Data Security in the UK

VERSION: 1.1
DATE: 25/11/2019
CLASSIFICATION: EXTERNAL

FCM TRAVEL SOLUTIONS

Table of Contents

Introduction

INTENT & SCOPE

The purpose of this document is to provide a high-level summary demonstrating our commitment to Information Security within our organisation, and to address client concerns related to security and data protection.

This document focuses on what FCM Travel Solutions in the UK is doing from a security and data protection perspective, with emphasis on areas where we are surpassing our competitors.

ASSUMPTION

No assumptions are made as to the nature of the reader of this document.

DISTRIBUTION

On demand from Flight Centre and under Flight Centre NDA with the receiving party.

CONTACT

This document is under the responsibility of the Data Protection Officer. For further information regarding the details of this document, the Data Protection Officer may be reached at: Data.Protection@uk.fcm.travel

GLOSSARY

Item	Meaning
CAB	• Change Approval Board • Team of key stakeholders that reviews and approves all changes prior to deployment to Flight Centre Travel Group.
DPO	• Data Protection Officer • Role responsible for maintaining compliance with local data protection laws, including GDPR.
FCM	• FCM Travel Solutions • A brand of the Flight Centre Travel Group. • FCM is a global travel management company partnering with global corporate companies with multinational spend requirements.
FCTG	• Flight Centre Travel Group • Flight Centre (UK) Limited's parent company.
FC(UK)L	• Flight Centre (UK) Limited
GDPR	• General Data Protection Regulations • A set of European Union data protection laws and regulations.
GDS	• Global Distribution System • Platform used by travel agents to access airline, hotel, and other travel-related content and inventory.
HUB	• The FCM version of the travel portal. Users can access profiles, bookings, reporting, approval, expense, and other tools in the portal.
IDS	• Intrusion Detection System • Software that monitors malicious activity on a network or system.
IPS	• Intrusion Prevention System • Software that monitors a network or system to detect and prevent identified threats.
ISMF	• Information Security Management Forum • FCTG's senior executives responsible and accountable for Information Security within the organisation.
ISMS	• Information Security Management System • FCTG's system of policies, processes, and procedures governing Information Security within the organisation.
ISO 27001	• International standards providing specifications for a best-practice Information Security Management System (ISMS).
NDA	• Non-Disclosure Agreement
OBT	• Online Booking Tool
PCI-DSS	• Payment Card Industry-Data Security Standard • Data Security Standard managed by the Payment Card Industry-Security Standards Council (PCI-SSC). This is a set of international information security requirements that apply to all companies accepting credit card payments.
SDLC	• Software Development Life Cycle • Process for designing, developing, and testing software

Governance, Risk, & Compliance

IS THERE A FORMAL SET OF POLICIES WHICH ARE SPONSORED AT EXECUTIVE LEVEL?

FCM in the UK has established an ISO 27001:2013 compliant Information Security Management System (ISMS) which outlines key policies, processes, and procedures for maintaining information security within the organisation. These are continually and regularly reviewed and vetted by internal and external auditors, ensuring that our security approach is dynamic and vigilant, not complacent and stagnant. Our top leadership has formed the Information Security Management Forum (ISMF) consisting of senior executives from our Legal, Data Protection, IT, Operations, HR, and Property Departments which oversee security throughout our organisation and sponsor the ISMS.

WHAT SECURITY STANDARDS DOES FCM MEET?

FCM in the UK is compliant to PCI-DSS, version 3.2 and GDPR-compliant for data protection and privacy. We are also certified to the ISO 9000 standard for quality and ISO 27001 standard for information security management. Relevant certifications can be provided upon request.

HOW OFTEN IS THE SECURITY PROGRAMME AUDITED?

Our IT security policies are regularly audited to ensure they are up to date and effective. At the very minimum, these policies and plans are audited annually as part of ISO 27001 certification and PCI-DSS compliance processes.

ARE CLIENTS PERMITTED TO CONDUCT SECURITY AUDITS OR ASSESSMENTS OF FCM SYSTEMS AND FACILITIES?

