responsiv

simple · effective · distinctive

Sovereignty Assessment

Responsiv Cloud

Report

Commercial in Confidence

Information in this document shall not be disclosed outside of your organisation and shall not be duplicated, used or disclosed in whole or in part for any purpose other than to evaluate the document, provided that if a contract is awarded to Responsiv as a result of, or in connection with, the submission of this document, you shall have the right to duplicate, use or disclose the information to the extent provided in the contract. This restriction does not limit your right to use information contained in the document if it is obtained from another source without restriction.

Disclaimer

Observations and recommendations included in this document are based on our opinions, experience, and meetings with you. They are as objective and representative as we can reasonably be, however, they do not take account of information that you may have but was not shared with us for the purpose of constructing this report. Responsiv makes no representation as to accuracy or fitness for purpose. Once you have chosen a course of action, it should be thoroughly evaluated to ensure its fitness for purpose.

Copyright

This document may contain intellectual property that pre-dates our engagement with your company and that remains the property of Responsiv Solutions Limited.

Obligation

This document is not an offer or contract. Neither Responsiv nor you have any obligations or liability to the other unless our authorized representatives enter into a separate definitive written agreement. Terms included in this document are not binding unless they are included in such a written agreement.

Table of Contents

INTRODUCTION 5
ASSESSMENT 5
THIS ASSESSMENT 5
Sovereignty Score Method 5
ASSESSMENT FINDINGS 6
Sovereignty Assessment 6
SOV-1 STRATEGIC SOVEREIGNTY 7
[10] Decisive Authority lies inside the UK/EU 7
[10] Non-UK/EU Finance Obligations 7
[10] EU/UK Value Creation 7
[5] EU/UK Initiatives 7
[10] Ability to sustain services 7
SOV-2 LEGAL & JURISDICTIONAL SOVEREIGNTY 8
[10] Governing Legal System 8
[10] Exposure to non-UK/EU laws 8
[5] Exposure to channels for access to data 8
[5] Data transfer restrictions 8
[10] Intellectual Property 8
SOV-3 DATA & AI SOVEREIGNTY 9
[10] Data Access 9
[10] Data Access Monitoring 9
[05] AI Model usage 9
[10] Data Located in UK/EU Locations 9
[00] AI Development Independence 9
SOV-4 OPERATIONAL SOVEREIGNTY 10
[10] Exit Planning 10
[10] UK/EU Support 10
[10] UK/EU Support Legal Jurisdiction 10
[10] Responsiv Escrow Service 10
[10] Decisive Authority lies inside the UK/EU 10
SOV-5 SUPPLY CHAIN SOVEREIGNTY 11
[08]Component Supply Locations 11
[08] Software Origins 11
[05] Reliance on non-UK/EU suppliers and vendors 11
[05] Supply chain visibility 11
SOV-6 TECHNOLOGY SOVEREIGNTY 12
[10] Integration and Standards 12
[02] Open Licenses 12
[02] Internal Software Visibility 12
SOV-7 SECURITY & COMPLIANCE SOVEREIGNTY 13
[7] Dependence on UK/EU Specialist Hardware 13
[08] UK/EU and internationally recognized certifications 13

[05] Adherence to GDPR, NIS2, DORA, and other EU frameworks 13
[10] UK/EU Security Operations 13
[10] Security Breach Reporting 13
[02] Customer Security Audit 14
SOV-8 Environmental Sustainability 15
[10] Energy Efficiency 15
[10] Circular Economy 15
[10] Transparency 15
[10] Renewable Sourcing 16
REFERENCES 17
APPENDIXES 17
Hosting and Datacentre 17
Redcentric 17
Hardware Suppliers / Vendors 17
Software Suppliers / Vendors 18

Introduction

This assessment describes how the Responsiv Cloud and associated Cloud Services measure up to Sovereignty Objectives defined by the European Commission "Cloud Sovereignty Framework" Version 1.2.1 October 2025 and relevant for the provision of Cloud services requested in this procedure.

The European Cloud Sovereignty Framework draws from initiatives including (1) CIGREF's Trusted Cloud Referential v2, (2) Gaia-X policy rules and architecture, (3) the European Cybersecurity Certification Framework (ENISA, NIS2, DORA). They also lean on international practice in export controls, supply chain resilience, and security auditability.

The "Cloud Sovereignty Framework" specifies a set of objectives to supplement security assurance requirements with sovereignty-specific safeguards defining clearly what sovereignty means.

Assessment

The "Cloud Sovereignty Framework" requires the contracting authority to assess the level of assurance provided by the cloud service supplier for each of the Sovereignty Objectives. Each assessment will establish a Sovereignty Effectiveness Assurance Level (SEAL) to be used as a Minimum Assurance Level for each objective.

A Sovereignty Score may be calculated to provide an overall assessment that is complementary to the minimum individual objective assessments.

