GET GDPR COMPLIANT WITH ORCHESTO-365!

ZEBWARE

Making your Microsoft 365 data compliant and protected

ORCHESTO®-365

ZEBWARE
Döbelnsgatan 21
111 40 Stockholm
SWEDEN
www.zebware.com

CONTENTS

ZEBWARE
Döbelnsgatan 21
111 40 Stockholm
SWEDEN
www.zebware.com

ORCHESTO-365
ENABLING COMPLIANT USE OF MICROSOFT 365

SUMMARY

GDPR and national data protection laws are preventing EU-based organisations from unrestricted use of third country cloud services. Orchesto-365 provides a solution to this and enables a compliant use of Microsoft 365 for documents.

Following the Schrems II judgement, supplementary measures need to be implemented to appropriately safeguard personal data when using a US-based cloud service. The Orchesto-365 software provides unique technical measures to make the use of Microsoft 365 compliant. Orchesto-365 is integrated to the Microsoft 365 solution and automatically protects data using e.g. strong encryption using customers own keys, before data is transmitted to the cloud.

CURRENT GDPR COMPLIANCE CHALLENGES WITH MICROSOFT 365

All EU-based organisations are obliged to comply to the GDPR law of data protection. However, from amendments in the US CLOUD Act of 2018, US-based cloud service providers are required to provide customer information, including personal data, to competent US authorities. Hence, for an EU-based organisation, the use of a US-based cloud service provider would constitute a direct breach of GDPR. The surveillance acts of Section 702 FISA44 and E.O. 12333, worsen this as they extend the power of US authorities to seize information by use of proactive data surveillance.

According to the Schrems II judgment of the Court of Justice of the European Union, the conflict between EU data protection laws and US surveillance laws, means that US cloud-based services cannot be used unless supplementary measures are implemented. These measures need to fill the gaps in the protection of data when US cloud-based services are used and bring the protection up to the level required by EU law.

- When US cloud service providers offer their services from locations and subsidiaries within the EU territory, the US CLOUD Act and FISA still apply. Therefore, offering its services from a European location, does not fill the gaps to make a US cloud service GDPR compliant.
- Using an encryption service offered as part of a cloud service, is not an adequate measure to bring the protection up to the required GDPR level. As the cloud service provider holds the decryption keys or copies thereof, the data is potentially exposed to US authorities and this solution is not compliant to EU data protection laws.

To support in identifying and applying appropriate supplementary measures where needed for GDPR compliance, the European Data Protection Board (EDPB) lists a series of recommendations. These recommendations include measures that could be put in place, e.g. using strong encryption of data before it is transferred to a third country.

Orchesto-365 provides a solution to the above requirements. The integration to Microsoft 365 makes the unique Orchesto data protection features available to Microsoft 365 users.

SPECIFIC CHALLENGES WHEN ADDRESSING THE PUBLIC SEGMENT

In addition to the GDPR, the public sector needs to follow specific national regulations and additional protocols to protect personal and other sensitive data.

- Public authorities, including any regional or municipality organisation, have a special obligation to protect sensitive information about its citizens. In Sweden, this is regulated in Sweden´s Public Access to Information and Secrecy Act[1] (OSL).
- Other regulations might also come in play when addressing the public sector: healthcare data security regulations, archives acts, to name a few.
- The interpretation of the OSL legislation from Swedish authorities, is that not only exposure but also risk of exposure of classified information to unauthorised parties, would result in a breach. Use of US -based cloud services is therefore considered to expose data to US authorities.

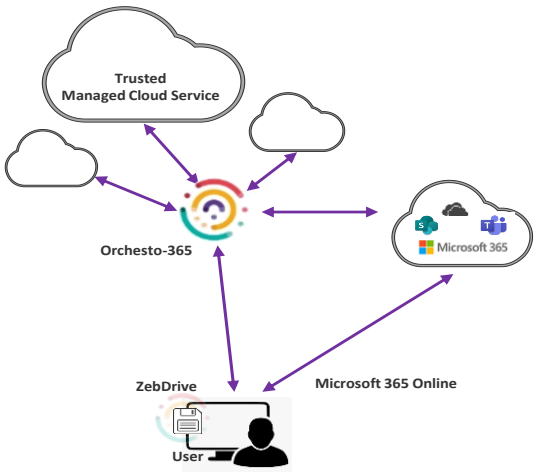
Orchesto-365 provides OSL compliance as it delivers the technical measures to protect data according to EU recommendations for GDPR.

THE ORCHESTO-365 SOLUTION

Orchesto-365 provides a technical solution to the conflicting EU and US laws and is thus enabling use of the Microsoft 365 suite.

The Orchesto-365 software is integrated to the Microsoft 365 solution and can act both on documents placed in Microsoft 365 and on documents placed outside of the Microsoft cloud-based solution.

