment and training, reducing inequalities linked to gender, disability, or background, and preventing exploitation or unfair practices across its operations and supply chain.

Our approach focuses on inclusive employment, accessible skills development, and modern slavery prevention.

2. Method Statement

a. Inclusive and Fair Employment

Objective: ensure fair, transparent, and accessible employment practices.

- Maintain a non-discrimination HR policy across all sites.
- Apply the annual pay-gap analysis in France with corrective action plans.
- Ensure digital accessibility of recruitment tools, intranet, and HR processes.

b. Skills Development and Progression

Objective: enable progression for all employees, including underrepresented groups.

- Build an inclusive training module covering unconscious bias, accessibility, and inclusive management.
- Implement in 2026 structured career development pathways, supporting both role and international mobility.
- Expand cross-mentoring between technical and functional roles.

c. Modern Slavery Risk Prevention

- Require supplier adherence to the Supplier Code of Conduct (anti-slavery clauses).
- Train Procurement and Legal teams to detect risk indicators.
- Monitor the confidential whistleblowing channel and escalation process transparency.
- Publish a Modern Slavery Statement in the 2026 CSR Report.

3. Timed Project Plan & Monitoring

Phase	Key Action	Lead	KPI / Target
Q1 2026	Diversity & accessibility audit	HR	Internal report delivered
Q2 2026	Supplier Code of Conduct published	Legal & Procurement	100% supplier adherence
Q3 2026	Inclusion & bias training for managers	HR	33% managers trained
Q4 2026	1st Equality & Diversity Report	CSR	Report shared internally

2026→2027	Annual review & improvement	CSR & HR	Pay gap reduction, diversity progress
-----------	-----------------------------	----------	---------------------------------------

4. Influence & Outreach

Odaseva will promote its commitments through its CSR reporting, encourage suppliers to align with the same ethical standards, and participate in inclusive tech initiatives within the Salesforce ecosystem.

Build an NHS fit for the Future

1. Commitment Statement

Odaseva is committed to supporting the physical, mental, and social wellbeing of its workforce by providing a safe, inclusive, and balanced working environment.

Our wellbeing strategy focuses on three priorities:

- Health and mental wellbeing,
- Work–life balance and hybrid flexibility,
- Community engagement and collective cohesion.

2. Method Statement

a. Health and Mental Wellbeing

All employees have free and confidential access to the TriNet Employee Assistance Program (EAP), which provides 24/7 counselling, life coaching, and stress management resources.

- In France, employees benefit from Malakoff Humanis health and prevention coverage, including medical support and mental health assistance.
- Odaseva’s workforce can access Salesforce Trailhead training modules on wellbeing, mindfulness, nutrition, and financial health.
- Psychosocial and ergonomic risks are monitored through the DUERP 2025 risk–prevention framework.

- An annual internal communication campaign consolidates all wellbeing and health resources (EAP, Trailhead, medical support, HR guidance).

b. Work–Life Balance and Safe Work Environment

- Odaseva applies its Hybrid Workplace Policy v2023, allowing two to three days of remote work per week and individual flexibility for medical or family reasons.
- The Code of Conduct v1.9 ensures mutual respect, anti-harassment measures, and safe working conditions.
- The Social and Economic Committee (CSE) and internal Fireside meetings promote regular employee dialogue and engagement tracking.

c. Community Engagement

- Odaseva’s CSR programme includes blood donations, tree-planting, sports inclusion, and recycling with Emmaüs.
- Employees are encouraged to volunteer or mentor through CSR and Salesforce.org initiatives.

3. Timed Project Plan & Monitoring

Phase	Key Action	Lead	KPI / Target
Q1 2026	Annual wellbeing & health communication	HR & CSR	100% staff informed
Q2 2026	Manager training on mental health prevention	HR	20% trained
Q3 2026	Employee engagement survey	HR	≥80% participation

Q4 2026	CSR report publication	CSR	Wellbeing data published
---------	------------------------	-----	--------------------------

Through these initiatives, Odaseva ensures measurable, transparent, and lasting wellbeing for its employees and partners.

Overview of the G-Cloud Service

Odaseva is an enterprise data management and data security platform specifically designed for complex, large-scale Salesforce environments or environments that require advanced security.

Our product offerings are divided into two main suites: Data Security and Data Management.

1. Data Security Suite

This suite focuses on protecting data and ensuring compliance.

- **Data Backup & Restore** | Provides best-in-class data protection with capabilities like real-time RPO (Recovery Point Objective) and RTO (Recovery Time Objective), allowing end-users to instantly restore field values and recover from data loss scenarios quickly.
- **Data Archiving** | Enables long-term, compliant storage of inactive Salesforce data, which helps reduce data storage costs and manage Large Data Volumes (LDV) without performance issues.
- **Data Encryption** | Secures sensitive data both in transit and at rest, often extending the capabilities of Salesforce Shield with patented no-view architecture and Zero Trust principles.
- **Data Masking** | Automatically anonymizes or masks Personal Health Information (PHI) or other sensitive data in non-production environments (like Sandboxes) to ensure data confidentiality and compliance while accelerating development.
- **Data Privacy** | Provides tools to manage complex data privacy regulations (like GDPR and CCPA), including the ability to automate data deletion requests for compliance.