This Assessment

This report is provided by Responsiv to illustrate our assessment of the Cloud Platforms and Services that we provide. It is not intended to replace your own assessment but does provide some of the information required for you to do so. Please contact Responsiv for more information.

Responsiv Score assessment is indicated in square brackets beside each question.

Sovereignty Score Method

The Sovereignty Score is computed according to the formula shown here. The maximum score is set to be 50 points, to allow 10 points per question in each section. Section weights are provided by the Cloud Sovereignty Framework.

$$Sovereignty\ Score = \sum_{n-1}^{n=8} \frac{Score(Sov_n) * Weight(Sov_n)\%}{MaxScore(Sov_n)}$$

Assessment Findings

These findings are arranged against the categories defined in section 4, Assessment of Sovereignty Effectiveness of the Cloud Sovereignty Framework, Version 1.2.1, October 2025.

Sovereignty Assessment

Details of each section and question are in the rest of this assessment report. Our assessment is based on our current understanding of the questions and intended to illustrate the general score. Specific cloud services may change the dynamic by adding or removing suppliers. Responsiv can respond to specific requirements and needs, for example arranging for government clearances.

Sovereign Requirement	Weight	Assessment	Weighted Score	Max Score
SOV-1 Strategic Sovereignty	15%	**50**	15%	50
SOV-2 Legal & Jurisdictional Sovereignty	10%	**40**	8%	50
SOV-3 Data & AI Sovereignty	10%	**35**	7%	50
SOV-4 Operational Sovereignty	15%	**50**	15%	50
SOV-5 Supply Chain Sovereignty	20%	**26**	13%	40
SOV-6 Technology Sovereignty	15%	**14**	7%	30
SOV-7 Security & Compliance Sovereignty	10%	**42**	8.4%	50
SOV-8 Environmental Sustainability	5%	**40**	5%	40
Calculated Sovereignty Score			**78.4%**	

SOV-1 Strategic Sovereignty

[10] Decisive Authority lies inside the UK/EU

Ensuring that bodies having decisive authority over your services are located within EU/UK jurisdiction and evaluating the assurances against change of control.

Responsiv Cloud compute, storage, backups, and service engineering are hosted across two datacentres and the Responsiv Offices. All locations are based in the UK and operate under UK jurisdiction and legal frameworks.

Responsiv rely primarily on the following suppliers to provide cloud services.

Class	Supplier	Dependency	Jurisdiction
1	Responsiv Solutions Limited	Primary Contract, Service Engineering, Support	England, UK
1	Redcentric	Hosting services, datacentre locations, physical network services, physical security, hardware maintenance.	Italy, EU
2	Proxmox	Virtualisation Software, Software Defined Networking, virtual firewalls.	Austria, EU
2	IBM Corporation	Software Components, Security, Process, Data, Integration	New York, USA
2	Hewlett Packard Enterprise	Hardware compute, storage	Texas, USA
2	Fortinet Inc	Firewalls	California, USA
2	Redhat	Operating Systems	North Carolina, USA
2	Open-source	Monitoring and Management	Global
2	Postgres	Data management	Global
2	Keycloak	Security Management	
2	NGINX	Security Protection	

All operational control, access to data, and physical positioning is based in the UK and relies immediately on resources controlled in the UK or Europe. Hardware devices and other equipment is sourced from companies that fall under the jurisdiction of the United States. See Appendix for detailed information about each supplier.

[10] Non-UK/EU Finance Obligations

Degree to which the provider relies on financing coming from EU/UK sources. Responsiv has no reliance on funding that originates with companies outside the UK or European jurisdiction.

[10] EU/UK Value Creation

Extent of investment, jobs, and value creation within UK/EU. Responsiv Cloud operations are performed in the UK/UE jurisdiction and employ skilled engineering staff as well as office, security, cleaning, and facilities staff to support those operations. Cloud Services are assembled and/or developed in the UK.

[5] EU/UK Initiatives

Involvement in EU initiatives, Consistency with digital, green, and industrial sovereignty objectives defined at EU level. Responsiv is ISO 14001 certified and endeavours to select low carbon, low polluting, low energy solutions where available and viable. Our hosting provider (Redcentric) has multiple

[10] Ability to sustain services

Ability to sustain secure operations against requests to cease or suspend the service, or if vendor support is withdrawn or disrupted. The Responsiv Cloud can sustain secure operations if the class-1 suppliers listed above are willing and able to continue to provide their respective services. Class-1 suppliers are under sole UK/EU jurisdiction and as such subject to UK/EU legislation.

- Requests to cease or suspend the service from actors authorised by UK/EU law to make such requests will be resisted to the extent of the law of the country but may be overwhelming.
- Requests to cease or suspend the service from actors outside the EU and with no jurisdiction or legal right to request such an action cannot legally compel the class-1 suppliers.
- Vendor support may be withdrawn or disrupted by class-1 suppliers. In this case the Responsiv Cloud Services cannot be relied upon to sustain secure operations.
- Vendor support may be withdrawn or disrupted by class-2 suppliers. In this case Responsiv Solutions is confident that cloud service can be relied upon to sustain secure operations.

