KDD057 - Business System Location

Status	Approved
Owner	WENNINGER-ext, Sascha
Stakeholders	ITHURALDE, Mariano Khedir, Nicolas Swance, Chad ANCORA, Marco AVRIL, Damien JAIN, Andrea CUENDET, Michael Goujard, Filipa Michel Morand, Francine Claustre

Issue

The creation of a new set of enterprise systems by the SyWay program provides an opportunity to revisit historical decisions about the hosting locations of IT systems which were made in a time of on-premises data centres and were potentially influenced by acquisitions of businesses or other legacy Solvay concerns. This is done to better leverage available cloud technologies and SaaS and PaaS components, improve security and data protection, improve end user experience, and enhance compliance with relevant regulations.

Recommendation

This document recommends continuing the current practice of using **the European Union as the primary hosting location for global IT systems** serving the Syensqo group as a whole. There are no architectural reasons to recommend building the new enterprise systems in the other viable alternative of the United States. A European location is expected to confer somewhat lower expected network latencies for the average end user, and a lower carbon footprint of the computing infrastructure. However most significant are legal and regulatory considerations that provide significant barriers to the use of a location outside of the EU, and would require at a minimum, the creation of internal contractual frameworks to ensure compliance with relevant data protection and export controls. The recommended option of hosting the systems inside the EU is also referred to as Option B in this document.

For both commercial and regulatory reasons, Ireland was selected as the specific hosting location for the SAP S/4HANA system in the RISE construct.

In addition to the above, the Executive Leadership Team of Syensqo decided in December 2024 that for strategic reasons, a separate SAP S/4HANA instance is required in China to serve the parts of Syensqo operating inside that country.

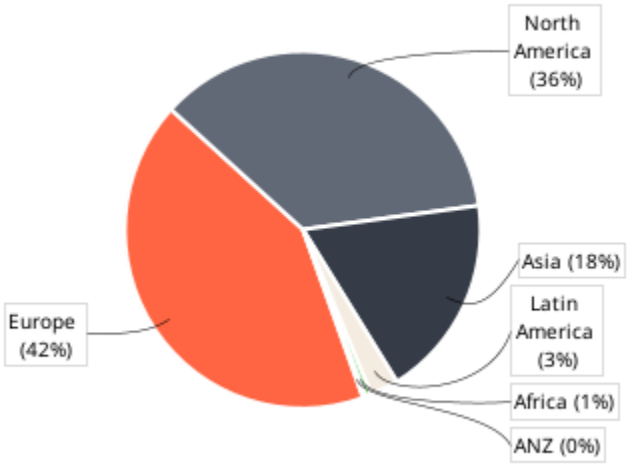
Background & Context

Geographic footprint

Historically most of Solvay's global IT systems have been located in on-premises data centres in Civirieux (north of Lyon in France), or AWS and GCP regions in Europe (predominantly Ireland, Netherlands, and Germany). Global SaaS applications have followed this allocation, with Salesforce and other global SaaS instances being placed in the EU. For the purposes of this document, the countries of the EU are treated as a single geopolitical entity, with no distinction being made between countries of the Union. One exception to this is the discussion on network latency, where geographical 'Europe' designation is used. This includes other geographically proximate countries not in the Union, e.g. the UK, Switzerland.

The map below shows the geographic distribution of Syensqo staff across the world, followed by a pie chart summarising allocation across major geographic regions.

Geographical staff distribution



CMMC Regulations

A review of Syensqo's IT systems landscape as it pertains to compliance with the US-originated CMMC v2 requirements concluded in December 2025 and determined that Syensqo's ERP systems do not contain any Controlled Unclassified Information (CUI). As a result, SAP ECC, and thus also its successor SAP S/4HANA, are treated as a Out-Of-Scope Assets (OOSA) for the purposes of CMMC compliance.