- **Data Trail** | Offers comprehensive audit history by tracking every single change, insert, and deletion on all Salesforce fields and objects for up to 10+ years, critical for SOX, HIPAA, and other compliance mandates.

2. Data Management Suite

This suite focuses on scaling operations and improving data quality across organizations.

- **Data Seeding** | Accelerates DevOps and testing by populating Sandboxes with realistic, relevant, and privacy-compliant data.
- **Data Replication** | Easily and efficiently moves data from Salesforce to external cloud platforms or data lakes, enabling analytics and business intelligence outside of the CRM.
- **Org Portability** | Supports large-scale, complex transformations like Org splits, mergers, and migrations by managing data movement with governance and security.

Data Automation | Allows users to build, automate, and schedule complex data operations, such as data standardization and aggregation, reducing reliance on manual developer support.

- **Multi-Org Insights** | Provides a centralized view and enhanced governance across a distributed Salesforce environment (multiple Orgs), offering actionable insights into business metrics and platform performance.

Each suite and its products can be purchased separately or bundled. Please refer to pricing for details.

Overall Benefits: Odaseva is trusted by the world's most regulated companies to ensure their Salesforce data is safe, compliant, and ready for AI by delivering a scalable, secure, and customizable platform built to handle Large Data Volumes.

Associated Services

Odaseva provides a powerful Enterprise Data Platform for Salesforce and also offers a variety of specialized associated services to ensure successful

implementation, compliance, and ongoing data management for large, complex organizations.

These associated services fall primarily into two categories:

1. Managed Services

These services offer hands-on, outsourced management of the Odaseva platform to ensure optimal performance and adherence to security standards without straining internal IT resources.

- **Managed Backup Services (MBS):**
 - **Customization and Configuration:** Odaseva experts design, configure, and optimize a backup plan tailored to the client's specific Salesforce implementation, use cases, and complex data model.
 - **Monitoring and Optimization:** They continuously monitor the backup plan, check for anomalies, and ensure the lowest possible use of Salesforce API calls to prevent system slowdowns.
 - **Restore Readiness:** The service ensures that the backup data is always in a state of readiness for recovery, meeting defined RTO and RPO targets.
 - These services are included in the price of the licence
- **Residency-as-a-Service:**
 - A critical compliance service that guarantees data is stored and processed in compliance with specific regional requirements (e.g., EU, Australia, Canada), a necessary feature for global enterprises dealing with regulations like GDPR.
 - These services may incur an additional cost, depending on the location of where the data needs to be stored

2. Expert/Professional Services

These services involve engaging Odaseva's Technical Architects and data security experts for advisory, audit, and implementation support on highly

specialized projects. These services are provided at an additional cost based on the scope of the project.

- **Advisory Expert Services:**
 - **Disaster Recovery Planning:** Assistance in creating and validating comprehensive, auditable data recovery plans.
 - **Archiving Strategy:** Consulting on a long-term strategy for data retention, deletion, and archiving to manage Large Data Volumes (LDV) and ensure compliance.
 - **Restore Readiness Audits:** Assessing the organization's ability to successfully recover data, pinpointing potential barriers, and providing tailored recommendations.
- **Implementation Services:**
 - **Hands-on Implementation:** Direct support for implementing complex features like Data Masking, Sandbox Seeding, Cloud Replication, and complex data privacy workflows.
 - **Training and Enablement:** Providing training to internal teams to help them become self-sufficient in managing the platform and implementing future use cases internally.
 - **Custom Automation:** Guidance and execution support for setting up tailored, sophisticated data automations to accelerate time-to-value.

2. Data Protection

Information Assurance

Security Accreditations and Certificates:

Odaseva maintains a robust set of security accreditations, certifications, and compliance standards, managing information safely through defined processes and policies.

Odaseva has achieved or maintains compliance with the following security frameworks and certifications:

- **ISO 27001:2022 – Information Security Management System (ISMS) – Certified by E&Y**

- SOC 2 Type II – System and Organization Controls 2 – Audited by E&Y
- HITRUST r2 – Health Information Trust Alliance Common Security Framework (CSF) – Certified by Coalfire
- IRAP – The Australian Information Security Registered Assessors Program (IRAP) – Audited by CyberCX
- HDS – Hébergeur de Données de Santé – Certified by E&Y
- TISAX – Trusted Information Security Assessment Exchange – Certified by E&Y
- CSA STAR (Level 1): Cloud Security Alliance (Self-Assessment)

Processes and Facilities for Managing Information Safely:

Odaseva relies on a shared responsibility model, leveraging certified third-party facilities while applying strict internal controls and processes to secure data.