SOV-2 Legal & Jurisdictional Sovereignty

[10] Governing Legal System

The national legal system governing the provider's operations and contracts.

Responsiv Cloud is governed by the UK legal system as it applies to cloud services, and to extra-territorial acts such as SOX and DORA as they apply to specific service provision.

[10] Exposure to non-UK/EU laws

Degree of exposure to non-EU laws with cross-border reach (e.g., US CLOUD Act, Chinese Cybersecurity Law).

[5] Exposure to channels for access to data

Existence of legal, contractual, or technical channels through which non-EU /UK authorities could compel access to data or systems.

[5] Data transfer restrictions

Applicability of international regimes, which may restrict usage or transfer.

[10] Intellectual Property

Location of intellectual property creation, registration, and development (EU vs. third countries), legal jurisdiction where IP is created and developed.

SOV-3 Data & AI Sovereignty

[10] Data Access

Ensuring that only the customer, not the provider, has effective control over cryptographic access to their data.

Responsiv uses data encryption for data that is resident on disk and when it is in flight. Customers can bring their own certificates for data encryption and can integrate the Responsiv Cloud Security Service into their own identity stores and certificate authorities. This means that Responsiv administrators have access to the software infrastructure but cannot read the data managed by those systems.

[10] Data Access Monitoring

Visibility into when, where, and by whom data is accessed, including auditability of AI model usage, mechanisms guaranteeing irreversible removal of data, with verifiable evidence.

Visibility of data access is dependent on cloud service. In all cases and by default the security system / reporting system records session start and completion for each user and the resources they have used. This activity does not have sight of the data, which remains encrypted.

Responsiv Cloud Data Compliance Service

Additional controls can be implemented using the Responsiv Cloud Data Compliance Service to record all access to data, including when, where, and by whom data is accessed. This service can be used to implement regulatory controls required for SOX compliance and similar regulations. The service requires encryption keys and will store information encrypted such that only the customer has access.

[05] AI Model usage

Monitoring AI model usage with regards to sovereignty involves ensuring that data ingestion, training, inference, and model outputs remain under local, regional, or organizational jurisdiction, preventing unauthorized access or data leakage. It requires an approach that extends data storage to include auditing AI workflows and managing dependencies.

Responsiv AI Services

Responsiv AI services and AI embedded in Responsiv Cloud Services is stored locally on the Responsiv Cloud (region pinned to UK) or in a location specified by the customer. Some Cloud Services allow external AI services to be attached, which has the effect of moving data and control away from the Responsiv Cloud. Responsiv use IBM Watson and Open Source on premises to retain full control. Contact Responsiv for information about specific AI services, including our arrangements for:

- Model Lineage & Provenance: Track the lifecycle of the model from training to fine-tuning and deployment to maintain a clear record of its provenance and compliance.
- Anomaly Detection: Use tools that alert on unusual behavior, such as data drift (a shift in data distribution) or data egress patterns that suggest data leakage.
- EU AI Act Compliance: Utilize frameworks like COMPL-AI to document AI usage, risk classification, and accountability.

[10] Data Located in UK/EU Locations

Strict confinement of storage and processing to European jurisdictions, with no fallback to third countries.

Responsiv Cloud services store data in their local datacentre and backup to an alternate datacentre for location recovery. Both locations are in the UK and operate under the laws of that jurisdiction.

[00] AI Development Independence

Extent to which AI models and data pipelines are developed, trained, hosted, and governed under EU control, minimizing dependency on non-UK/EU technology stacks.

No Information.

SOV-4 Operational Sovereignty

[10] Exit Planning

Ease of migrating workloads or integrating with alternative UK/EU controlled solutions without vendor lock-in.

Responsiv Cloud agreements allow data to be extracted and moved to alternate service providers. Responsiv can support this activity for a service charge as agreed in our engagement contracts. Data may be extracted, transformed, and loaded to alternate solutions subject to product constraints and tooling.

[10] UK/EU Support

Capacity for UK/EU operator to manage, maintain, and support the technology without requiring non-UK/EU vendor involvement and existence of an EU/UK-based talent pool with the expertise to operate and sustain the service.

Responsiv Service Engineering is based in the UK and operates under the UK legal system. The team have all the skills needed to operate the Cloud Services and Responsiv Cloud. Our hosting supplier (Redcentric) are also UK based and have the hardware and networking skills to provide all the support needed to maintain a secure operational service. No organisations outside the UK/EU area are required to maintain the operational service.

The Responsiv Cloud Service Engineering team are recruited from the UK workforce and demonstrate that the skills are available in that jurisdiction. The technologies used to deliver the cloud services are well understood by many IT developers and administrators in the UK and Europe.

[10] UK/EU Support Legal Jurisdiction

Assurance that operational support is delivered from within the EU/UK and subject exclusively to EU/UK legal frameworks.