The determination that information inside SAP systems, including technical information such as Bills of Material and Routings, is not CUI removes the requirement (from DFARS 252.204-7012) to locate the system inside a FedRAMP-certified cloud environment. In the SAP RISE model, the only such environment is provided by SAP's sovereign cloud offering SAP NS2. This determination thus removes a constraint on the location decision and in turn enables the implementation of the recommended Option B (locating the system in the EU), provided that adequate security controls are implemented. The use of NextLabs DAE for granular data protection, along with strong and well-managed authorizations, encryption and key management practices, provides some of these controls.

Irish Export Controls

The Irish Department of Enterprise, Trade and Employment confirmed that hosting export-controlled data in Ireland will not automatically make it subject to Irish jurisdiction, provided that all of the following conditions are met at all times:

- the data remains encrypted, and
- access authorization is appropriately managed, and

- the data is not viewed, retrieved or modified in Ireland (e.g., by an Irish employee of Syensqo).

Assumptions

- The SyWay program aims to, where possible, deploy a single, global instance of every enterprise system in scope of the program.
- Due to strategic considerations, the Executive Leadership Team of the company decided in December 2024 to use a separate SAP S/4HANA system for the business in China.
    - Syensqo users located in mainland China are able to access various other business systems not being deployed locally into China, including SaaS systems such as Salesforce or SuccessFactors, via Syensqo-managed VPN tunnels regardless of the physical location of these systems. See also Specific architecture for China.
- There are no technical barriers which currently limit access of Syensqo staff to the jurisdictions being considered for hosting the enterprise systems.
- The European Union is treated as a single contiguous geopolitical region for the purposes of this document.
- Syensqo does not have a requirement to locate infrastructure inside the borders of Belgium.
- Syensqo enterprise systems do not contain any data that is formally Classified by the government of the US or any other nation.
- Hosting in the EU satisfies export control requirements by the UK, EU, China, and other countries to whose regulations Syensqo is exposed to, potentially via export licenses, because Syensqo's existing ERP systems are hosted in the EU and thus presumably data export to the EU and storage inside the EU has been authorised.
- ITAR is generally more restrictive than the US Export Administration Regulation ("EAR") covering dual-use products. Any solution that is sufficient for ITAR will also be sufficient for EAR.
    - One known exception to this assumption is the requirement for FIPS 140-2-certified encryption modules. ITAR does not require FIPS 140-2, deeming "equivalent or better than AES128" to be sufficient (22 CFR 120.54(a)(5)(iii)), while EAR *does* require FIPS 140-2 certification (15 CFR 734.18(a)(5)(iii)). Historically the use of the Voltage Format-Preserving Encryption module was required inside the NextLabs DAE solution due to its certification, however since 2025 NextLabs provides native support without third-party add-ons.
- Data subject to UK export controls must also be encrypted using the same mechanisms that are used for ITAR and EAR data when stored outside of the UK.
- Adopting the recommendation described in this document would entail an export from the US to the EU of information beyond that which is governed by export controls such as ITAR and EAR, because the existing "BOM Vault" system WPX contains information that is not subject to the export controls of ITAR and EAR, but may be covered by other regulations, such as US data privacy regulations. It is assumed that no regulatory obstacles exist to the export of such data. The WPX system contains no personal data that is not already in EU-hosted systems.

Constraints

- Due to the incumbency of the European Union as both the physical location for Syensqo's existing enterprise systems and data processing (e.g. by Shared Services staff in Portugal, management staff in Belgium and France), Syensqo does not have a comprehensive internal contractual framework for the export of various data from the EU to other jurisdictions. Scoping and implementing such a framework is a prerequisite for the implementation of enterprise systems outside of the EU. It may not be possible to fully implement the required contracts and processes within the timeline of the SyWay program.
- Locating the core business systems in the EU precludes these from hosting any Controlled Unclassified Information (CUI), as no FedRAMP-certified SAP RISE hosting environments exist in Europe as of December 2025. This is however not an issue since a comprehensive review of Syensqo's CMMC posture and CUI footprint in 2025 concluded that information inside SAP is not CUI. This constraint must be considered when considering:
    - any future initiatives that expand the functional scope of the business systems, or
    - expansion of business activities into new markets or customer segments exposed to regulation, or
    - new or updated regulations enter into force.