Data Security: Customer data at rest is protected using customer owned and managed encryption keys (AES-256). Odaseva employees and its third party service providers do not have access to the customer data since they do not have access to the keys. Data in transit is encrypted using TLS 1.2+.

Data Hosting (Facilities): Odaseva's architecture extends the security offered by Salesforce, AWS, and Azure. Odaseva relies on the physical security measures implemented by its cloud providers. The platform front end is hosted on Salesforce secure infrastructure. Underlying data centers (AWS and Azure) are managed by these third parties.

Protective Monitoring: The Security team annually reviews compliance reports (e.g., SOC 2, ISO 27001) of critical vendors to verify logical and physical security measures. Logs sent by providers are surveilled to detect anomalies indicative of malicious acts. A File Integrity Monitoring (FIM) tool is implemented to notify administrators of unauthorized changes to the production environment. A SIEM tool is in place to centralize log collection and enable monitoring.

Change Management: Changes to information systems and facilities are subject to formal Change Management procedures. All changes are logged and controlled using tools (e.g., JIRA). Changes are tested and formally approved before migration to production. Development, testing, and production environments are separated and secured.

Vendor Risk Management: Odaseva assesses and manages risks associated with critical vendors (redacted). Confidentiality provisions are included in contracts/terms & conditions for vendors hosting customer data. Monitoring of supplier security practices and service delivery occurs regularly.

Personnel Security: Background verification checks on all candidates for employment and contractors are carried out prior to joining the organization, proportional to the business requirements and perceived risks, complying with ISO 27001 (A.7.1.1 Screening).

Policies and Standards:

Regulatory and Industry Framework Compliance: Odaseva's processes and controls align with several international regulations and industry-specific mandates: For example

- GDPR (General Data Protection Regulation)
- HIPAA (Health Insurance Portability and Accountability Act of 1996)
- CCPA (California Consumer Privacy Act)
- ACSC IRAP (Australian Cyber Security Centre Information Security Manual) requirements
- NIST SP 800-53 Rev. 5 (used as a reference framework for security controls)
- Australian Privacy Act 1988

Odaseva maintains comprehensive, formally documented policies and procedures (which adhere to the ISMS framework) to

manage information security and compliance. (For example, Data Classification and Encryption Policy, Incident Management Procedure, Vulnerability and Patch Management Procedure, Security Policy, Account Management Procedure, etc).

The complete listing of and the policies are available upon request.

Data Back-Up and Restoration

Odaseva provides an Enterprise-grade Backup and Restore solution designed specifically for Salesforce data, metadata, and files. Our Intelligent Backup Plan automates the protection of customer environments with configurable frequency, scope, and retention options, ensuring data resilience against loss or corruption.

As a standard, full backups are performed once a week and incremental backups every four hours, providing near-continuous protection. Customers also have the possibility to define higher-frequency backups for critical objects based on their operational needs. This service can be subject to an additional cost. Customers retain full control over what is backed up, with the flexibility to include or exclude specific objects, files, and metadata. All backups are encrypted in transit and at rest, and the Managed Services team proactively monitors and maintains backup plans to ensure reliability, performance, and compliance with best practices.

Odaseva operates as a No-View Provider, meaning that customer data remains fully encrypted and inaccessible to Odaseva staff. In the event a restoration is needed, customers can rely on Odaseva's intuitive Restore Wizard, which guides users step-by-step through restoration options from granular record-level restores to full-environment recoveries. Our Support team is also available to assist at any time through a ticket opened directly from the Odaseva platform.

Specific customer requirements (e.g., custom backup frequencies, retention policies, or compliance configurations) can be discussed and agreed upon prior to order placement and reflected in the Order Form, and will also be reviewed in detail during onboarding with the Managed Backup

Services (MBS) team to ensure proper configuration and alignment with business needs.

Business continuity statement/plan

Odaseva maintains a comprehensive Business Continuity Policy (BCP) and related Disaster Recovery Plans (DRP), which are designed and audited annually as part of our SOC 2 Type II and ISO 27001 compliance.

Scope of the Plan: The BCP scope centrally covers the development, provision, maintenance, and customer support of the Odaseva Platform and its supporting processes. It applies to all staff and contracted workers. The plan specifically addresses information systems containing highly critical information assets, including protected health information, and systems supporting business critical processes (e.g., Internal CRM, source code repository). Non-critical systems, services, and functions are deemed out of scope.

Key Business Areas and Critical Functions: Critical functions are organizational streams and associated assets identified through an annual Business Impact Analysis (BIA). The primary critical functions requiring recovery plans are related to the continuous delivery of platform services, including:

1. Platform Front-end operations (Salesforce).
2. Platform Back-end operations (AWS and Microsoft Azure data storage/compute).
3. System and data backup plans, adhering to the Recovery Point Objective (RPO).

