ACCA SOFTWARE

ENTRUSTMENT OF CLOUD SERVICES

FOREWORD

The entrusting of data in the cloud according to ISO 27017:2015 requires the verification of certain requirements for both the customer and ACCA software S.p.a.

ACCA software S.p.a. in complete transparency for the management of the services offered provides below a summary of the fulfilments referred to the Customer to those adopted by ACCA software S.p.A. as a supplier in compliance with ISO 27017: 2015.

Should you find any discrepancies with regard to what is stated below and any services offered, please inform us via our usual communication channels.

PROTOCOL FOR ENTRUSTING CLOUD SERVICES

The data stored in the cloud computing environment may be subject to access and management by ACCA software S.p.A.; to protect the customer, ACCA software S.p.A. adopts methods and processes certified by third parties in the ISO 27001, ISO 27017 and ISO 27018 areas;

1. ACCA software S.p.A. has identified the “Garante della Privacy”, “Agid” and the “Postal Police” as the relevant data protection authorities.
Should the Customer consider modifying and/or supplementing these bodies, it is obliged to define these aspects in advance in a specific agreement between the parties.
Please note that you are required to add the following to your training programmes

- the heads of functions;
- function contact persons (sys admin, security admin, etc.);
- the users of the cloud service, including the employees and contractors concerned.

Information security awareness, education and training programmes on cloud services should be formalised to management and supervisors, including those in business units.

These efforts support the effective coordination of information security activities in areas such as:

- standards and procedures for the use of cloud services;
- information security risks related to cloud services and how these risks are managed;
- risks to the network and system environment with the use of cloud services;
- legal and regulatory considerations.

2. ACCA software S.p.A. provides its cloud services on infrastructures residing within the European Economic Community and specifically at Data Centres located in the AWS Regions called Europe (Ireland eu-west-1) and Europe (Frankfurt eu-central-1).
3. ACCA software S.p.A. will notify the Customer with a 15-day notice of any impact and/or change location on the activated cloud services to other Amazon Web Services Data Centres located within the EU and compliance with the European Data Protection Directive (GDPR. 679/2016).

4. ACCA software S.p.A. classifies all information exchanged with the customer, labelling follows various levels of classification:
5. The inventory of resources that ACCA software S.p.A. carries out periodically takes into account the information about the resources associated with and stored in the cloud computing environment. The inventory records indicate where the resources are maintained.
6. Every piece of information located in ACCA software S.p.A.'s cloud is identified and labelled. A special internal procedure guarantees its application.
7. ACCA software S.p.A. adopts an appropriate allocation of information security roles and responsibilities and confirms that it is in a position to fulfil its data security roles and responsibilities.
To this end, regular risk analysis re-evaluations, vulnerability assessments and penetration tests are conducted.
The customer who considers modifying and/or supplementing ACCA software S.p.A.'s control practices is obliged to define these aspects in advance in a specific agreement between the parties.
ACCA software S.p.A. remains at the customer's complete disposal both to provide him with a record of the processing of existing services and to give him guidance on the procedure for classifying information via its website - https://www.acca.it.
8. The Customer must request information from ACCA software S.p.A. on the management of technical vulnerabilities that may affect the services provided. In any case, in this area ACCA software S.p.A. adopts its own vulnerability assessment and penetration test policy; at the express request of the Customer, ACCA software S.p.A. is able to provide documentation in this regard.
9. All access to ACCA software S.p.A.'s information systems must be secure and protected.
10. The Customer must always use sufficient authentication techniques to authenticate its users with administrator (but also user) profiles; to this end, appropriate policies adopted by ACCA software S.p.A. prevent the use of credentials that are weak or unsuitable for the purpose.
11. The Customer is responsible for verifying and ensuring that access to information in the cloud service can be restricted in accordance with its access control policy and that such restrictions are implemented by including:

- the restriction of access to cloud services; - the functions of the cloud service;
- to customer data managed by the cloud service.

12. The management process of the cloud service offered to the Customer takes into account the service access profile provided by ACCA software S.p.A., which informs the Customer of the standard access mode during service activation.
13. To use the cloud service, users must be clearly defined. To this end, ACCA software S.p.A. adopts two different profiles for customer use:

- Customer User as Administrator - administrators of the cloud service who have privileged access;
- Customer User - Users with a User profile, who can perform limited operations.