We will allow client auditors to review architecture diagrams while on-site and to inspect our data-processing facilities, provided that copies and pictures are not taken. Where information is not subject to confidentiality restrictions owed to third parties, we will make available to the client on request information necessary to demonstrate compliance with contracts. To protect the confidentiality of our clients, FCM is unable to share any classified documents, security assessments, or audit reports with external parties. We also cannot allow customers to directly audit our systems or environment through penetration or vulnerability testing.

HOW DOES FCM ENSURE THIRD PARTY SERVICE PROVIDERS ARE ALSO FOLLOWING FCM'S SECURITY STANDARDS?

We carefully and systematically evaluate all our third-party service providers to ensure that we protect the confidentiality, integrity, availability, and auditability of our information assets. Before we officially engage with any service provider, we use comprehensive security risk assessments to make sure all our security requirements, ranging from up-time, classification, encryption, backup and recovery, etc are met and these requirements are clearly defined in all our contracts with service providers. We also have ongoing internal review processes to ensure the terms of the relationship are met and maintained. This includes review of service providers' yearly certification and audit reports, such as SSAE-18 SOC1, SOC2, and ongoing PCI-DSS Attestation of Compliance, and ISO 27001 maintenance.

ARE ALL PARTIES REQUIRED TO SIGN NON-DISCLOSURE AGREEMENTS AND/OR CONTRACTUAL CONFIDENTIALITY REQUIREMENTS BEFORE SENSITIVE INFORMATION IS SHARED?

Yes, all employees, third party service providers, and clients are either bound by contractual confidentiality clauses or are required to sign Non-Disclosure Agreements before they can have access to our information assets.

IT, Network, & Infrastructure Security

DOES FCM HAVE AN ACCESS CONTROL POLICY?

Yes, we have an Access Control Policy which outlines physical, technical, and organisational controls to limit user access on a roles and least privileged basis. Controls include (but are not limited to): segregation of duties, accountability for users with privileged access, log monitoring, password management, and teleworking. Our access controls operate on a need-to-know basis, with the default to deny access unless expressly justified and specifically permitted.

IS THERE A PASSWORD MANAGEMENT POLICY?

In line with PCI-DSS requirements, user passwords to authenticate and access FCM systems are required to contain a minimum of 8 alphanumeric characters with at least 1 number, 1 upper case, and lowercase characters including special characters. Passwords expire every 90 days and the last 5 passwords cannot be repeated. Account access is temporary suspended after 6 attempts, and the account remains locked for 30 minutes. Passwords as keyed in the system are masked on entry and cannot be revealed to any roles within the system.

IS THERE AN ASSET MANAGEMENT POLICY?

Yes, we have an asset management policy that establishes rules for the control of hardware, software, applications, and information assets used by the company. The policy includes assigning asset ownership, maintaining up-to-date inventories of assets, and returning assets. This policy has an owner responsible for approving and reviewing access to assets, under the responsibility of the CIO.

DOES FCM HAVE POLICIES GOVERNING THE USE OF REMOVABLE MEDIA?

