



SYMPHONY'S GDPR COMPLIANCE STRATEGY



We have prepared this brief to explain our compliance strategy for the EU General Data Protection Regulation ("GDPR").

The GDPR is the new EU data protection framework and comes into effect on 25 May 2018. Many of our customers – particularly those established in the EU – will be subject to this regime. The GDPR requires organisations to develop robust data protection programmes with an emphasis on accountability, transparency, individual rights over personal data and security standards.

APPLICATION OF GDPR TO SYMPHONY & YOU

Symphony Communication Services, LLC offers a secure product that allows our customers to collaborate and communicate effectively. Our customers may be subject to the GDPR where they are established in the EU or where they offer goods or services to, or monitor the behavior of, individuals in the EU.

Although we are incorporated in the United States, we may still be subject to the GDPR in certain circumstances because, under Article 3(2)(b), we offer a solution that allows companies to monitor the behavior of individuals in the EU (e.g., our solution allows a customer's compliance administrator to monitor chat room activity).

Symphony provides:



Fully integrated messaging, document sharing, conferencing, bots and apps



A trusted community of users that can collaborate securely within and across companies



Apps, software integrations and bots that enrich and extend the user experience



SYMPHONY'S ROLE UNDER THE GDPR

The GDPR distinguishes two roles that organisations can play: controllers and processors. A controller is the entity that makes decisions about personal data. On the other hand, a processor is essentially a service provider that processes personal data on the instructions of a controller.

Our customers act as controllers of the personal data processed through our product. This is because our customers control who uses our product (by granting access rights to end users), how the data is used, where the data is hosted, retention periods and certain security standards such as encryption (where we have no access to the key).

We act as a processor on behalf of our customers, following their instructions with regard to data processed through our product. To help provide our service, we can access chat metadata (which does not include the content of chats, but may include limited personal data such as user names).

HOW SYMPHONY HELPS CUSTOMERS COMPLY WITH THE GDPR

In order to help our customers comply with the GDPR, we have developed:

- a robust data processing agreement which meets the contractual requirements at Article 28, and can be signed by clicking [here](#) and we process personal data only on your instructions (as set out in our contract with you);
- compliant data storage solutions, so customers can elect to either store their data encryption keys in-house on the customer's own on-premises hardware security module, on their own in-house server, or on cloud servers within the EU (or, for non-EU personal data, in other regional hubs in the US and Asia);





SYMPHONY'S GDPR COMPLIANCE STRATEGY

- controls for customers through the Symphony Admin Portal to enable your security officers to, among other things, establish information barriers, create expression filters, assign entitlements, monitor rooms, and export content into regulatory record archives;
- security standards to keep personal data safe and secure, such as state-of-the-art encryption with customer-owned keys, and our security standards are audited by third parties. Our platform was developed based on ISO 27001 and ISO 22301 standards, and in compliance with NIST 800-53. We are EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield certified, an FS-ISAC affiliate member, compliant with the HIPAA security rule for the protection of electronic protected health information, and obtain an annual SOC 2 Type II report from an independent audit firm, which is available upon request under cover of an NDA;
- tools to enable compliance with data subject rights on subject access, rectification, erasure, restriction of processing and data portability, such as search, content export functionality through the Symphony Admin Portal and Admin-managed message suppression - whereby the content of sensitive messages is concealed vis-à-vis other users but the underlying data can still be recalled by a customer's administrator (e.g., for audit purposes);
- functionality to upload customer Privacy Policies and provide notice to users of the processing and meet the transparency, notice and fair processing standards;
- robust diligence procedures to ensure that, for any vendor who might process customer personal data, only those vendors who agree to enter into data processing agreements that meet the Article 28 requirements for compliance with EU laws are engaged, and we conduct a security and privacy review of each such vendor;



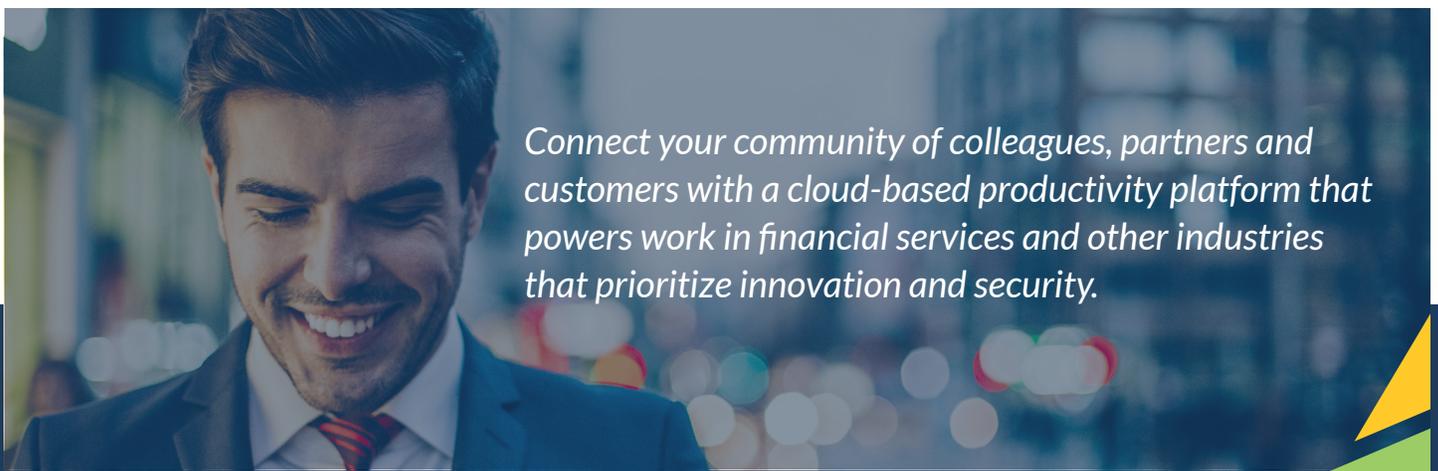


SYMPHONY'S GDPR COMPLIANCE STRATEGY

- follow-the-sun support model designed to help you use Symphony and solve any technical issues, which uses European Commission-approved Model Clauses to ensure that EU personal data is transferred subject to appropriate safeguards; and
- procedures to assist you with other GDPR obligations relating to data breach notification, data protection impact assessments and prior consultation obligations.

| SYMPHONY'S GDPR COMPLIANCE STRATEGY

Symphony is committed to complying with all laws and regulations to which it is subject, and to assisting our customers in meeting their compliance obligations. We use the Model Clauses and are certified under the EU-US Privacy Shield and Swiss-US Privacy Shield. We have undertaken the relevant data protection impact assessments with regard to our product, and partner with external counsel to assist us in this compliance programme.



For more information, please visit [symphony.com](https://www.symphony.com)