KÖKSAL & PARTNERS
KÖKSAL • ÖZDAMAR
ATTORNEY PARTNERSHIP

Burhaniye Abdullahağa Cd., Merdiven Çıkmazı Sk., No:2, Üsküdar, İstanbul
T +90 216 700 1833
F +90 216 700 1834
www.koksalpartners.com

CBRT Updated the Guidelines on Service Providers Providing Community Cloud Services to Payment Institutions

The conditions that external service providers who will provide community cloud services must fulfill in order to be eligible and other important issues regarding the application, evaluation and supervision processes are detailed in the Guideline on External Service Providers Providing Community Cloud Services to Payment and Electronic Money Institutions ***("Guidelines")*** issued by the CBRT in July 2022.

With the first update to the Guideline in April 2023, the conditions under which the CBRT will grant eligibility to external service providers were added.

At this stage, a new update was made in the Guideline as of September 2023. With this latest update to the Guideline, all details regarding the procurement of cloud services by payment and electronic money institutions from external service providers are as follows:

A. Criteria That Fulfilled by External Service Providers Intending to Offer a Community Cloud Service Model

- **Only the Companies listed in the Guideline may provide Community Cloud Services as External Service Providers.**
  According to the Guideline, external service providers must be a credit institution, a financial institution, a company operating under an association, an electronic communication operator, a system operator or a public institution, an organization or a foundation established in the field of industry-technology. Service providers that do not fulfill at least one of these qualifications will not be approved by the CBRT.

- **Services must be provided by the External Service Provider itself.**
  External service providers are not allowed to provide community cloud services to the Institutions as a separate outsourced service.

  An exception has been made in the Guideline. In case the external services provider does not have its own data center, this external services provider shall only be able to receive hardware hosting or dedicated hardware services from external service providers that fulfill the data center requirements.
- **Employment of a Certain Number and Qualification of Personnel is Mandatory.**
  In order to ensure the uninterrupted and efficient continuity of services provided, external service providers are required to employ at least 2 (two) personnel for each of the

Burhaniye Abdullahağa Cd., Merdiven Çıkmazı Sk., No:2, Üsküdar, İstanbul
T +90 216 700 1833
F +90 216 700 1834
www.koksalpartners.com

operation/monitoring team, and information security team with a minimum of 7 (seven) years of experience in similar fields and to have established the necessary information systems and technological infrastructure.

- **All Certificates Listed in the Guideline must be held.**

Certificates for Data Standards	TSE TS EN 50600 123 Data Center Operations Documents
Certificates for Community Cloud Service	TS ISO/IEC 27001 Information Security Management System
	TS EN ISO 22301 Business Continuity Management
	TS ISO/IEC 20000-1 Information Technology Service Management System
	TS ISO/IEC 27017 Information Security Management System in Cloud Services
	TS ISO/IEC 27701 Personal Data Management System

- **Penetration Tests must be completed.**
  Penetration tests must be conducted in accordance with the Information Systems Penetration Tests Procedures and Principles annexed to the Communiqué and the results must be eliminated. These tests must have been conducted within 1 (one) year as of the application to be made to the CBRT.

- **Risk Management Framework with Policies and Procedures needs to be established.**
  It is mandatory to establish policies, procedures and process documents in writing that include the procedures and principles regarding the measures to be implemented and the controls to be established in order to ensure that all risks that may jeopardise the smooth operation of information systems are identified, measured, monitored and effectively executed. In this context, it is mandatory to have a risk management framework approved by the Company's Board of Directors.

- **Data Centers must be set up in Türkiye.**

Burhaniye Abdullahağa Cd., Merdiven Çıkmazı Sk., No:2, Üsküdar, İstanbul
T +90 216 700 1833
F +90 216 700 1834
www.koksalpartners.com

The primary and secondary systems and data backup centres dedicated to the community cloud service must be located in Turkey.

B. Application to the CBRT and Assessment

Pursuant to the Guideline, external service providers that intend to provide community cloud services and fulfil the criteria set out in Article 16/7 of the Communiqué are required to apply to the CBRT with the information and documents listed below:

- Documents indicating that the requirements listed in Article 16/7 of the Communiqué have been fulfilled
- A risk assessment report conducted within the last 1 (one) year
- Documents indicating information systems architecture and network topology
- Management and organizational chart and personnel data
- Information on external services received
- Information on services provided as an external service provider
- Information on the organizations to which external services are currently provided
- Information on services provided within the scope of community cloud
- Contact details

Upon submission of the listed documents to the CBRT the application will be submitted and the eligibility assessment process will begin. Following the finalization of the assessment, the CBRT will notify the result in writing.

C. Compliance Oversight

Following a positive assessment by the CBRT, the external service provider will be able to provide services. There are also a number of rules that providers are obliged to comply with during the provision of services. The external service providers are obligated;

- to notify the CBRT without delay of any significant changes in the information and documents submitted to the CBRT at the time of application. In any case, the documents shall be updated at least once every 2 (two) years.
- to conduct penetration tests at least once per calendar year and to notify the CBRT of the results of these tests and the actions undertaken.
- to conduct a risk assessment of its information systems at least once a year and report the results of this assessment to the CBRT.
- To notify the outsourcing service provider is obliged to notify the CBRT of any structural problems and outages within 12 hours at the latest.

D. Enforcement

Burhaniye Abdullahağa Cd., Merdiven Çıkmazı
Sk., No:2, Üsküdar, İstanbul
T +90 216 700 1833
F +90 216 700 1834
www.koksalpartners.com

With the latest updates, the Guideline has been implemented as of September 4, 2023. External service providers who intend to or currently providing community cloud services are obliged to comply with the latest version of the Guideline by 31 December 2024.