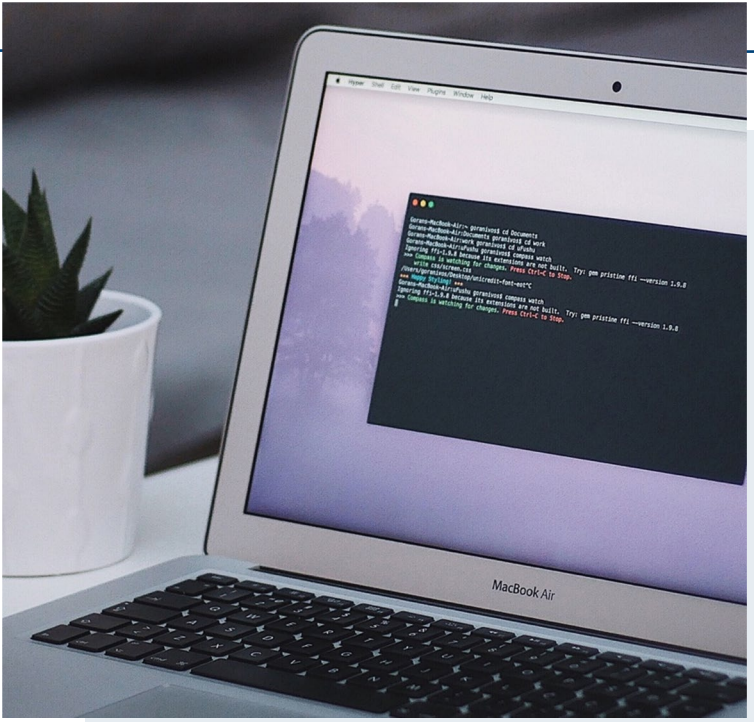
Yes, FCM has documented policies which outline the security of removable media. We maintain an inventory of removable media as part of our Asset Register and data on physical media must be encrypted according to its classification. No critical or sensitive client data are to be stored on removable media. Production data are not permitted for reuse in any other environment.

ARE PROCEDURES IN PLACE FOR REUSE OR DISPOSAL OF REMOVABLE MEDIA?

Media that may contain confidential, personal, or operational information must be obscured, erased, destroyed, or rendered unusable prior to disposal. We perform validation checks on a regular basis to ensure sensitive information is rendered inaccessible. We track and document all media reuse and destruction practices.

DOES FCM HAVE A POLICY TO MANAGE MOBILE DEVICES?

Yes, Mobile Device Management and commercial grade software solutions are implemented to enable remote wiping of devices and mitigate the risks of malicious code and unauthorised access. The Mobile Device Policy is governed under the Acceptable Use Policy which establishes requirements for approval to use company mobile devices, including laptops and cell phones. These are provisioned according to roles-based privileges. Bring Your Own Device (BYOD) is prohibited across FCM and no client data is to be stored locally on mobile devices.



DOES FCM HAVE AN ENCRYPTION POLICY? HOW IS INFORMATION SENT SECURELY OVER THE NETWORK?

Yes, our Encryption Policy requires that any customer sensitive data sent across the company network must be encrypted. These include remote access sessions over VPN tunnels, web applications, and email. Encryption is implemented for data at rest (in storage) and in transit, and at both the disk and column level. At present, data in transit is encrypted using TLS v1.2 and data at rest is encrypted to the AES 256 standard. The Encryption Policy also covers key generation, storage, expiry, compromise, revocation, and conveyance.

We implement additional technical measures to ensure that information is securely sent over the network. We forbid any physical transfers of backup media. We use Secure File Transfer Protocol (SFTP) when setting up client profile data transfers. The network is also protected by best in class IDS and IPS.

IS THERE AN ANTI-MALWARE POLICY? ARE ALL SYSTEMS PROTECTED FROM VIRUSES & MALWARE?

Yes, we have an Anti-Malware policy. We recognise the need for ensuring the cyber-security of information systems. We review this policy at least annually or whenever a major change takes place to ensure the ongoing effectiveness of our solutions. To pre-emptively combat and minimise the risk of infiltration and malicious activity, we utilise leading edge commercial grade anti-virus/malware solutions such as McAfee and Symantec, firewalls, and Intrusion Protection and Detection Solutions for all our systems, networks, and endpoints. Other measures taken to reduce our exposure to threats include web browsing and email attachment scanning through tools such as Mimecast, as well as restricting users' ability to install unapproved software on their devices.

DOES FCM HAVE MEASURES IN PLACE TO PRODUCE AN AUDIT TRAIL IN THE CASE OF SYSTEM MISUSE?

Yes, we have appropriate measures in place to monitor, log, and document user activity, including when data is entered, modified, and removed (deleted), and by whom. The following measures are implemented:

- Documentation of administration activities (user account setup, change management, access and authorisation procedures)
- Archiving of password-reset and access requests
- System log-files enabled by default and logging of events types
- Storage of audit logs to enable audit trail analysis
- Centralisation of audit logs to correlate incidents across systems

We prevent tampering of audit logs by writing to secure servers which can only be accessed through multi-factor authorisation. Even privileged users are denied access without this authorisation.

