PDPA at DocuX

Last updated: November 1, 2021

The Personal Data Protection Act, 2012 (No.26 of 2012) ('PDPA') is the principal data protection legislation in Singapore governing the collection, use, and disclosure of individuals' personal data by organizations. The PDPA was enacted on 15 October 2012 and was amended on 2 November 2020, which is the culmination of the first comprehensive review of the PDPA since its enactment in 2012.

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 PDPA 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 Singapore but also to all our customers worldwide.

1. KEY PRINCIPLES OF THE PDPA

The PDPA imposes the following data protection obligations on organizations in respect of their data activities:

a. **Consent**: Obtain an individual's consent before collecting, using, or disclosing his/her personal data for a purpose.
b. **Purpose limitation**: Collect, use, or disclose personal data only for purposes that a reasonable person would consider appropriate.
c. **Notification**: Notify the individual of the purpose(s) for which it intends to collect, use, or disclose his/her personal data on or before such collection, use, or disclosure, and may only collect, use, and disclose personal data for such purposes.
d. **Access and correction**: Upon request, allow an individual to access, and correct his/her personal data and provide information about the ways in which personal data may have been used or disclosed during the past year.
e. **Accuracy obligation**: Make a reasonable effort to ensure integrity and accuracy of the personal data, if it is likely to use such personal data to make a decision that affects the individual concerned or disclose such personal data to another organization.
f. **Protection**: Protect personal data in its possession or under its control by making reasonable security arrangements to prevent (a) unauthorized access, collection, use, disclosure, copying, modification, disposal or similar risks, and (b) the loss of any storage medium or device on which personal data is stored.
g. **Retention limitation**: Cease to retain documents containing personal data, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that the retention of such personal data no longer serves the purpose for which it was collected and is no longer necessary for legal or business purposes.
h. **Transfer limitation**: Not to transfer personal data to a country or territory outside Singapore except as prescribed under the PDPA.
i. **Accountability**: Appoint a person (Data Protection Officer ('DPO')) to be responsible for ensuring that it complies with the PDPA, and develop and implement policies and practices that are necessary. In addition, communicate to staff information about such policies and practices and make information available upon request to individuals about such policies and practices.
j. **Data breach notification**: Assess data breaches that have occurred affecting personal data in their possession or under their control, and are required to notify the PDPC, as well as affected individuals, of the occurrence of certain data breaches.

2. HOW WE ENSURE COMPLIANCE WITH PDPA?

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 LGPD. 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 appropriate requests from individuals or customers.

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. 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 and LGPD 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 LGPD.

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.