14. the Customer is obliged to verify that ACCA software S.p.A.'s management procedure for the allocation of secret authentication information, such as passwords, meets its requirements.
15. ACCA software S.p.A. adopts a specific written procedure for checking and maintaining the effectiveness of cryptographic keys for each phase of the life cycle, i.e.: generation, modification or update, storage, withdrawal, recovery, maintenance and instruction. ACCA software S.p.A. normally applies cryptographic controls on all transactions to/from the customer, with protection standards in line with the market, with periodic evaluation of the status of the certificate used.

It is up to the Customer to examine all information provided by ACCA software S.p.A. to confirm whether the encryption functionality:

- meet its policy requirements;
- are compatible with any other cryptographic protection already in use;
- are applied to data at rest and in transit and within the service.

16. ACCA software S.p.A. has specific written policies and procedures for the safe disposal or reuse of resources. If requested, ACCA software S.p.A. will provide such documents.
17. All incorrect log-on attempts are recorded. After thirty incorrect log-on attempts, access to the services is blocked for 15 minutes, subsequent attempts may be made at most once per minute for 12 hours.
18. Passwords are never recorded in plain text.
19. Access keys cannot be shared and must be unique for each user.
20. Access keys must not be kept on written media with indications that may facilitate unauthorised access by third parties.
21. ACCA software S.p.A. provides automatic backup and disaster recovery functionality for cloud services provided to its customers.
22. Every twelve months, ACCA tests its backups, verifying that they are in good condition in order to achieve safe and uncompromised recoveries.
23. All activities aimed at resolving security issues and/or usability of cloud services shall be performed by ACCA software S.p.A. personnel with appropriate permissions and delegations. Accesses will be recorded with timestamps and certified by external audits. The activities will be strictly related to solving the problem in compliance with the criteria of integrity, confidentiality, availability and authenticity.
24. Where required, each operator carrying out outdoor activities may connect to the Facilities by establishing a point-to-point virtual VPN (Virtual Private Network) connection between the operator - client - and the target *site,* following a defined and segregated path for access to the target.
25. ACCA software S.p.A. adopts a synchronisation policy for all company clocks, and periodically checks its application, to ensure that each environment is synchronised.
26. ACCA software S.p.A. adopts a network segregation policy to achieve isolation in the shared environment for the cloud service. At the express request of the customer, ACCA software S.p.A. can provide documentation in this regard.
27. The Customer must determine the information security requirements and then assess whether the services offered by ACCA software S.p.A. meet those requirements. For this assessment, the Customer may always ask ACCA software S.p.A. for information security features adopted.
28. ACCA software S.p.A. carries out development operations in a secure and dedicated environment with non-real test data. Development operations are governed by specific written procedures. At the express request of the customer, ACCA software S.p.A. is able to provide documentation in this regard.
29. The customer must include ACCA software S.p.A. in its information security policy when dealing with suppliers. This will help mitigate the risks associated with access to and management of data managed in the services offered by ACCA software S.p.A.
30. ACCA software S.p.A. has a specific written procedure for handling information security incidents.

This policy is designed to ensure a consistent and effective approach to the management of information security incidents, including the communication of security events and vulnerabilities.

The policy aims to mitigate the following risks:

- reduce the impact of information security breaches by ensuring that incidents are properly followed up.
- help identify areas for improvement to reduce the risk and impact of future incidents, decreasing the attack surface and the possibility of data breaches.

Information security incidents are to be reported as soon as possible by sending an email to cybersec@acca.it verified by the responsible personnel, an extraordinary meeting of the Incident Response Team will take place, which will decide on the appropriate corrective action and/or blocking.

In the event of a 'Data Breach', they must be reported to the DPO, who will forward them to the Personal Data Protection Authority, the 'Garante', in the means that the Garante will make known.

The definition of an 'information security incident' is an adverse event that has caused or has the potential to cause damage to ACCA software S.p.A.'s assets, reputation, customers and/or personnel, in the sense that the attacks or incidents may also be directed at or be necessary for the Processing Systems that provide the Services used by ACCA software S.p.A. itself.