Impacts

- The use of a single-instance SAP S/4HANA system located in Europe requires careful implementation of additional technical controls to ensure continued compliance with the data export restrictions imposed by ITAR and EAR. The use of NextLabs DAE is foreseen to provide field-level encryption of export-controlled data inside S/4HANA (and potentially also SAP GTS). Although the relevant details are out of scope of this document, in summary, when protected by encryption end-to-end, ITAR/EAR-relevant data can be transmitted and stored outside of the USA without being considered to have been exported (for ITAR, see US CFR § 120.54 and explanatory notes by the Department of State; for EAR see 15 CFR 734.18). For more details on NextLabs, please refer to Logical Architecture of NextLabs DAE. The design using NextLabs DAE to protect ITAR/EAR-relevant data in systems physically hosted outside of the US has also been reviewed by external legal firm Arnold & Porter, who deemed this design to be in compliance with ITAR and EAR requirements (see memo and additional clarifying memo).
- Since S/4HANA is treated as an Out-Of-Scope Asset for the purposes of CMMC, controls must be implemented to prevent the insertion of CUI data into SAP S/4HANA. This is expected to be achieved through process controls which define how CUI that is received from customers must be handled.
- Inside S/4HANA, export control classification statuses must be maintained separately for both Products and Bills of Material, and this classification information must be used by NextLabs to selectively encrypt export-controlled data in line with the relevant regulations.
- The NextLabs environment that controls the encryption keys and policies used to protect export-controlled data ("Access information") must be managed by Syensqo; management cannot be outsourced to third parties, nor be performed by non-US persons under ITAR.

Business Rules

- When entering into agreements for software systems provided as SaaS, PaaS, or IaaS to the Syensqo group globally, preference must be given to the use of the EU as the physical hosting location unless adequate contractual and legal safeguards and controls are in place.
- During the process of creating new products, the export controls applicable to the product and its Bill of Materials must be determined, and the outcome of this determination recorded as part of the master data inside S/4HANA. The export control status of a product may differ from that of its associated Bill of Material, hence these attributes must be maintained separately inside S/4HANA.
- Information designated as CUI (Controlled Unclassified Information) must not be stored inside the S/4HANA systems as these are considered to be Out-Of-Scope Assets for the purposes of CMMC, and are thus not authorised to store or process CUI.
- Users located in China must use the S/4HANA system located in China, as well as other ancillary systems which exist in China to support the S/4HANA system resident there.

Options considered

The scope of this discussion is limited to globally-used instances of enterprise systems, such as S/4HANA, SAP Datasphere, Salesforce, etc. Local site-based applications in the Manufacturing Execution Systems, Laboratory Management Systems, and R&I domains are not covered by this document, and should continue to be deployed in line with operational requirements and applicable data protection and data export control requirements. The creation of a separate system in China, for businesses operating in China, was mandated by the Executive Leadership of Syensqo and is thus not further considered for evaluation.

Option A: Build Syensqo's new global business systems in the USA

This option would seek to build all new enterprise systems in data centre locations in the USA. Relocation of existing SaaS systems would be considered on a case-by-case basis depending on integration requirements and data residency and export control requirements. If possible, systems would be located on the East Coast of the continental United States to maximise geographical proximity to Europe, and thus reduce latency from the approx. 42% of Syensqo employees based in that geography.

Option B: Continue to locate global systems in the EU

This option continues the current practice of the use of the EU as the primary location for enterprise IT systems used globally by the Syensqo group. New systems being established by the SyWay program would be located in the EU.