Dependencies between Areas and Functions: The Business Continuity Management (BCM) process requires the identification of events that can cause interruptions to business processes, along with their probability and impact. Critical functions rely heavily on underlying infrastructure provided by three main specialists: Amazon Web Services (AWS), Salesforce, and Microsoft Azure. The BCP process assesses internal and external business dependencies and reviews contractual agreements in place to manage these risks.

Acceptable Downtime (RTO): The Business Continuity Management (BCM) process establishes the Maximum Tolerable Downtime (MTD), which dictates the acceptable loss the business stakeholders are willing to incur from an outage. This MTD is aligned with the required Recovery Time Objective (RTO), which guides staff on the time frame specified for recovery and restoration of operations.

Maintaining Operations: Odaseva's strategy relies on Prevention, Mitigation, and Recovery controls.

- **Proactive Prevention:** The architecture uses redundant, secure, and hardened hosting in cloud infrastructure (IaaS). The infrastructure is based entirely on an autoscaling plan, and critical AWS components are replicated across multiple Availability Zones (AZs).
- **Recovery and Testing:** DRPs are established to restore operations and ensure the availability of information at the required level and in the required time scales following interruption. Corrective actions include the activation of failover systems, backup restoration, and security measures (e.g., IP blacklisting, credential removal). The BCPs and DRPs are formally tested annually, including restoration tests of backups, to ensure they meet the RTO.
- **Incident Response:** Odaseva maintains a comprehensive Incident Reporting Process to triage incidents, ensuring stakeholders have quick access to information and tracking corrective/preventive action plans (CAPA)

A more detailed plan can be provided to the buyer on request.

Privacy by Design

Odaseva proactively embeds privacy and security into the core of its platform design and operations to adhere to the requirements of the EU General Data Protection Regulation (GDPR) and other global privacy laws, emphasizing the concept of Privacy by Design.

Odaseva's commitment to security-first design is central to its platform, accommodating stringent industry regulations, including the GDPR.

1. "No-View Provider" Architecture: Odaseva operates as a "No-View Provider". This means that Odaseva employees and public cloud providers cannot see customer data. The architecture is specifically designed with technical safeguards that prevent access to clear text customer data, including Personally Identifiable Information (PII) and Protected Health Information (PHI).
2. Granular Encryption (BYOK): Data privacy is ensured by encrypting customer data at rest using customer-created encryption keys ("Bring Your Own Key" or BYOK). The data is encrypted at the column/file/field-level using AES-256 encryption. This logical separation of customers' data is key to ensuring confidentiality.
3. Data Minimization and Retention: Odaseva supports the Data Minimization principle by instructing employees to collect, store, and process only necessary PII. Odaseva mandates that data should be kept no longer than necessary, and employees must define and enforce Data Retention policies for purging data afterwards.
4. Dedicated Privacy Products: Odaseva offers specific products to accelerate compliance and address privacy requirements:
 - Data Privacy: Covers confidentiality by enforcing data lifecycle policies and allows processing Data Subject Requests for data access and erasure.
 - Data Anonymizer: Accelerates development and testing without compromising customer data privacy laws.
 - Salesforce API Firewall and Zero Trust Data Encryption: Provides end-to-end encryption and data masking, securing data extraction and ultra-sensitive data storage.

Adherence to GDPR Requirements:

- **Legal Compliance:** Odaseva acts as a Data Processor, processing data only in accordance with the Customer's documented instructions.
- **Data Subject Rights:** Customers can process Data Subject Requests via the Data Privacy feature.
- **Data Protection by Design:** Odaseva implements processes to integrate privacy considerations into the design of systems and processes from the outset, known as Privacy by Design.
- **Security of Processing:** Odaseva ensures data security via TLS 1.2+ for data in transit and AES-256 encryption for data at rest, utilizing BYOK.
- **Data Residency:** Odaseva provisions architecture pods globally to offer strict Data Residency, ensuring customer data does not cross national borders as defined in the residency requirements.
- **DPO and Accountability:** A Data Protection Officer (DPO) is responsible for the Data Protection program. Employees must ensure accountability and auditability, and consult the DPO to update the data processing register.

3. Using the service

Ordering and Invoicing

The client can get in touch with Odaseva (alliance@odaseva.com) to review requirements and discuss options. Based on the client specifications and criteria, the Odaseva AE will provide a quote with all details to the client. The client can then verify: prices, descriptions, products, bill to / ship to address, reference to MSA, potential special terms, etc. Then an Order Form which is basically the approved quote with the Order status must be signed by the client in order for Odaseva to trigger the provisioning of the subscription and services.

Availability of Trial Service

Odaseva offers prospective clients the ability to test their use cases in Proofs of Concept (PoCs). These PoCs can take the form of in-depth workshops or guided sessions (typically over a 2-4 week period) in

which the client can actually get their hands on the Odaseva platform in order to confirm a technical fit with their requirements. Generally, POCs are provided at no extra cost.