All Operational Support is delivered primarily from the Responsiv Offices in Bracknell UK with additional support as needed from Redcentric UK support locations.

[10] Responsiv Escrow Service

Availability of full technical documentation, source code, and operational know-how enabling long-term autonomy.

Responsiv provide non-sensitive documentation to customers as requested. Sensitive information and proprietary source code is arranged to allow it to be made available under conditions defined in our standard terms and conditions.

[10] Decisive Authority lies inside the UK/EU

Location and legal control of critical suppliers or subcontractors involved in service delivery. See SOV-1.

SOV-5 Supply Chain Sovereignty

[08]Component Supply Locations

Geographic source of key physical parts, manufacturing location - countries where hardware is manufactured or assembled. And jurisdiction and provenance of embedded code controlling hardware, firmware.

Class	Supplier	Dependency	Jurisdiction
2	Hewlett Packard Enterprise	Hardware compute, storage	Texas, USA
2	Fortinet Inc	Firewalls	California, USA

[08] Software Origins

Origin of Software: where and by whom software is architected and programmed, location and jurisdiction governing software packaging, distribution, and updates.

Class	Supplier	Dependency	Jurisdiction
2	Proxmox	Virtualisation Software, Software Defined Networking, virtual firewalls.	Austria, EU
2	IBM Corporation	Software Components, Security, Process, Data, Integration	New York, USA
2	Hewlett Packard Enterprise	Hardware compute, storage	Texas, USA
2	Redhat	Operating Systems	North Carolina, USA
2	Open-source	Monitoring and Management	Global
2	Postgres	Data management	Global
2	Keycloak	Security Management	
2	NGINX	Security Protection	

[05] Reliance on non-UK/EU suppliers and vendors

Degree of reliance on non-UK/EU vendors, facilities, or proprietary technologies.

The Responsiv Cloud Services rely on software and hardware that originates outside UK/EU jurisdiction. That software is purchased, managed, and operationally supported by Responsiv. This means that a vendor refusing to support the software will not have an immediate impact on the service and is highly unlikely to undermine our ability to deliver a secure and robust service in the medium term.

All foundational cloud components are replaceable, and the cloud services are designed in a modular fashion that allows all elements to be replaced independently.

Individual cloud services may rely on proprietary software that cannot be replaced like for like using another vendor. Such software is licensed under partnering agreements, managed, and supported by Responsiv. Data can be extracted to be moved to alternative vendors, which may require transformation to complete migration.

[05] Supply chain visibility

Visibility into the entire supplier and sub-supplier chain, including audit rights.

Software vendors have audit rights to confirm running instances and capacity. They do not have the right to investigate data, or to access software owned by other vendors, Responsiv, or the customer.

Responsiv consider that our visibility for immediate vendors is good to excellent and our relationships with the primary vendors is good. We cannot accurately judge the sub-supplier arrangements for hardware. For software we believe that all components are royalty free and therefore controlled by the primary supplier.

SOV-6 Technology Sovereignty

[10] Integration and Standards

Ability to integrate with other technologies through well-documented and non-proprietary APIs or protocols, extent to which the solution adheres to publicly governed and widely adopted standards, reducing dependency on single vendors.

Responsiv Cloud services that are designed to integrate with other systems and technologies provide excellent connectivity and are well documented. The interfaces conform to well documented standards where appropriate.

[02] Open Licenses

Whether software is accessible under open licenses, with rights to audit, modify, and redistribute, ensuring transparency and adaptability.

Responsiv Cloud Software cannot be acquired through open licenses, cannot be redistributed, and the customer does not have a right to audit under our standard terms and conditions. Contact Responsiv for more information and special terms.

[02] Internal Software Visibility

Visibility into the design and functioning of the service, including architectural documentation, data flows, and dependencies

Responsiv Cloud cannot be investigated, and the customer does not have a right to investigate under our standard terms and conditions. Contact Responsiv for more information and special terms.

SOV-7 Security & Compliance Sovereignty

[7] Dependence on UK/EU Specialist Hardware

Degree of EU independence in high-performance computing capabilities, including processors, accelerators, and software ecosystems.

Responsiv Cloud Services generally do not depend on specialist high performance computing hardware. Specific Services, for example AI based services may require specialist hardware. Contact Responsiv for more information.