An information security incident includes, but is not limited to, the following:

- loss or theft of data or information (Data Loss);
- the transfer of data or information to those who are not entitled to receive that information (Data Leakage);
- Attempts (failed or successful) to gain unauthorised access to data or archives (DataStore) of information on a computer system of the Organisation or its Customers;
- changes to information or data or to system hardware, firmware or software without authorisation and/or without the knowledge or consent of RSGSI or Management;
- Unintended interruption of a service provided by the organisation's systems;
- the unauthorised use of a system for processing or storing data by any person inside or outside the organisation;
- the action of a malware or DDOS attack.

It is therefore vital for customers and employees using the organisation's information systems and services to record and report any information security weaknesses that have been observed or suspected in the systems or services.

Security incidents must be evaluated and a decision must be made whether to classify them as information security incidents.

ACCA software S.p.A. shall respond to information security incidents in accordance with documented procedures.

The knowledge gained from analysing and resolving information security incidents must be used to reduce the likelihood or impact of future incidents.

The organisation must define and implement appropriate procedures for the identification, collection, acquisition and storage of information that can be used as evidence.

In the first instance, the analysis of incidents is the responsibility of the SOC and in case of particular difficulties of the SOC Supervisor and the RSGSI.

If the information security incident relates to personal information, whether on paper or electronically, the Data Protection Officer (DPO), in addition to those mentioned above, must be informed.
The level of impact of an information security incident will be determined according to the risk management strategy established by RSGSI, with the SOC Supervisor in consultation with the Data Subject and the DPO. A separate document will be drawn up of these meetings and strategy guidelines, which will be updated with each audit.

Of Information Security incidents, an 'Incident Report' log should be prepared and this list will form part of the annual review and Interim Audits.

Incident management concerns the intrusion, compromise and misuse of information and information resources and the continuity of critical information related to systems and processes.

The IT Services Manager (RSGSI) will maintain coverage of the incident management process in relation to the identification, assessment, management and monitoring of information security incidents, including the collection of any evidence that may be required for analysis as forensic evidence.

The IT services of ACCA software S.p.A. will ensure that only identified and authorised personnel have access to the affected systems during the incident and that all corrective actions are documented in as much detail as possible.

The knowledge gained from analysing and resolving information security incidents must be used to reduce the likelihood or impact of future incidents.

ICT Managers will regularly review information security incidents by conducting an ex post review of the incident.

The types and volumes of incidents and costs incurred during the occurrence of incidents will be analysed to identify any patterns or trends (downward or upward).

In the event of an upward trend, security countermeasures will obviously have to be reviewed (Review).

The IT Service Manager (RSGSI) will share this analysis, where appropriate, with the designated 'Reporting Point' (SOC Supervisor or NOC Supervisor) to assist the automatic alerting process for the organisation and establish Warning and Critical mechanisms in line with the needs identified for better and more timely intervention.

31. All data handled in transit or not are encrypted by ACCA software S.p.A.. For data in transit, TLS 1.2 or higher encryption is used. Otherwise, AES 256 encryption or later is used.
32. The Customer must consider that relevant Laws and Regulations may be those of the jurisdictions that govern ACCA software S.p.A., in addition to those that govern him.
33. The customer must request evidence of ACCA software S.p.A.'s compliance with the relevant regulations and standards required for its activities. Such evidence may be certifications produced by third-party auditors in ISO or management models displayed at https://www.acca.it .
34. In the event of force majeure - natural disasters, terrorist events, or any reasonably unforeseeable catastrophic event, resulting from determining events, and in turn reasonably unforeseeable to the structures deployed for the provision of the Cloud services of the customers, if Disaster Recovery subscription is foreseen, these will be migrated to another DC specified in the contractual phase.
35. Please note that the Customer must define or extend its existing policies and procedures in accordance with its use of cloud services and make service users aware of their roles and responsibilities in the use of the cloud service.
36. Data stored on ACCA software S.p.A.'s servers will always be the property of the Customer.
37. ACCA software S.p.A. grants the possibility of downloading a copy of the data at any time and in complete autonomy and declares with the utmost transparency the physical location where the data reside.
38. ACCA facilitates portability in case the customer decides to migrate applications and data from one cloud environment to another avoiding 'vendor lock-in'.
39. The Customer must ask ACCA software S.p.A. for a documented description of the service termination process covering the removal of the Customer's resources followed by the deletion of all copies of such resources from ACCA software S.p.A.'s systems. To this end, ACCA software S.p.A. has a specific written procedure for the termination of the service, including how to return data (where necessary).