Prior to starting a PoC, Odaseva and the prospective client would need to agree upon the key success criteria for the exercise. The client is able to use their own Salesforce sandbox for the PoC (or Odaseva can provide a test one) along with their own datasets, and Odaseva will provide supporting materials such as detailed test paths for common scenarios, video guidance, access to the Knowledge Base and the technical support team, in addition to one or more experts who will lead the guided sessions.

On-Boarding, Off-Boarding, Service Migration, Scope etc.

Onboarding:

- Our onboarding process begins with a formal Kickoff to align on objectives, followed by detailed planning and provision of all necessary documentation.
- Our onboarding process is managed by our MBS (Managed Backup Services team). The goal is to quickly achieve operational independence and compliance readiness. • **Mandatory Documentation:** We provide comprehensive documentation, including platform recommendations based on an initial Salesforce organization audit, ensuring your teams have the necessary resources to maintain and optimize backup plans and compliance processes.
- For Client above £10K / year we provide a dedicated Client Success Manager (CSM) at no extra cost. The CSM can help with:
 - **Guided Implementation & Configuration:** The CSM facilitates workshops and provides expert guidance to configure the Odaseva platform specifically for your needs, including addressing any unique Salesforce organization requirements.
 - **Comprehensive Training:** We deliver formal, tailored training sessions focused on platform operation, configuration, and development best practices. This includes specialized instruction on restorability readiness and data operations.

- Business Continuity Planning (BCP): The CSM assists in the implementation and testing of your BCP, ensuring robust data security and management from day one.
 - The CSM remains the contact for ongoing support and acts as the escalation point for any platform performance or operational issues.
- Our Enterprise Support team is also engaged to initialize, run, monitor, optimize, and maintain your backup plan on behalf of your organization.
- Optional dedicated Advisory Hours delivered by our Expert Services can also be purchased for on-demand expert guidance, and can be used flexibly throughout a contracted period (typically one year). Additionally, our Premier Success Plan includes 24/7 support with a 2-hour response time, designated Workshops, and Architect Credits for optimization. This is provided and an extra cost.
- Comprehensive documentation is provided during the planning phase, including Restore execution plans, prioritized remediation plans, Quick Start Guides, and interpretation of detailed audit results.
- Formal training sessions are included in our standard onboarding process to enable customers to run the Odaseva platform independently. Additional advanced training is available and provided to clients and their partners at an additional cost, to empower your center of excellence. It covers implementation of Business Continuity Plans, audit tools, and best practices.
- Our team assists in configuring, initializing, and optimizing the backup plan, as well as implementing optional features such as Salesforce Sandbox Seeding and Zero Trust Connect. We partner with customers throughout the engagement to ensure timely go-live and knowledge transfer.

Off-boarding:

The process of off-boarding from Odaseva involves several key steps:

- The end-of-contract process is designed to ensure the customer retains control and access to their data.
- Odaseva will align with the GC15 termination procedures.

- Upon initiation of termination, Odaseva engages with the client to outline the off-boarding process and formulate a plan for data retrieval and migration.
- All customer data available on the Odaseva platform at the time of termination is provided for export. The ability to retrieve or export data is guaranteed upon termination of service. After data export, Odaseva destroys all customer data, including backups, within 30 days.
- Documented procedures exist for the voluntary and involuntary termination of users, including removal of logical and physical access to resources and the return of company-owned equipment.
- For a period of 15 days before the contract's expiry or termination date, customers can download their data directly via the Odaseva portal at no additional cost. Customers can export their data in Salesforce-readable formats, such as packaged CSVs and files, ensuring compatibility and ease of migration to alternative solutions.
- Should the customer require access immediately after the contract ends, they have a further 15 days from the effective termination date to request a final data retrieval. Upon this request, we will reactivate the portal for 10 days at no cost, allowing for the final download of all customer data.
- After 10 days following the end of the contract, we delete or destroy all copies of the customer's data held within our systems, unless we are legally required to retain it. Customers remain responsible for confirming their data has been successfully retrieved prior to this final deletion date.

Off-boarding costs

- Odaseva Expert Services shall provide reasonable off board services according to the off boarding plan at no additional cost. Advanced support beyond the standard procedure will be chargeable, as per our pricing document.

Training

Odaseva provides formal training sessions and support as part of our standard onboarding process for new customers, enabling them to

operate the Odaseva platform independently. Our onboarding includes assistance from our Enterprise Support team, who initialize, run, monitor, optimize, and maintain backup plans on behalf of customers. This approach accelerates ramp time and reduces backup TCO costs.

Additionally, Odaseva Expert Services are available to audit Salesforce organizations for backup and restore readiness, offer tailored recommendations, document restore execution plans, and deliver additional training to empower customer teams. These services facilitate comprehensive orientation to the new service. For ongoing assistance, customers have access to the Odaseva Knowledge Base available on the platform, which provides step-by-step guidance and online help. Odaseva Expert Services are provided at an extra cost, please see pricing for additional details.

