UNSC GWG

Global Platform of Data, Services and Applications (GP)

Platform Security

1. Security
   1. General Security Requirements

| Ref | Description | Type | Priority |
| --- | --- | --- | --- |
|  | The data must be processed at all times in accordance with the European directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. | Non-functional | Must Have |
|  | The Supplier MUST provide detailed Recovery Time Objectives (RTOs) for their Cloud infrastructure components. | Non-functional | Must Have |
|  | The Supplier MUST provide detailed Recovery Point Objectives (RPOs) for their Cloud infrastructure components. | Non-functional | Must Have |
|  | The Supplier MUST assure the data owner that they provide full disclosure (aka ‘transparency’) regarding security practices and procedures as stated in their SLAs. | Non-functional | Must Have |
|  | The Supplier MUST ensure their ability to identify on request the geographical location of data. | Non-functional | Must Have |
|  | The Supplier MUST warrant the denial of access to data as a fundamental philosophy (i.e., “Default Deny All”). This specifically applies to cloud services employees and their customers other than the data owner’s employees and authorised personnel. | Non-functional | Must Have |
|  | The Supplier MUST ensure that location of operational data is stored in the European Economic Area only. Examples of operational data are audit logs, security logs, invoicing. | Non-functional | Must Have |
|  | The Supplier MUST support AES 256 SSL or TLS encryption or equivalent for the all transactions (not just login) | Non-functional | Must Have |
|  | The Supplier MUST actively monitor intrusion attempts, failed logins, and provide log information on all access attempts on request | Non-functional | Must Have |
|  | The Supplier MUST ensure secure procedures exist for identifying and liaising with customer system administrators / privileged users ( e.g. forgotten passwords ) | Non-functional | Must Have |
|  | The Supplier MUST ensure it has secure procedures to mitigate threats from social engineering (e.g. Impersonation of administrator) | Non-functional | Must Have |
|  | The Supplier MUST have password policies that are highly configurable | Non-functional | Must Have |
|  | The Supplier MUST accept a contractual commitment to assist with forensics requests in the event of a data breach. | Non-functional | Must Have |
|  | The Supplier MUST have the numbers of staff whose duties and related elevated privileges enable them to access customer data are at the minimum necessary | Non-functional | Must Have |
|  | The Supplier MUST detail the number and geographical location of staff with elevated privileges specified in the contract | Non-functional | Must Have |
|  | The Supplier MUST provide information on any 3rd party dependencies for core services | Non-functional | Must Have |
|  | The Supplier MUST have security testing and QA (vulnerability testing) processes are in place for application development | Non-functional | Must Have |
|  | The Supplier MUST have systems and procedures for regular audit of system admin / privileged user activity. | Non-functional | Must Have |
|  | The service SHOULD meet ISO/IEC 27018:2014 - Information technology - Security techniques - Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors, or equivalent  http://www.iso27001security.com/html/27018.html | Non-functional | Should Have |
|  | The Supplier MUST provide details of all relevant certifications along with expiration and renewal dates | Non-functional | Must Have |
|  | The Supplier MUST provide a list of the data protection codes of conduct, standards and certification mechanisms that the service complies with | Non-functional | Must Have |
|  | The Supplier MUST have robust compartmentalisation of job duties, perform background checks, require / enforce non-disclosure agreements for employees, and limit employee knowledge of customers to that which is absolutely needed to perform job duties. | Non-functional | Must Have |
|  | The Supplier MUST provide details of their patch management policies and procedures and how these may impact their environments. This understanding should be reflected in the contract. | Non-functional | Must Have |
|  | The Supplier MUST provide details on how the contracting authority can audit their service. | Non-functional | Must Have |
|  | Please provide details on subcontracting or arrangements with third parties used in the provision of your service? This should include any remote administration or remote storage of data, e.g. Backups. | Non-functional | Must Have |
|  | The Supplier MUST support the Safe Harbor Protocol for any data located in the USA | Non-functional | Must Have |
|  | The Supplier MUST state if the Patriot Act applies to any of the service components | Non-functional | Must Have |
|  | The Supplier MUST notify the contracting authority if any changes to their business mean that the Patriot Act may apply | Non-functional | Must Have |
|  | The Supplier MUST allow a designated third party to test for vulnerabilities in the system or provide a report from a third party. | Non-functional | Must Have |