[08] UK/EU and internationally recognized certifications

Attainment of EU and internationally recognized certifications (e.g., ISO, ENISA schemes)

Identifier	Name	Short Description
ISO/IEC 27001	Information Security Management Systems	A framework for managing risks to the confidentiality, integrity, and availability of information assets, covering both digital and physical data. This standard helps organizations protect sensitive information, such as employee and client details, intellectual property, and financial data. It involves a risk-based approach to secure information in any form, including digital files and physical documents.
ISO 9001	Quality Management Systems (QMS)	Sets out requirements for consistent product/service quality and enhanced customer satisfaction, focusing on process management and continuous improvement. Enables organizations to meet customer requirements consistently, streamline operations, and enhance competitiveness. It is suitable for any industry and emphasizes continuous improvement (PDCA cycle).
ISO 14001	Environmental Management Systems (EMS)	Provides a structure for identifying, managing, and reducing the environmental impact of business operations, including waste management and sustainability. Guides organizations in improving their environmental performance through more efficient resource use, waste reduction, and compliance with environmental laws.
ISO/IEC 20000-1	IT Service Management System (ITSM)	Specifies requirements for establishing, implementing, and improving a Service Management System (SMS) to deliver reliable, high-quality IT services. Establishes a system to ensure IT services meet business and customer needs, offering structured processes (often aligning with ITIL) for incident handling, service delivery, and management.

[05] Adherence to GDPR, NIS2, DORA, and other EU frameworks

Responsiv adheres to GDPR for all data handling activity and DORA for in scope Open Banking and Open Finance cloud services.

Responsiv adheres to ISO 27001 and UK regulations as they overlap with NIS2

[10] UK/EU Security Operations

Security Operations Centres and response teams operating exclusively under EU/UK jurisdiction, control over security monitoring/logging - customer or EU/UK authority ability to oversee logs, alerts, and monitoring functions directly.

The Responsiv Cloud Security Operations monitoring and response is based in Bracknell UK and operates entirely under UK jurisdiction.

[10] Security Breach Reporting

Transparent, timely, and EU-compliant reporting of breaches or vulnerabilities, maintenance Autonomy - ability to develop, test, and apply security patches independently of non-EU vendors.

The Responsiv Cloud Development Operations is in Bracknell UK and can apply security patches and maintaining the cloud foundation and cloud services independently of other organisations subject to vendor patch availability.

Security weaknesses identified to require patching but that do not have patches available can be mitigated by additional barriers and controls that can be designed and implemented by Responsiv independently of the specific software vendor. This means additional application firewall rules and inbound traffic inspection, removal of access, and other security measures.

[02] Customer Security Audit

Capacity for EU entities to perform independent security and compliance audits with full access.

Responsiv Cloud cannot be investigated, and the customer does not have a right to investigate under our standard terms and conditions. Contact Responsiv for more information and special terms.

SOV-8 Environmental Sustainability

[10] Energy Efficiency

Adoption of energy-efficient infrastructure (e.g., low PUE) and measurable improvement targets.

Redcentric Reading and Byfleet data centres demonstrate ISO 14001-aligned environmental management by achieving a high-efficiency 1.14 Power Usage Effectiveness (PUE), well below the 1.57 industry average. They utilize 100% renewable energy, advanced cooling technologies (free air, liquid), and strict, monitored, and optimized, operational, controls to minimize environmental impact.

Key aspects of their energy-efficient, ISO 14001-compliant operations include:

- **Operational Control & Monitoring:** Implementation of strict environmental management systems (EMS) to monitor hot spots, maintain ISO certification, and ensure continuous improvements in energy usage.
- **Cooling Optimization:** Utilization of advanced techniques such as cold aisle containment, higher temperature set-points, and re-engineered chiller systems to reduce energy consumption.
- **Infrastructure Efficiency:** Data centres in Reading and Byfleet use 100% renewable energy sources (solar, wind, hydro) and support high-density, efficient colocation, significantly reducing carbon footprints.
- **Performance Metrics:** Achieving a PUE of 1.14, demonstrating highly efficient energy usage compared to industry averages.

These efforts reflect a commitment to sustainability, reducing energy waste, and supporting ESG initiatives for their customers.

[10] Circular Economy

Circular economy practices ensuring reuse, refurbishment, and responsible end-of-life treatment of hardware.

Redcentric Reading and Byfleet data centres demonstrate a circular economy approach to hardware by prioritizing longevity, energy efficiency, and waste reduction. They utilize advanced, efficient cooling to extend equipment lifespan, operate on 100% renewable energy, and focus on maximizing the operational life of hardware, reducing the need for premature replacements.

Key elements of their approach include:

- Hardware Longevity & Efficiency: Infrastructure is designed or managed to maximize life cycles, supported by energy-efficient cooling (free air and liquid cooling).
- Sustainable Infrastructure: The Byfleet site, specifically, focuses on density, ISO-certified racks aimed at sustainable, efficient operation, while both locations, including Reading, leverage 100% renewable energy.
- Reduced Environmental Impact: By focusing on energy efficiency (low PUE of 1.14) and potentially reducing the need for frequent hardware refreshes, they minimize the "take-make-dispose" impact.

[10] Transparency

Transparent measurement and disclosure of carbon emissions, water usage, and other sustainability indicators.

Redcentric Reading and Byfleet data centres demonstrate transparent measurement and disclosure of sustainability indicators through comprehensive ESG reporting, adherence to rigorous standards, and the adoption of low-emission, high-efficiency infrastructure. By utilizing a location-based methodology for emissions reporting rather than just a market-based one, Redcentric ensures consistent year-on-year transparency of its energy and carbon performance.