When handling GDPR data, the end-users work with the desktop versions of the Microsoft office applications. End-users label documents according to set data management policy for GDPR. With Orchesto-365, users are enabled to place non-sensitive documents in Microsoft 365 and sensitive documents in a trusted cloud via Orchesto-365. Orchesto-365 automatically performs actions on documents according to the document labelling and the associated rules for data. Examples of Orchesto-365 actions are strong encryption of sensitive data or moving sensitive data to a trusted storage.



To secure a fully compliant solution, Orchesto-365 also acts on documents placed in the Microsoft 365 solution by mistake and moves it to the trusted cloud within seconds. Every customer defines what actions Orchesto-365 should take on a document to comply to GDPR and other applicable regulation.

Applying sensitivity labels and using Orchesto-365 secures GDPR compliance to Microsoft 365 documents.

ORCHESTO-365 GDPR COMPLIANCE TO MICROSOFT 365 DOCUMENTS

Orchesto-365 provides a solution to current GDPR regulatory requirements for Microsoft 365 documents by the provisioning of:

DATA PROTECTION BY DESIGN AND BY DEFAULT

- Orchesto-365 strong AES-256 encryption of data using customers own encryption before transmitting the data outside of customer control – in combination with the Orchesto-365 automatic enforcement to documents carrying GDPR data,
- Orchesto-365 functionality to automatically move documents containing sensitive information out of the Microsoft 365 cloud to a trusted storage,
- The option to further increase data protection by use of the Zebware zIDA algorithm to fragment and disperse data fragments across several data storage backends,
- The Orchesto-365 functionality to secure protection and immutability of data when stored in a trusted storage,
- The Orchesto-365 versioning and immutability of data placed in trusted storage,

DATA SPECIFIC STORAGE & RETENTION RULES GOVERNED BY JURISDICTION:

- Orchesto-365 strong AES-256 encryption of data using customers own encryption before transmitting the data outside of customer control – in combination with the Orchesto-365 automatic enforcement to documents carrying GDPR data,
- The Orchesto-365 versioning and immutability of data placed in trusted storage,
- The option to use direct access to a compliant storage and a compliant sharing functionality of Microsoft 365 documents in a separate and trusted storage thus solving the issue of exposure to US laws of COUD Act, FISA etc,

ACCESS CONTROL TO ELIMINATE UNAUTHORIZED OR INADVERTENT LOSS, MODIFICATION, OR MOVEMENT OF DATA

- The Orchesto-365 versioning and immutability of data placed in trusted storage
- Orchesto-365 IAM trusted storage access rights management (including possibility to share documents) defined by customers.
- For documents placed in the Microsoft 365 service, the rights defined there will be copied to and managed also by Orchesto-365.

DATA GOVERNANCE INCLUDING OPERATION LOGS AVAILABLE FOR AUDIT PURPOSES

- Orchesto-365 operational reporting to log and monitor all access to data and operations. The logging and monitoring functionality on data under Orchesto-365 management delivers GDPR compliance and documentation for audit purposes.

RESPONSE MECHANISM TO DATA SUBJECTS AND MANAGEMENT OF REQUESTS

- Supported by the Orchesto-365 logging and monitoring

BREACH NOTIFICATION MECHANISM

- Supported by the Orchesto-365 logging and monitoring

REFERENCES

Official references

[1]https://www.regeringen.se/4a76f3/contentassets/2c767a1ae4e8469fbfdofc044998ab78/public-access-to-information-and-secrecy.pdf

https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf

http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=16438951

https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&qid=1607201178269&from=EN

https://www.esamverka.se/download/18.1d126bc174ad1e6c39cac3/1542007824143/eSam%20-%20Ra%CC%88ttsligt%20uttalande%20om%20ro%CC%88jande%20och%20molntj%C3%A4nster.pdf

https://www.forsakringskassan.se/wps/wcm/connect/30cc57bd-b5cd-4e04-94cd-1f7a02a9ae1a/vitbok.pdf?MOD=AJPERES&CVID=

https://dataskydd.net/files/JO-Anmalan_Goteborgs_stad_molntjanster.pdf

Legal analysis and comments

https://kahnpedersen.se/wp-content/uploads/2020/12/KP_3-20_Publika-molntja%CC%88nster_webb_add.pdf

https://www.kramerlevin.com/en/perspectives-search/europes-highest-court-invalidates-eu-us-privacy-shield-data-transfer-framework.html

Key opinion leaders' posts

https://www.linkedin.com/pulse/r%C3%A4ttigheter-i-en-digital-v%C3%A4rld-daniel-melin/

https://www.linkedin.com/pulse/fisa-702-extraterritorial-daniel-melin/

https://www.linkedin.com/pulse/analys-av-azure-microsoft-molndesign-offentlig-sektor-andr%25C3%25A9-catry/?trackingId=ryK1%2F4F6Rq6eXBP66RwJsg%3D%3D