40. Outline and main annexes of an ACCA software S.p.A. cloud computing services contract:
    - Background and Definitions;
    - Subject and Purpose;
    - Technical specifications of the service entrusted to one or more annexes;
    - Arrangements for finalising the contract;
    - Levels and Modalities of Service Maintenance and Support;
    - Fees (pay for use or fees for differentiated services);
    - Supplier Responsibility and Customer Responsibility (possible suspension of service);
    - Withdrawal and termination (with express termination clause);
    - Confidentiality obligations (including after the conclusion of the contract);
    - Ownership and licensing of the services covered by the contract (software also of third parties, domain
    - names, logos, etc.);
    - Pathological phase (disputes, bankruptcy of the service provider and the customer etc.);
    - Communication modalities and data protection;
    - Contract Amendments and Contract Assignment;
    - Duration of the contract;
    - Applicable Law and Competent Judge (or Arbitrator);
    - SLAs [service levels on accessibility to the platform, service levels on recovery modes, service levels on support time (and resolution) in the event of utilisation problems, levels of platform usability and verification of possible slowdowns in service provision, service levels on data (and document) maintenance, etc.] and penalties (and possible limits on compensation).
    - Admissibility also in the case of gross negligence or violation of minimum, necessary or appropriate security measures);
    - Platform Use Policy;
    - Privacy Policy with appointment of the cloud provider as Data Processor; - Data Privacy Officer - privacy@acca.it;
    - Definition of security measures to protect the platform (definition of policies to prevent unauthorised access with definition of functional techniques for access control and data integrity verification and monitoring/reporting in the event of unauthorised access with possible partial loss of data);
    - Technical specifications on solutions provided and technology used;
    - Any certifications obtained.

41. ACCA software S.p.A. undertakes that all information, concepts, ideas, procedures, methods and/or technical data of which the personnel used by it will become aware in the performance of the service are considered confidential and covered by secrecy.

Lastly, ACCA software S.p.A. agrees not to disclose, communicate or disseminate the data acquired by it as a result of the activities referred to in this procedure, nor otherwise use them for the promotion and marketing of its services.

ACCA software S.p.A. undertakes to take all necessary precautions with its employees and consultants to protect the confidentiality of such information and/or documentation and to sign an appropriate confidentiality agreement at the start of the services.

ACCA software S.p.A. complies with the legislation on the processing of personal data and the rights of individuals and other subjects in accordance with the Personal Data Protection Code (Legislative Decree 196/03 and subsequent amendments and Regulation 2016/679 and its applications).

42. The termination of cloud services follows a flow divided into five states.
    a.i. Receipt by PEC of the request for termination of the service(s) by the Customer
    a.ii. Customer status check and contract duration
    a.iii. Technical Verifications iv. Termination of service/services
    a.iv. Sending notice by PEC to the Customer of the termination.

Depending on the specific purpose of the processing, retention periods are set by law (24 months for the retention of telephone records, for instance).

ACCA software S.p.A. complies with the right to be forgotten under Article 17 of the GDPR is the right to the deletion of a natural person's data, which is also extended and regulated with reference to the digital society.

The right to deletion therefore prevails over the interest in storage: in the cases provided for, if a data subject requests the deletion of his or her data ACCA software S.p.A. will proceed without undue delay, and therefore without reserving the right to continue processing the data until the originally established expiry date, whether or not it is imminent.

43. ACCA software S.p.A. adopts hardening, i.e., the strengthening of installed platforms from a security point of view.
44. All communication provided by ACCA software S.p.A. takes place via HTTPS, SSL and TLS protocols, ensuring that the transmitted data reaches the correct destination.
45. ACCA software S.p.A. records the logs of all backup restores on special repositories.
46. ACCA software S.p.A. ensures limited use of paper material. The material in turn is destroyed through shredding.
47. ACCA software S.p.A. ensures that copies of security policies and operating procedures are maintained for a period of 12 months.