Redcentric uses the EcoVadis sustainability portal to publish comprehensive, independently verified ESG data. Sustainability efforts are tracked through TCFD (Task Force on Climate-related Financial Disclosures) frameworks and ESOS (Energy Savings Opportunity Scheme) reports. The company holds quarterly ESG committee meetings with operational board members to review risks, obligations, and progress on targets.

The sites utilize modern infrastructure, including cold-aisle containment and, in some cases, innovative chemical-free water treatment systems to optimize efficiency. The facilities support high-density, AI-ready workloads while maintaining a focus on energy efficiency.

Key Sustainability Metrics and Disclosure (Reading & Byfleet)

- **Carbon Emissions & Energy Use:** Redcentric publishes detailed carbon reduction plans that include full Scope 1, 2, and 3 emissions calculations. They have adopted a location-based approach, which allows for accurate tracking of actual energy consumption and emission improvements over time.
- **Efficiency Metrics (PUE):** The facilities are recognized for high efficiency, with a reported Power Usage Effectiveness (PUE) of 1.14, which is significantly better than the European industry average of 1.8.
- **Renewable Energy:** The Byfleet and Reading data centres are powered by 100% renewable energy, sourced from solar, wind, and hydro.
- **Water Usage Transparency:** Redcentric has demonstrated commitment to water efficiency by adopting advanced adiabatic cooling towers that utilize evaporation and are working toward incorporating Water Usage Effectiveness (WUE) reporting, in alignment with Climate Neutral Data Centre Pact (CNDCP) targets, aiming for compliance by 2040.

[10] Renewable Sourcing

Sourcing of renewable or low-carbon energy to power infrastructure and operations

Redcentric Reading and Byfleet data centres are powered by 100% renewable energy sourced from wind, solar, and hydro, with a commitment to sustainable sourcing maintained since 2011. The facilities further minimize their environmental impact through high-efficiency infrastructure—including adiabatic cooling and high-efficiency UPS systems—and plans for on-site solar generation. Learn more about Redcentric sustainability initiatives at Redcentric.

References

Cloud Sovereignty Framework, Version 1.2.1, October 2025

Appendixes

Hosting and Datacentre

Redcentric

Milan, 28 May 2024 – WIIT S.p.A. ("WIIT"), one of the leading European players in the market of Cloud Computing services for enterprises focused on the provision of continuous Hybrid Cloud and Hosted Private Cloud services for critical applications, notes the announcement by Redcentric of 24 May 2024.

WIIT S.p.A., a company listed on the Euronext Star Milan ("STAR") segment, is a leader in the cloud computing market. The company has a pan-European footprint and is present in key markets such as Italy and Germany, positioning itself among the main operators in the provision of innovative Hosted Private and Hybrid Cloud technological solutions. WIIT operates its own data centres in 6 regions - 4 in Germany and 2 in Italy - of which 2 are Premium Zone-enabled, i.e. with Tier IV data centres certified by the Uptime Institute and with the highest levels of security in the design phase.

https://investors.wiit.cloud/files/press_release/wiit-statement-regarding-redcentric-eng.pdf

Hardware Suppliers / Vendors

Hewlett Packard Enterprise (HPE)

Hewlett Packard Enterprise (HPE) hardware manufacturing is globally distributed, with key assembly locations strategically situated to serve regional markets. Primary manufacturing hubs are in the Czech Republic (Kutná Hora) for Europe, India, China, and the United States (Chippewa Falls, Wisconsin).

In response to growing demands for data sovereignty, HPE has expanded its manufacturing footprint to include Riyadh, Saudi Arabia, focusing on producing ProLiant Gen11 servers locally. While final assembly occurs in these diverse locations, key physical components—such as processors (Intel/AMD), memory, and storage—are sourced from a complex global supply chain predominantly based in Asia-Pacific, with increasing efforts to validate sourcing through secure supply chain programs.

The embedded code, firmware, and management systems controlling HPE hardware—most notably the Integrated Lights-Out (iLO) technology—are largely developed and managed under US jurisdiction, with significant engineering resources also based in India. To establish provenance and security, HPE employs a "silicon root of trust," which anchors the firmware directly into the chipset, validating code integrity before the operating system boots. For sensitive applications, HPE offers a "Trusted Supply Chain" initiative where servers are assembled in the US by vetted personnel to ensure the integrity of the firmware and prevent the insertion of malicious code. This approach aims to provide 360-degree visibility, with firmware security measures aligning with standards such as NIST SP 800-147B and NIST SP 800-193.

Fortinet

The Fortinet FortiGate 90G hardware series is designed and engineered by Fortinet, Inc., a US-based corporation headquartered in Sunnyvale, California. While the company maintains a global presence, key hardware components and manufacturing assembly, including the sourcing of proprietary Security Processing Unit (SPU) ASIC chips, frequently involve locations in Asia, with specific commercial listings indicating China as a place of origin for FG-90G hardware.