Implementation Plan

A detailed implementation plan from Odaseva can be provided to the buyer on request. It includes a comprehensive outline of the tasks and responsibilities required to keep the solution operational. This encompasses technology deployment, organizational alignment, and process integration. We provide Odaseva Data Protection Backup, Odaseva Data Protection Ultra Availability, Odaseva Governor Limit Monitoring, and Odaseva Archiving for Performance.

Our Managed Backup Services can be combined with fee-based Expert Services to extend customer support and guidance, including audit tools to ensure alignment with best practices for restoration and disaster recovery.

Customers are expected to define their organization, prepare a Disaster Recovery Plan, undergo training on Odaseva technology, apply best practices for recoverability in Salesforce design, and maintain the Disaster Recovery Plan with each major release. Odaseva collaborates closely with customers throughout the implementation process to ensure all such requirements are met and the solution is fully integrated and operational.

Service Management

Odaseva service is managed through comprehensive policies and procedures aligned with industry-leading standards, focusing on rigorous controls for security, availability, capacity, and change management.

Service Procedures

The service procedures define operational boundaries regarding availability, changes, and customization:

- **Availability and Maintenance:** Odaseva provides real time information about the platform availability, prior incidents if any and scheduled maintenance windows ahead of time on our Trust public site.
- **Capacity Management:** Odaseva monitors resources (storage, CPU, RAM) and manages capacity demand, implementing auto-scalability processes on Azure and AWS infrastructure to adjust processing power based on business needs. Critical AWS system components are replicated across multiple Availability Zones and backups are maintained.
- **Changes:** Major planned changes are communicated ahead of time to customers via the platform.
- **Customization:** Odaseva is a SaaS service that is common to all customers but also offers some configuration options for securing the platform and for using the services.

Odaseva's management system is structurally aligned with several international standards and includes numerous procedures that align with ITSM principles:

- **Information Security Management System (ISMS):** Odaseva implements and manages an ISMS aligned with ISO 27001 and HITRUST CSF ISMP guidelines. The ISMS is based on multiple frameworks and regulations, including ISO 27001, SOC 2, GDPR, ACSC iRap, HDS, HIPAA, and HITRUST.

- Service Management Processes: Odaseva maintains specific documented policies and procedures relevant to service management, including for example:
 - Incident Management Procedure: Defines procedures to manage incidents (including security incidents) and minimize their impact. An incident is defined, referencing ITIL, as "an unplanned interruption to an IT service or reduction in the quality of an IT service or a failure".
 - Change Management: Handled via the Software Development Lifecycle (SDLC) Policy, which addresses configuration management.
 - Business Continuity Policy: Developed and maintained to facilitate efficient response to emergencies and situations that could damage operations or critical information systems. Business continuity plans must be tested and updated regularly, at a minimum annually.
 - Audit Logging and Monitoring Procedure: Defines how monitoring and logging activities are conducted.
 - Odaseva platform maintains a Knowledge Base to help customers with configuration and setup, and provide answers to frequently asked questions.
- Our organization focuses on comprehensive security and compliance, as proven by our ISO 27001:2022, SOC 2 Type II, and HITRUST r2 certifications. These standards collectively assure that our service management processes are highly secure, reliable, and compliant with key industry regulations. More information about our certification has been provided in this document in the section "Information Assurance".
- Odaseva is committed to providing exceptional customer support through a highly skilled global team. The company employs Technical Architects (often holding Salesforce CTA certifications) and expert data management professionals with deep technical skills and enterprise-level experience. With specialized assistance across its three service teams—Managed Backup Services, Expert Services, and Customer Success Services—Odaseva ensures that

customers receive tailored guidance, advanced technical support, and rapid solutions for any data management issues they might face.

Service Levels

The standard support availability for the Odaseva Platform is 24/5. This operational window is defined as from Monday 9 am to Friday 6 pm.

Support hours vary based on the selected Success Plan:

- Enterprise Plan: Support Hours are 24/5.
- Premier Plan: Support Hours are 24/7.
- Signature Plan: Support Hours are 24/7

The support initial response time is defined contractually based on the case Severity Level and is tied to the customer's Success Plan (Enterprise, Premier, or Signature) .

The definitions and corresponding initial response times for each severity level are detailed below:

Severity Level	Definition	Enterprise (Initial Response Time)	Premier (Initial Response Time)	Signature (Initial Response Time)
Severity 1 (Urgent)	Production issue affecting all users; system unavailability	3 Hours	2 hours	1 hour
Severity 2 (High)	Persistent issue affecting many users; major functionality is impacted	6 Hours	4 hours	3 hours
Severity 3 (Normal)	System performance issue or bug affecting some but not all users	24 Hours	18 hours	12 hours

Severity 4 (Low)	Inquiries about routine technical issues; information requests on application capabilities, navigation, or configuration	48 Hours	36 hours	24 hours

Outage and Maintenance Management

Odaseva maintains a comprehensive Business Continuity Policy (BCP) and related Disaster Recovery Plans (DRP), which are designed and audited annually as part of our SOC 2 Type II and ISO 27001 compliance.