Option C: Continue to locate global systems in the EU, and build a US-resident system for businesses handling CUI data

This option is a hybrid of options A and B: The EU would continue to be the default hosting location for global systems used by all Syensqo businesses outside of China; however a specific exception is created for businesses processing CUI (Controlled Unclassified Information), which must use US-based cloud environments due to the requirement to host CUI inside FedRAMP-certified clouds. FedRAMP certification is only available for US-based environments, such as Microsoft Azure GovCloud or SAP NS2, thus this option necessitates the creation of a separate environment in the US. In order to tightly define the scope of this separate US-based environment, the following rules are applied:

- Company codes will not be split across environments - each legal entity is represented inside the SAP landscapes by one company code which resides in exactly one SAP environment; and
- Plants belong to one company code. If a Plant handles CUI, then it, and its parent Company code, are operated from the US-based environment.
- If a Plant operating in the global environment expects to develop products subject to CUI controls, then a new Company code and Plant must be created in the US-based environment. All R&I activities and product development must be confined to that Plant and Company code, and must occur in the US-based environment.

Evaluation

The EU and USA are approximately equivalently beneficial hosting locations from a technical perspective. Europe presents a marginally more beneficial location from a network latency perspective for the 18% of Syensqo users who are located in greater Asia (China, India, South Korea, Thailand); otherwise the user experience obtained via network latency is deemed immaterially different. Both locations offer great breadth of available technology solutions, with multiple "hero regions" of AWS, Azure, and SAP present in each location, thus offering early access to new technologies and sufficient depth of infrastructure to ensure resiliency and scalability.

However Syensqo's historical choice of the EU as primary hosting location means the company is well-equipped to handle data protection and export controls in this legislative regime, and is ill-equipped to do the same when systems are hosted in the US. As there is no compelling technical reason to deviate from the existing use of the EU, while there are significant and currently largely unknown, legal complexities, this document recommends to continue to use the EU as the primary hosting location (i.e. Option B below).

The use of a separate instance of S/4HANA and associated systems in China, for all parts of the business operating in China, is common to all three options as a result of an executive mandate.

	Option A: + Located in USA, plus separate instance in China	**Option B: + Located in EU, plus separate instance in China**	**Option C: + + Located in the EU, plus a separate US-based system for any businesses handling CUI, plus separate instance in China**