The firmware (FortiOS) controlling the FortiGate 90G hardware, along with its security services, has its core development and provenance in the United States and Canada. The Operating System and control code are developed by Fortinet, with security operations and threat intelligence managed by their global FortiGuard Labs. The firmware undergoes signed validation to prevent unauthorised code, and the company adheres to a secure development lifecycle, ensuring that the jurisdiction of the software development and intellectual property remains under US-led control, while components are assembled globally.

Software Suppliers / Vendors

Responsiv Software

Responsiv Software is designed and developed in the UK. Responsiv Cloud Services are assembled from software developed primarily by the vendors listed here. Established in 2015, the company is privately owned and free from venture capital influence.

IBM Integration Software

IBM MQ and App Connect Enterprise (ACE) are premium middleware products primarily developed by IBM's software laboratory in Hursley, United Kingdom, which serves as a major hub for integration and messaging technology

. While the core development and architectural stewardship originate from the UK, key software parts are assembled globally, leveraging IBM's international development centres, with significant engineering resources in the USA, India, and China. The software is engineered to be platform-agnostic, designed, and assembled for deployment on Windows, Linux, and Unix systems, as well as being packaged for containerised environments like Red Hat OpenShift.

Regarding jurisdiction and provenance, IBM MQ and ACE are intellectual property of IBM Corporation, a multinational corporation headquartered in Armonk, New York, USA. Therefore, the primary jurisdiction for the IP rights is the United States, and licensing agreements often operate under US laws, although they are sub-licensed globally. The products are generally considered to be of US provenance but developed within a global supply chain that adheres to international quality and security standards. When deployed as a managed service, such as App Connect Enterprise as a Service, the hosting is provided by Amazon Web Services (AWS) in designated, often global, data centres.

IBM Process management and Business Rules Software

IBM Business Process Management (BPM) and Business Rules Management Systems (BRMS), such as IBM Operational Decision Manager (ODM) and IBM Business Automation Workflow, are developed and assembled by a global network of IBM laboratories, with key research and development centres in the United States, France, Canada, and India. While core software components are developed by IBM, the products are frequently assembled in a modern software context, integrating third-party open-source components from various international sources (e.g., Google and Docker) into the final software packages. These products, which often stem from acquired technologies like Lombardi and ILOG, are manufactured into distributable software images in major hubs, including the US, leveraging a worldwide development team.

The jurisdiction and provenance of these software tools are principally American, governed by United States law under IBM's intellectual property management, headquartered in Armonk, New York. The software is heavily regulated by international standards and IBM's internal security policies, ensuring compliance for global deployment on premises. As such, while the development is globally distributed, the controlling legal authority, copyright, and ultimate responsibility for the software's provenance lie with the IBM Corporation in the USA.

IBM Database Management Software

IBM Db2 and Guardium data security software are primarily developed and maintained by International Business Machines Corporation (IBM), a US-headquartered multinational company, with key research and development labs operating globally, including significant facilities in the United States, Israel, and other international locations. Guardium, which was acquired by IBM in 2009, was originally established in Massachusetts with substantial technology research contributions from Israel.

The software originates from within the United States legal framework, as IBM is an American company based in Armonk, New York, and it adheres to U.S. law regarding digital intellectual property and security standards. Jurisdictionally, this means the software is subject to US federal law, while for on-premises deployments the processing and storage of data are managed within specific geographical locations in accordance with global data protection regulations like GDPR. The provenance of Guardium, specifically, is a combination of its initial Israeli and Massachusetts-based startup roots, which have since been fully integrated into the global IBM Security division.

Red Hat Enterprise Linux (RHEL)

Red Hat Enterprise Linux (RHEL) is developed by Red Hat, Inc., an American company headquartered in Raleigh, North Carolina, which operates as a subsidiary of IBM. While the corporate HQ is in the US, the software is engineered globally, with significant development centres in Brno (Czech Republic), Bengaluru and Pune (India), and throughout North America. The source code is fundamentally derived from open-source upstream projects, most notably Fedora Linux, CentOS Stream, and the Linux kernel, to which Red Hat is a major contributor alongside global partners. As such, the "manufacturing"—or assembly, testing, and

packaging—of RHEL takes place in distributed, virtualised, and secure, containerised environments managed by Red Hat's global engineering teams.

RHEL is subject to United States law, due to its parent company, IBM. However, the software components possess a transparent open-source pedigree, with provenance managed through in-toto attestations and secured pipelines, ensuring the integrity of the build process from source code to final product. As of 2023, the full source code is primarily made available to customers via CentOS Stream. Red Hat provides Enterprise Linux worldwide, adhering to international security standards and holding a wide range of certifications, including FIPS 140-2, to meet global compliance requirements.