Scope of the Plan: The BCP scope centrally covers the development, provision, maintenance, and customer support of the Odaseva Platform and its supporting processes. It applies to all staff and contracted workers. The plan specifically addresses information systems containing highly critical information assets, including protected health information, and systems supporting business critical processes (e.g., Internal CRM, source code repository). Non-critical systems, services, and functions are deemed out of scope.

Key Business Areas and Critical Functions: Critical functions are organizational streams and associated assets identified through an annual Business Impact Analysis (BIA). The primary critical functions requiring recovery plans are related to the continuous delivery of platform services, including:

1. Platform Front-end operations (Salesforce).
2. Platform Back-end operations (AWS and Microsoft Azure data storage/compute).
3. System and data backup plans, adhering to the Recovery Point Objective (RPO).

Acceptable Downtime (RTO): The BCM process establishes the Maximum Tolerable Downtime (MTD), which dictates the acceptable loss the business stakeholders are willing to incur from an outage. This

MTD is aligned with the required Recovery Time Objective (RTO), which guides staff on the time frame specified for recovery and restoration of operations.

Maintaining Operations: Odaseva's strategy relies on Prevention, Mitigation, and Recovery controls.

A more detailed plan can be provided to the buyer on request.

Financial Recompense Model for not Meeting Service Levels

Odaseva does not offer service, monetary nor time credits. Our service levels are that we commit to certain uptime percentages, and, depending on the Success Plan a customer purchases, we commit to certain response times based on the severity of the issue. All SLAs focus on giving customers quick access to senior Odaseva officers in case of issues.

4. Provision of the service

Customer Responsibilities

Such responsibilities are outlined in the 'Customer Obligations' Section of our Master Service Agreement.

During the implementation process with Odaseva, customers are responsible for defining their organization, preparing a Disaster Recovery Plan, getting trained on Odaseva technology, and applying best practices of recoverability in the design of their Salesforce environment. Customers must also maintain the Disaster Recovery Plan with each major release.

Odaseva provides technology solutions, managed backup services, expert services, and audit tools to guide customers through these processes and ensure alignment with best practices that facilitate restoration operations.

Regarding termination, Odaseva will align with the GC15 termination procedures.

Technical Requirements and Client-Side Requirements

[As outlined in our Master Service Agreement] The solution is network accessible from mobile devices, laptops, and workstations, supporting all access methods and platforms that Salesforce supports. Odaseva does not have a standalone mobile app. Clients will need to run any Salesforce Cloud (Salesforce Public Sector Solutions, Sales, Service or Industry clouds) that run on Hyperforce, the backbone of Salesforce's modern architecture (Core).

No local client needs to be deployed.

Customers must define their organization, prepare a Disaster Recovery Plan, get trained on Odaseva technology, apply best practices of recoverability in the design of Salesforce, and maintain the Disaster Recovery Plan at each new major release.

Odaseva provides technology such as Odaseva Data Protection Backup, Odaseva Data Protection Ultra Availability, Odaseva Governor Limit Monitoring, and Odaseva Archiving for Performance, as well as Managed Backup Services and Expert Services.

Customers are expected to allocate resources including people and time to ensure proper organization, process definition, and ongoing maintenance.

All specific system requirements and resource provisions should be documented in the Order Form as agreed between both parties prior to placing an order.

Outcomes/Deliverables

Odaseva's service provides the following deliverables, outputs, and outcomes to the client:

- Managed Backup Service operations, including initialization, monitoring, optimization, and maintenance of backup plans, as well as assistance with specific backup-related tasks such as pausing plans or retrieving backups.
- Multiple backup options: full backups, incremental backups (scheduled as frequently as every 5 minutes), and differential

backups for files and binaries, ensuring flexible and efficient data protection.

- Data is available for download in CSV format throughout the subscription period and for 30 days after termination, with no charge for download.
- Detailed security logs covering platform interactions, user activities, and security-related events, accessible via the platform and exportable in CSV format.
- Release notes and documentation with each update, training sessions, webinars, and dedicated customer success engagement to keep customers informed and prepared for platform changes and new features.
- Support for disaster recovery and restoration, including assistance from the Support and Expert Services teams to retrieve the correct snapshot and define recovery strategies.
- Audit tools and expert guidance to detect misalignment with best practices, support organizational process definition, and maintain disaster recovery readiness.
- Access to Odaseva's modular, scalable backend architecture, designed for enterprise-grade compliance and high availability, with customizable deployments to meet regulatory and operational requirements.