* 1. Hosting Security Requirements

| Ref | Description | Type | Priority |
| --- | --- | --- | --- |
|  | The Supplier MUST provide detailed Recovery Time Objectives (RTOs) for their Cloud infrastructure components. | Non-functional | Must Have |
|  | The Supplier MUST provide detailed Recovery Point Objectives (RPOs) for their Cloud infrastructure components. | Non-functional | Must Have |
|  | The Supplier MUST perform regular data extractions to a format that MUST be usable without the Supplier. | Non-functional | Should Have |
|  | The Supplier MUST provide evidence that the data is backed up and recovery MUST be in place and effective in order to prevent data loss, unwanted data overwrite, and destruction. | Non-functional | Must Have |
|  | The Supplier MUST provide evidence that the Business Continuity Program is certified and / or mapped to internationally recognised standards such as ISO 22301 or equivalent - ″Societal Security — Business continuity management systems — Requirements″ and ISO 22313 - ″Societal Security — Business continuity management systems — Guidance″ | Non-functional | Must Have |
|  | The Supplier MUST detail the practices used for decommissioning of disks and storage devices. | Non-functional | Must Have |
|  | The Supplier MUST provide advance notification to the data owner if the data will be seized. | Non-functional | Must Have |
|  | The Supplier MUST destroy the data on request and provide evidence that there are techniques for completely and effectively locating data in the cloud, erasing / destroying data, and assuring the data has been completely removed or rendered unrecoverable. | Non-functional | Must Have |
|  | The Supplier MUST perform regular backup and recovery tests to assure that logical segregation and controls are effective. | Non-functional | Must Have |
|  | The Supplier MUST detail the data search capabilities and limitations when attempting to view ‘inside’ the dataset for data discovery. | Non-functional | Must Have |
|  | The Supplier MUST provide details on how metadata can be preserved and migrated. | Non-functional | Should Have |
|  | The Supplier MUST ensure that data is encrypted at rest | Non-functional | Must Have |
|  | The Supplier SHOULD provide a forensic image if required | Non-functional | Should Have |
|  | The Supplier MUST specify the extent and purpose of any monitoring of customer use of the system | Non-functional | Must Have |
|  | The Supplier SHOULD have a single sign-on option (SAML2 compliant) | Non-functional | Should Have |
|  | The Supplier MUST provide regular reports to the customer on threat events | Non-functional | Must Have |
|  | The Supplier MUST undertake regular penetration / vulnerability testing of its services | Non-functional | Must Have |
|  | The Supplier SHOULD make results of penetration / vulnerability tests available to its customers | Non-functional | Should Have |
|  | The Supplier SHOULD support certificates on mobile devices for authentication | Non-functional | Should Have |
|  | MUST specify the extent and purpose of any monitoring of customer use of the system/s. | Non-functional | Must Have |
|  | The Supplier MUST enforce the data owner’s access requirements. Such responsibilities should be in the contract and enforced and audited for compliance. | Non-functional | Must Have |
|  | The Supplier MUST have a secure process for creating, modifying and deleting user accounts, and for assigning privileges to those accounts | Non-functional | Must Have |
|  | The Supplier MUST provide the details of parameters that are captured within log files, what log file entries the Authority has access to and what period the log files are available for analysis. | Non-functional | Must Have |
|  | The Supplier MUST detail the roles & responsibilities related to electronic discovery, including such activities as litigation hold, discovery searches, who provides expert testimony, etc. | Non-functional | Must Have |