Legal /regulatory requirements for data localisation	⊕ Superficially appears to be more compliant with the export controls imposed by ITAR and EAR, however... ⊖ ...merely locating a server in the USA does not by itself ensure compliance with ITAR or EAR if non-US Residents are also able to access export-controlled data. If personnel who are not US residents must access the system (e.g. IT personnel for administration or maintenance), then mechanisms such as field-level encryption via Next Labs DAE must still be used; alternatively, all non-US Residents must be excluded from access. ⊖ Besides the US-based ITAR and EAR, Syensqo is also exposed to data export controls from the European Union, United Kingdom, Canada, Mexico, and Germany (for selected weapons-related products). Significant investigative work is required to understand the impact of these regulations on any decision to change Syensqo's historic use of the EU as its primary hosting location.	⊕ Syensqo has decades of experience handling global data protection requirements with IT systems located in the EU, and subject to EU regulation. ⊕ As a company incorporated in the EU, locating core enterprise data in the same jurisdiction minimises total overall exposure to legal and regulatory regimes. Locating this data in another jurisdiction could expose Syensqo to additional regulatory requirements or legal discovery mechanisms.	⊕ Superficially appears to be more compliant with the export controls imposed by ITAR and EAR, however... ⊖ ...merely locating a server in the USA does not by itself ensure compliance with ITAR or EAR if non-US Residents are also able to access export-controlled data. If personnel who are not US residents must access the system (e.g. IT personnel for administration or maintenance), then mechanisms such as field-level encryption via NextLabs DAE must still be used; alternatively, all non-US Residents must be excluded from access. ○ Since the determination in December 2025 that data inside SAP ERP and SAP S/4HANA is not CUI, the regulatory driver for this option is eliminated. Compliance with US export controls has been shown to be possible with a system located in the EU provided that data access controls enabled by NextLabs are implemented.
Internal legal support, inc. data export and data processing agreements	⊖ Syensqo currently lacks a contractual framework to fully govern the wholesale export of data from the EU to another jurisdiction. As confirmed by the Group Data Protection Officer, Syensqo decided not to implement at this time Binding Corporate Rules to govern export of data outside of the EU. Establishing such Rules is possible, but requires effort, time, and approval by the relevant competent data protection authority in the EU. This timeline is considered to be beyond that available to the Detailed Design phase of the SyWay program. ⊖ On 10 July 2023 the European Commission adopted an adequacy decision for the data transfers of personal data between the EU and USA ("EU-US Data Privacy Framework" or "DPF"). This establishes a set of simplified measures for exchanges of personal data and commits organisations to several obligations regarding the processing of personal data. Adherence to the DPF must be certified by the Department of Commerce in the US. Syensqo has not commenced the process of establishing the required measures and obligations, and thus cannot yet take advantage of this mechanism. ⊖ The import into the US of information related to military or dual-use items from third countries may cause this data to fall under the scope of the relevant US export control law, and then subsequently prevent use of this data outside of the US unless a relevant license is obtained from the US government.	⊕ Data protection principles as defined in the EU by the GDPR are among the most comprehensive and protective in the global landscape. Many regulatory regimes in other countries broadly permit data transfer into jurisdictions with equivalent or higher degrees of data protection; hence transfer from third countries into the EU is less likely to be problematic or require complicated compliance mechanisms. ⊕ Ability to reuse existing export licenses permitting the movement of data from third countries into the EU country where Syensqo's current ERP systems are located. ⊕ Simplified compliance with the export requirements of the German BAFA authority, which has established that the electronic transfer of software or technology from the EU to a server in a third country constitutes an export, even if the data is solely transferred and stored in encrypted form, and no one in the third country has access to this data. The "encryption exemption" which exists in ITAR (22 CFR 120.54) and EAR (15 CFR 734.18) does not exist in the German regulation.	⊕ Potential to more explicitly handle data residency and cross-border data movements, and to reduce exports due to data localisation. ⊖ Syensqo currently lacks a contractual framework to fully govern the wholesale export of data from the EU to another jurisdiction. Although such exports would be limited in scope, they would still need to be governed by an appropriate contractual framework. As confirmed by the Group Data Protection Officer, Syensqo decided not to implement at this time Binding Corporate Rules to govern export of data outside of the EU. Establishing such Rules is possible, but requires effort, time, and approval by the relevant competent data protection authority in the EU. This timeline is considered to be beyond that available to the Detailed Design phase of the SyWay program.
Implementation Cost & Complexity	○ No significant difference in implementation cost or complexity	○ No significant difference in implementation cost or complexity	⊖ A significant number of additional interfaces and configurations, along with necessary testing effort, was estimated by the SyWay program to amount to approx. €13.6m of additional implementation costs over the course of the SyWay program.
Operating Cost & Complexity	○ No significant difference in operational cost or complexity. SAP RISE fees do not vary based on the hosting location.	○ No significant difference in operational cost or complexity. SAP RISE fees do not vary based on the hosting location.	⊖ Operating costs are significant due to duplication of infrastructure and unavoidable duplication of some licensing fees due to ring-fenced operations and commercials in a sovereign cloud construct. A sovereign SAP NS2-hosted environment for S/4HANA and associated cloud products was quoted at €5.1m per annum. Additional costs would need to be incurred for Kinaxis Maestro and OpenText, thus further adding to the TCO of this option.
Availability of SaaS applications	○ There is no significant difference between the EU and USA when considering the SaaS and PaaS services from SAP and Salesforce in each geography. An analysis of SAP's Data Center listing (see also below) shows that all SAP SaaS and PaaS services relevant for Syensqo are available in the EU and USA. While SAP's region strategy is less well known than the strategies of AWS and Azure, it appears to be clear that both geographies receive new services upon release, and provide an equivalent degree of hosting location and provider diversity as evidenced by major SaaS and PaaS applications being available in multiple locations in each geography.		

