On-line Banking in the Cloud

BankGemini would like to move their online banking services to the cloud because of the advantages in cost savings, usage-based billing, business continuity and agility.

These online banking services include a wide range of banking operations: debit and credit cards management, display of the bank statement, national and international money transfers, utility bills and taxes payment, phone credit charging, loans and online trading. Customers should be able to access these services via a web application or via a mobile application.

BankGemini must consider issues around security and regulatory compliance. The confidentiality and security of financial and personal data and mission-critical applications is paramount. BankGemini cannot afford the risk of a security breach. In addition, many banking regulators require that financial data for banking customers stay in their home country. Certain compliance regulations require that data not be intermixed with other data, such as on shared servers or databases. As a result, BankGemini must have a clear understanding of where their data resides in the cloud.

To help companies in their choice of a Cloud Provider, the European Commission has drafted a recommendation for number of technical requirements to consider and its legal arm has also published a list of issues to consider in terms of Data Protection Compliance.

The technical requirements identified by the EU Commission are listed below: [1]

1. **Performance:** Availability, Response time, Capacity, Capability, Support, Reversibility and the Termination Process
2. **Security:** Service reliability, Authentication and Authorization, Cryptography, Security Incident management and reporting, Logging and monitoring, Auditing and security verification, Vulnerability Management, Service changes
3. **Data Management:** Data Classification (customer, provider, derived data), Cloud service customer data mirroring, backup and restore, Data lifecycle, Data portability
4. **Personal data protection:** Codes of conduct, standards and certifications, Purpose specification, Data minimization, Use, retention and disclosure limitation, Openess, transparency and notice, Accountability , Geographical location of cloud service customer data, Intervenability

The general legal and data protection compliance requirements are listed below[2]

1. Details on the (extent and modalities of the) client's instructions to be issued to the provider, with particular regard to the applicable SLAs (which should be objective and measurable) and the relevant penalties (financial or otherwise including the ability to sue the provider in case of non-compliance).

---

[1] Requirements derived fromEU Commission, Cloud Service Level Agreement Standarditazion Guidelines:available at the link http://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines

[2] Derived from Opinion 05/2012 on Cloud Computing – Article 29 Data Protection Working Party (art. 30 of Directive 95/46/EC art. 15 of Directiv 2002/58/EC), available at the link http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

2. Specification of security measures that the cloud provider must comply with, depending on the risks represented by the processing and the nature of the data to be protected. It is of great importance that concrete technical and organizational measures are specified. This is without prejudice to the application of more stringent measures, if any, that may be envisaged under the client's national law.
3. Subject and time frame of the cloud service to be provided by the cloud provider, extent, manner and purpose of the processing of personal data by the cloud provider as well as the types of personal data processed.
4. Specification of the conditions for returning the (personal) data or destroying the data once the service is concluded. Furthermore, it must be ensured that personal data are erased securely at the request of the cloud client.
5. Inclusion of a confidentiality clause, binding both upon the cloud provider and any of its employees who may be able to access the data. Only authorized persons can have access to data.
6. Obligation on the provider's part to support the client in facilitating exercise of data subjects' rights to access, correct or delete their data.
7. The contract should expressly establish that the cloud provider may not communicate the data to third parties, even for preservation purposes unless it is provided for in the contract that there will besubcontractors. The contract should specify that subprocessors may only be commissioned on the basis of a consent that can be generally given by the controller in line with a clear duty for the processor to inform the controller of any intended changes in this regard with the controller retaining at all times the possibility to object to such changes or to terminate the contract. There should be a clear obligation of the cloud provider to name all the subcontractors commissioned (e.g., in a public digital register). It must be ensured that contracts between cloud provider and subcontractor reflect the stipulations of the contract between cloud client and cloud provider (i.e. that sub-processors are subject to the same contractual duties than the cloud provider). In particular, it must be guaranteed that both cloud provider and all subcontractors shall act only on instructions from the cloud client. As explained in the chapter on sub-processing the chain of liability should be clearly set in the contract. It should set out the obligation on the part of the processor to frame international transfers, for instance by signing contracts with sub-processors, based on the 2010/87/EU standard contractual clauses.
8. Clarification of the responsibilities of the cloud provider to notify the cloud client in the event of any data breach which affects the cloud client's data.
9. Obligation of the cloud provider to provide a list of locations in which the data may be processed.
10. The controller's rights to monitor and the cloud provider's corresponding obligations to cooperate.
11. It should be contractually fixed that the cloud provider must inform the client about relevant changes concerning the respective cloud service such as the implementation of additional functions.
12. The contract should provide for logging and auditing of relevant processing operations on personal data that are performed by the cloud provider or the subcontractors.
13. Notification of cloud client about any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.
14. A general obligation on the provider's part to give assurance that its internal organisation and data processing arrangements (and those of its sub-processors, if any) are compliant with the applicable national and international legal requirements and standards

Therefore, BankGemini must select the right cloud service provider that offers services deployment, and operating models to address security and compliance concerns.