Development life cycle of the solution

We use agile methodology, a project management approach that uses an iterative, flexible process to deliver projects in small, incremental steps, emphasizing continuous collaboration, adaptability, and customer feedback. Instead of a single, detailed plan, Agile breaks projects into short cycles called "sprints" where teams plan, execute, and review their work, allowing them to quickly adapt to changes and improve their product or service over time.

After-sales Account Management

Odaseva builds and maintains customer relationships through several key practices:

- Communication channels for product updates and maintenance include release notes, documentation, training sessions, webinars, and a dedicated service status portal (trust.odaseva.com). Customers are proactively notified of updates, scheduled maintenance, and any potential service disruptions.
- Odaseva provides dedicated customer success engagement, enabling organizations to leverage new features and best practices as they become available, and supports customers with guidance and expert services to optimize their use of the platform.
- In the event of platform performance issues, customers can contact support@odaseva.com. The larger clients (with licences higher than £10K/year) can request further escalation from their Customer Success Manager or Account Executive, ensuring prompt resolution and continued satisfaction.
- Odaseva continuously innovates by aligning its roadmap with Salesforce, delivering monthly product releases, and engaging customers through training and webinars. This approach fosters long-term business relationships and enables growth by keeping customers at the forefront of technological and regulatory advancements.
- Odaseva actively solicits customer feedback through business reviews, dedicated surveys, and user group meetings. This input is a critical component of product planning, ensuring that the product roadmap and service delivery are directly informed by customer needs and experiences.
- To ensure we're constantly meeting and exceeding our customers' expectations, we conduct regular Customer Satisfaction (CSAT) and Net Promoter Score (NPS) surveys. These surveys are essential tools that allow us to systematically gather feedback across the entire customer journey. The results provide quantitative data on how happy customers are with our products, services, and support, and identify our most loyal advocates, which directly informs our strategic decisions, product improvements, and service delivery standards.

Termination Process

Odaseva will align with the GC15 termination procedures. Upon contract termination, all backup data available on the Odaseva platform at the time will be provided to the customer, and the data will be delivered in Salesforce readable format (packaged CSVs and files).

The customer has the right to retrieve or export their data upon termination of service. There are no fees that the customer must incur at the end of the service.

The customer acknowledges purchasing the Services with Term and Renewal Term(s) as defined in the Certificate or Order Summary.

5. Our experience

Case Studies

CASE STUDY 1

Odaseva Helps Service New South Wales Government in Australia (NSW) Simplify Complexity

The Odaseva case study details how Service NSW, the single point of contact for New South Wales government services, used the Odaseva platform to address complex Salesforce data retention and compliance challenges.

The Challenge: Service NSW manages two large Salesforce Orgs and was struggling with complex data models, varying regulatory retention periods (ranging from two to ten years), and the need for a new enterprise-grade backup solution after Salesforce's own service was discontinued. Ensuring mandatory data classification and retention for compliance was paramount.

The Solution: After a thorough market evaluation, Service NSW selected Odaseva. The decision was based on its ability to offer a holistic data protection solution that simplified complexity. Key criteria met by Odaseva included its ease of use, comprehensive data retention features, and the availability of a local Sydney-based support team.

The Outcome: Implementing Odaseva allowed Service NSW to shift from actively managing backups to simply monitoring daily reports and dashboards. The agency now possesses a reliable, enterprise-grade system for fast and precise data backup and restoration. Ultimately, the solution provided the CRM Platform Manager with "peace of mind" and the trust needed to ensure all data residency, governance, and compliance requirements are consistently met.

CASE STUDY 2

How Accenture and Odaseva helped Dallas County Protect Salesforce Data

The case study outlines how Dallas County Health and Human Services (DCHHS) partnered with Accenture and Odaseva to proactively secure its vast volume of Salesforce data, particularly sensitive Personal Health Information (PHI) collected during the COVID-19 pandemic.

The Challenge: As a technology-forward public health department serving over 2.6 million people, DCHHS needed a powerful, reliable backup and restore solution for its new Salesforce CRM to prevent data loss or corruption, a need intensified by the sudden influx of PHI during the pandemic response.

The Solution: Accenture conducted a technical evaluation and recommended Odaseva due to its proven track record in protecting highly-sensitive data for government agencies and large enterprises.

The Outcome: The implementation of Odaseva significantly enhanced DCHHS's data security by automating backup and restore processes, which reduced manual effort and potential downtime. This automation strengthened their disaster recovery plan and increased trust in the Salesforce platform, as they could now quickly prove data restorability. DCHHS plans to expand its use of Odaseva for Data Anonymization and Data Archiving to further comply with regulatory requirements and automate tasks.

Clients

The Largest Salesforce Customers Trust Odaseva



Contact Details

Include contact details of the person responsible for G-Cloud leads, should a buyer have any other queries.

G-Cloud Contact person: Gonzalo Higuera Hare, VP alliances EMEA

Email: alliance@odaseva.com

Mobile number: +33 749 57 71 41