	An analysis of Salesforce's public documentation reveals no significant differences in the regional coverage between the EU and USA for their core product. The exception to this is the Data Cloud product whose only EU-based hosting option is Frankfurt, although this is spread across multiple AWS Availability Zones for DR purposes.		
Depth and breadth of technology platform components	There is no significant difference between the EU and USA when considering the available depth and breadth of technology solutions and platform components. AWS and Azure operate multiple "hero regions" in both the EU and USA; these are generally the first locations to receive new features and products, offer the largest number of Availability Zones for redundancy, and largest infrastructure footprints to ensure infrastructure is available when needed. This bears greater importance to cutting-edge features such as AI/ML functions than commoditised server and storage services, because delays of a year or more are not uncommon between deployment to hero regions and products reaching smaller locations.		
Network latency impact for end users		The EU will provide a marginally superior network latency for the average user at Syensqo. An analysis of network latency data between the capital cities of countries with a Syensqo presence and the two most-likely hosting locations of Asheville, Virginia (USA), and Amsterdam (EU), when weighted by headcount in each country, reveals that the average latency for the US location is 44% higher than for the EU location. Syensqo's user base is heavily weighted towards Europe (42%) and North America (36%), followed by Asia (18%). Only 3% of the Syensqo user base is located outside these regions. The Asian geography has generally materially lower latencies to Europe than to North America; India and South Korea can expect to incur latency penalties of up to 120ms when connecting to North America rather than Europe. From a latency perspective, a European location is thus marginally more favourable for the Asian user base.	Any benefit to US-based Composite Materials personnel, who gain lower-latency access to a US-based system, would be offset by correspondingly higher latency for Composite Materials personnel in the UK and Germany who must access a US-based system. However due to the large number of high-performance network links between Europe and the US, the magnitude of these effects is very limited, thus resulting in very small gains and losses.
Carbon footprint		The electricity grid in major EU data center locations (e.g. Netherlands) tends to be marginally less CO-intensive than in major US locations (e.g. Virginia) when judged on an annual basis. For example, in the year 2025, the CO intensity of the Dutch grid on a consumption basis was 335gCOeq/kWh vs. 415gCOeq/kWh for Virginia.	
	A caveat to this analysis is that all major IaaS providers purchase electricity directly from power generators via direct purchase agreements that favour renewable energy, rather than obtaining power from the national grid. They also tend to purchase renewable energy offsets for a large part of their operations (e.g. AWS offsets 100% of carbon emissions in most Regions in 2023; Azure will offset 100% of emissions by 2025). Their actual CO footprint is likely much lower to that of the respective national grids.		

Below follows a summary analysis of the effect of various combinations of system location and use of NextLabs DAE on the ease of compliance with export controls of the US and EU, as well as EU data protection regulations.

The conceptual architecture of NextLabs DAE integration into SAP systems is depicted on the separate page Logical Architecture of NextLabs DAE.

	Located in USA		**Located in EU**	
	With NextLabs DAE	**Without NextLabs DAE**	**With NextLabs DAE**	**Without NextLabs DAE**
US Export Controls (i.e. ITAR, EAR)	Data subject to US export controls is encrypted, at rest, a field level, and can only be decrypted by explicitly authorised persons. The rest of the system can be accessed by persons who are not US Residents and who are located outside of the USA. The system can be remotely supported by SAP.	Data subject to US export controls is not encrypted at rest, and visible to system administrators as well as potentially other users. This means only US Residents located in the US may act as system administrators, developers, etc. The SyWay program as currently staffed and located, cannot use this system to develop configuration, code, etc.	Data subject to US export controls is encrypted, at rest, a field level, and can only be decrypted by explicitly authorised persons, hence not deemed to be exported under 22 CFR 120.54 or 15 CFR 734.18. No export license is required. This was also validated by the specialist law firm Arnold & Porter in November 2024 (see memo and addendum).	Data subject to US export controls is exported from the US without being protected by encryption. An export license is required.
EU Export	Storage of export-controlled data outside of the EU is considered to be an export		Encryption of export-controlled data is not	No issues.

