GDPR at DocuX

Last updated: November 1, 2021

To strengthen individual's rights to privacy, the European Union adopted the General Data Protection Regulation (EU) of 2016/679 ("GDPR") which came into force since May 25, 2018. GDPR enforces data protection mechanisms for processing personal data of European subjects.

Privacy is by design at DocuX. We do not need to, and we do not collect and process customers and individual's personal data beyond what is required for providing DocuX Services.

DocuX adheres to global regulations and industry practices to maintain privacy and security of customer's data. Effective compliance addresses data privacy and security requirements no matter where your business is located or which industry you belong to. We enhance business value of our services by adhering to necessary standards and policies. Hence, our cloud ecosystem is capable of providing a robust and scalable structure for safe processing of your and your customer's data. Our platform is GDPR ready to help you meet your compliance obligations. As a standard practice, we extend such capabilities and practices not only to our customers in the EU but also to all our customers worldwide.

1. KEY APSECTS OF THE GDPR

GDPR provides a framework to businesses for security and privacy needs of an individual's data used for business purposes. The key principles which the GDPR requires businesses to operate on are:

a. **Lawful, fair, and transparent processing**: Emphasizes transparency i.e., when individual's data is collected, businesses must be clear as to why data is being collected and what will it be used for.

b. **Purpose limitation**: Emphasis that data should be collected only for legitimate and specific purpose. The use of the data cannot be other than for what it has been collected.

c. **Data minimization**: Emphasizes the relevancy. Businesses must ensure data captured is adequate, relevant, and limited.

d. **Accurate and up-to-date processing**: Emphasizes integrity of the data and purpose to ensure data remains accurate, valid, and fit for purpose. Businesses must institute processes and policies to address how they maintain data they are processing and storing it. It also requires businesses to institute policies and processes to maintain integrity of these processes.

e. **Confidentiality and security**: An organization collecting and processing data is solely responsible for implementing appropriate security measures to protect the individual's data.

f. **Accountability and liability**: Establishes the responsibility of ensuring confidentiality and security of the personal data of an individual with the businesses. Businesses must be accountable and liable for their action and responsibilities in relation to collection, processing, storage, security, disposal of individual's data.

2. HOW WE ENSURE COMPLIANCE WITH GDPR?

We pay utmost attention to the data collection, processing, security, storage, and related practices at DocuX, both as data controller and processor. We ensure that all our practices and processes are designed to protect rights of individuals under GDPR. More particularly,

a. We collect only such data from individuals as is necessary for the purpose for which it is collected. Refer our Privacy Policy for more information on what data is collected, stored, and processed. At individual's request and subject to our obligations to Customers under relevant Terms of Service, or Privacy Policy or DPA, we shall respond to the requests from individuals or customers wanting to know what data we have about them.

b. By design, our processes, products, services, programs, projects, are aligned to the privacy principles right the inception. This ensures the culture and practices of privacy and compliance are default principles. We have standard framework of policies and processes in relation to data protection compliance. We have clearly defined responsibilities and defined metrics for monitoring and governing privacy practices.

c. We conduct periodic audit of our own processes and maintain adequate records of the processing of customers data.

d. We select and work with only those vendors and Subprocessors who are GDPR compliant. We ensure we have related documentation and agreements in place before we engage with them. A list of such Subprocessors can be found here.

e. We keep updated with the changes in law and business practices and keep our employees well aware of the same by regular training and dissemination of relevant information across organization.

f. We have appointed a Data Protection Officer.

g. Our Terms of Service, Privacy Policy and DPA, are fully recognize and in compliant with the data processing requirements of GDPR.

h. We ensure all data is encrypted in transit as well as at rest, based on the level of sensitivity and associated risks.

i. We regularly cleanup our databases to ensure that we have only the relevant, the latest and most accurate information. This cleanup process includes removing terminated and dormant accounts.