Proxmox Virtual Environment (Proxmox VE)

Proxmox Virtual Environment (Proxmox VE) is developed and maintained by Proxmox Server Solutions GmbH, a software manufacturer headquartered in Vienna, Austria. Founded in 2005, the company develops its core software, including Proxmox VE, Mail Gateway, and Backup Server, primarily within Austria. As an open-source virtualization platform, the software incorporates key technological components developed globally, such as the Debian GNU/Linux distribution, KVM hypervisor, and LXC containers, which are integrated, assembled, and secured at their Austrian facility.

The jurisdiction and provenance of Proxmox software are firmly within the European Union (Austria). Proxmox Server Solutions GmbH is an independent company, and its software is released under the terms of the GNU Affero General Public License (AGPL-v3), promoting open access and transparency. As it is based in Austria, the company operates under EU law, including strict data protection and security regulations. The provenance is transparent, with all proprietary management interface components and modifications designed in Vienna, ensuring that the software's intellectual property and development governance are not subject to non-European jurisdictions, enhancing its suitability for sovereign IT infrastructure.

Established in 2005, the company is privately owned and free from venture capital influence.

Open-Source Software (OSS)

Open-Source Software (OSS) is characterised by a decentralised, global development model rather than a centralised manufacturing location. Key software parts and components are developed collaboratively by voluntary contributors and corporate employees located worldwide, with significant hubs in the United States, China, India, and across Europe (particularly Germany and the UK). OSS components are curated and integrated via online repositories like GitHub or Source Forge, which serve as the digital manufacturing floor. While major contributors often reside in tech-mature regions, the open nature of the development process allows for a dispersed, international provenance, often described as a "global internet community".

The jurisdiction and provenance of OSS are governed by the license under which the software is released, which acts as a legal document establishing copyright and usage rights. Popular licenses include the GNU General Public License (GPL) and the MIT License, which define the rights for users to modify and distribute the software. While these licenses are legally binding and enforceable in courts worldwide—often under the jurisdiction of the original developer's country—the collaborative, multi-contributor nature of projects can lead to complex ownership scenarios. Ownership and compliance are usually managed by non-profit organizations like the Linux Foundation or the Apache Software Foundation, which often work across borders to support global collaborative efforts.

NGINX is owned and developed by F5 Inc

NGINX is a widely used web server and reverse proxy software originally created by Russian Igor Sysoev and first released in 2004. Critical software parts including its event-driven architecture, HTTP cache, and load balancer were developed and refined in Russia over the following decade. Following a significant acquisition in 2019, NGINX became part of F5, Inc., a company headquartered in the United States.

The software is open-source and released under a 2-clause BSD license. Current development is distributed, with significant contributions from the global community and F5, Inc. engineers. In 2022, following the Russian invasion of Ukraine, F5 discontinued its operations in Russia, relocating the development efforts. The legal jurisdiction, provenance, and ownership of the commercial components (NGINX Plus) now lie with F5, Inc. in the United States, although the open-source code remains publicly available for contribution.

PostgreSQL

PostgreSQL is an open-source relational database management system (RDBMS) with foundational provenance being the University of California, Berkeley, in 1986, where it was developed as a successor to the Ingres project. While the original POSTGRES research team was US-based, the modern software is manufactured and assembled globally. The source code is

maintained and continuously updated by the PostgreSQL Global Development Group—a diverse, international community of individual developers and corporations, rather than a single geographic location. Key software parts and contributions originate from developers worldwide, with major support, hosting, and professional services often concentrated in North America, Europe (including Germany, UK, and France), and parts of Asia.

The software is released under the PostgreSQL License, which is a liberal Open-Source Initiative (OSI) approved license similar to BSD or MIT. Its jurisdiction and provenance are thus decentralised; the copyright is shared among the PostgreSQL Global Development Group and contributors rather than holding a single country's proprietary jurisdiction. As open-source software, there is no physical "manufacturing" location in the traditional sense; instead, the code is assembled and distributed electronically through the official PostgreSQL website and managed on Git repositories, allowing for deployment on all major operating systems, both on-premises and across global cloud platforms (AWS, Google Cloud, Azure).

Keycloak

Keycloak is an open-source Identity and Access Management (IAM) software product that originated under the stewardship of Red Hat, based in North Carolina, USA, with development starting around 2013. In April 2023, the project was donated to the Cloud Native Computing Foundation (CNCF), a subsidiary of The Linux Foundation. As such, its provenance is that of a global community-driven open-source project, with core contributions historically coming from Red Hat engineers located in various international locations, including significant development work in Brno, Czech Republic.

Regarding the geographic source and "manufacturing" of the software, Keycloak is a Java-based application, meaning the code is written, assembled, and tested by contributors worldwide rather than in a physical factory. The source code is maintained in public repositories (GitHub), with containerized images (Keycloak.X) published by Red Hat/CNCF via registry services like Quay.io. The jurisdiction of the project is primarily governed by the Apache License 2.0, providing open-source access, while its stewardship falls under the CNCF, which operates as a US-based non-profit entity.