Controls (inc. German BAFA)	regardless of encryption. An export license is required. Depending on its nature, data may fall under the scope of US export controls. An export license from the US State Department may be required in order to use this data outside of the US, even though it originated outside of the US.	required, but can be used. Storage in the EU means data is not exported; no licenses needed.	Encryption of export-controlled data is not required. Storage in the EU means data is not exported; no licenses needed.
Data Protection regulations (e.g. GDPR)	After completing the development of its governance, Syensqo would need to establish Binding Corporate Rules, and seek necessary endorsements by the relevant data protection authorities, before being able to export protected data from the EU to the USA.	Existing compliance mechanisms continue to be applicable.	
US CMMC (for protection of CUI)	Detailed investigations in 2025 determined that SAP systems do not process or store CUI information, and that the SAP systems are outside of the CMMC boundary. Export controls continue to apply, but controls specific to systems storing and processing CUI need not be implemented for SAP S/4HANA and associated systems being deployed by SyWay.		

See also

Maps showing the carbon intensity of the electricity grid by geography

Regional coverage of relevant SAP SaaS and PaaS Solutions

A summary of the List of SAP Data Centres for SAP Cloud Services for products and services relevant for Syensqo is represented below. Numbers indicate the number of physical locations (i.e. data centres or IaaS regions) in which each product or service is available. Availability of a product or service in only a single region in a particular geography may limit the Disaster Recovery options available for that service. This is thus represented as a paler shade of green in the table below. The information for this summary table was retrieved in December 2025, using the then-current version v.12-2025 of the document. The latest-available version can be retrieved at List of SAP Data Centres for SAP Cloud Services.

Product	EU	US	China
AI	2	3	1
Application Development and Automation	6	10	2
Customer Data Solutions	2	2	1
Data and Analytics	7	10	2
Data Custodian KMS	1	2	0
Foundation / Cross-Services	7	10	2
Integration	7	10	2
Miscellaneous	7	10	2
RISE with S/4HANA, Private Edition	21	18	7
SAP Advanced Financial Closing	1	1	0
SAP Ariba	2	3	1
SAP Asset Performance Management	2	2	0
SAP Business Network	2	2	1
SAP Cloud ALM	2	1	1
SAP Cloud Identity Access Governance	2	4	0
SAP Concur	1	1	1
SAP Green Ledger	1	0	0
SAP Risk and Assurance Management	1	0	0
SAP SuccessFactors	5	7	1
SAP Sustainability Control Tower	1	1	0
SAP Sustainability Footprint Management	1	2	0
SAP Test Automation by Tricentis	1	1	0

Salesforce Locations

Salesforce documentation provides a list of data centre locations from which their application is served. Salesforce maintains 3 separate data centre locations in the USA, and 4 inside the EU (plus one in the UK). Each location provides multiple separate data centres with separate, completely redundant infrastructure. Salesforce additionally leverages AWS locations to deliver the Hyperforce and Data Cloud services. Despite a Dec. 2023 press release announcing the availability of core products on Alibaba Cloud in China, available documentation including those linked below, do not mention hosting locations in China.

	EU	US	China
Salesforce-managed data centers	4	3	?
Hyperforce locations (hosted in AWS)	4	3	?
Data Cloud	1	2	?

See also the Salesforce Security, Privacy, and Architecture documents for Salesforce Services and Hyperforce.

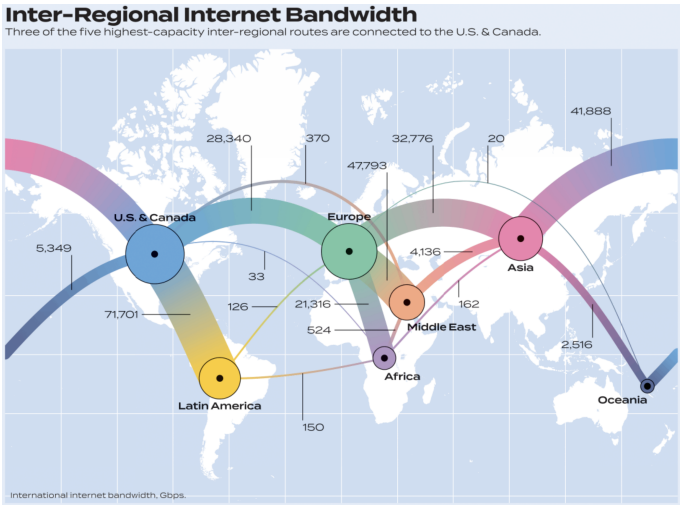
Technical Resources related to Network Latency

WonderNetworks - latency data for many locations around the world

CloudPing - measure latency to various IaaS locations

Submarine Cable map - showing routes of fiberoptic cables carrying internet services

Excerpt from the 2022 Global Internet Map, published by Telegeography, showing aggregate internet bandwidth between major geographies:



File	Modified
PDF File Endorsement - Trade Compliance.pdf	Mar 26, 2026 by WENNINGE R-ext, Sascha
PDF File Endorsement - Filipa Goujard.pdf	Jan 27, 2026 by WENNINGE R-ext, Sascha
PDF File CMMC Scope Summary - Syensqo 10 Dec 2025.pdf	Dec 29, 2025 by WENNINGE R-ext, Sascha
PDF File CUI Positions - Syensqo.pdf	Dec 29, 2025 by WENNINGE R-ext, Sascha
PDF File Arnold & Porter Memo - U.S. Export Control Analysis Regarding Use of a EU-based Data Storage System 2024-10-30.pdf	Dec 17, 2024 by WENNINGE R-ext, Sascha
PDF File Arnold & Porter Memo - Follow-on Analysis Regarding Use of a EU-based Data Storage System Under U.S. Export Controls 2024-11-13.pdf	Dec 17, 2024 by WENNINGE R-ext, Sascha
PDF File Meeting Minutes - KDD057 - Business System Location 2024-11-19.pdf	Dec 11, 2024 by WENNINGE R-ext, Sascha

Microsoft Excel Spreadsheet PingTimingAnalysis.xlsx	Sept 12, 2024 by WENNINGER-ext, Sascha

Download All

Change log

Version	Published	Changed By	Comment
CURRENT (v. 40)	**Mar 25, 2026 19:01**	**WENNINGER-ext, Sascha**	
v. 39	Jan 29, 2026 03:47	**WENNINGER-ext, Sascha**	
v. 38	Jan 29, 2026 03:41	**WENNINGER-ext, Sascha**	
v. 37	Jan 22, 2026 08:06	**WENNINGER-ext, Sascha**	
v. 36	Jan 22, 2026 07:31	**WENNINGER-ext, Sascha**	
v. 35	Jan 19, 2026 13:22	**WENNINGER-ext, Sascha**	
v. 34	Jan 07, 2026 16:08	**WENNINGER-ext, Sascha**	Updated based on Andrea Jain's feedback that SAP is OOSA rather than CRMA.
v. 33	Dec 29, 2025 10:27	**WENNINGER-ext, Sascha**	added links to DEFCERT documents
v. 32	Dec 29, 2025 09:51	**WENNINGER-ext, Sascha**	updated following conclusion of the DEFCERT review of CMMC boundaries and controls.
v. 31	Apr 30, 2025 10:51	**WENNINGER-ext, Sascha**	

Go to Page History

Workflow history

This view shows the 5 most recent entries. The complete workflow log is available from the 'Document Activity' menu item.

Mar 31, 2026	Actor	Type	Activity	Version
Approved	LEIGHTON-ext, Dean	State	changed state to Approved at 11:26 am	v40
Pending SteerCo Review	LEIGHTON-ext, Dean	State	gave *Final Approval* approval at 11:26 am *Previously discussed in steerco, not required to return for approval*	

Mar 26, 2026

	WENNINGER-ext, Sascha	State	changed expiry date to '09 Apr, 2026 01:59 pm' at 2:59 pm	
		State	changed state to Pending SteerCo Review at 2:59 pm	v40
Edited following Stakeholder Review	WENNINGER-ext, Sascha	State	gave *Minor change* approval at 2:59 pm *Updated based on feedback from Trade Compliance team*	

Mar 25, 2026

	WENNINGER-ext, Sascha	Edit	updated the page at 7:01 pm	