ARE TESTS AND SCANNED PERFORMED REGULARLY TO ENSURE THE SECURITY OF FCM SYSTEMS?

Yes, the security of our systems is regularly tested, and any issues remediated accordingly. Internal vulnerability scans are conducted at least weekly and external vulnerability scans are conducted quarterly. Penetration tests performed by external third-party testers are carried out at least annually and during any infrastructure changes.

HOW DOES FCM ENSURE EFFECTIVE CHANGE MANAGEMENT?

We recognise that change in our organisation and practices must be carefully implemented within a developed security framework to prevent business disruption and exposure to risks. We have a formal Change Control Policy to establish the rules for creation, evaluation, implementation, and tracking of changes made to our information resources. We have a Change Approval Board (CAB) consisting of key stakeholders from Business, Enterprise Risk, and Technology. Our CAB must review and approve all changes and their respective risk assessments, before any changes are deployed to servers, applications, networks, firmware, or hardware.

IF USING CLOUD SERVICES, HOW IS THE SECURITY ENSURED?

FCM only employs cloud service providers that meet the highest standards in data management. Our primary cloud service provider MS Azure is ISO 27001 certified and follows industry-standard best practices in data encryption and data controls. As with all our third-party service providers, cloud service providers are annually reviewed.

DOES FCM HAVE MULTIPLE FAIL-OVER SOLUTIONS FOR HOSTED NETWORKS AND SERVERS?

Our hosted networks and servers have built-in high availability, redundancy, and load balancing solutions to our system, thereby supporting the network in the case of failover and recovery.

WHAT IS FCM'S DISASTER RECOVERY STRATEGY FOR DATA CENTRES?

FCM maintains appropriate levels of redundancy and fault tolerance for accidental destruction or loss of data, including:

- Extensive and comprehensive backup and recovery management systems
- Documented disaster recovery and business continuity plans and systems
- Storage and archive policies
- Data centres are appropriately equipped according to risk, including physically separated backup data centres, uninterruptible power supplies (backup generators), fail redundant hardware and network systems and alarm and security systems (smoke, fire, water)
- Network built to N+1 redundancy level throughout
- Server clustering used in most applications to protect against hardware failures
- Mirror of hard disks is used in all systems (e.g. RAID), in both local storage and SAN-based storage environments
- On-site UPS systems provide uninterrupted power to platforms and on-site generator systems provide long-term power in the event of a prolonged outage
- All critical systems have failed redundant services running in parallel in a secondary data centre

DOES FCM HAVE CLEARLY DEFINED AND DOCUMENTED BACKUP PROCEDURES FOR FCM SYSTEMS?

Yes. Regular system backups mitigate the impact of information loss on our business. We have documented backup policies based on classification and criticality levels which define the information to be backed up and the frequency of backups.

These include:

MS Azure - Our backup archives are stored externally using Microsoft Azure backup solutions. Full backups are made daily with a 15-minute incremental backup interval. Backups are encrypted.

GDS backup - All GDS systems are backed up daily and all information is stored in case of system faults.

FCM data files backup - FCM data files are backed up on a separate system in case of system error and to protect data integrity.

Server backup - Servers are backed up regularly with standardised backup software which allows for the restoration of data on any of the appropriate servers. We have a fully tested plan for all systems with redundancy servers as backup in the event of a major disaster.

DOES FCM HAVE A PERIMETER FIREWALL IN PLACE? ARE RULES REVIEWED REGULARLY?

Yes, network segregation is enforced using a firewall and rulesets that only allows authorised traffic to pass through. Rules are reviewed semi-annually.

Application security

DOES FCM HAVE A FORMAL SOFTWARE DEVELOPMENT LIFE CYCLE (SDLC) IN PLACE?

Yes, we have a formal SDLC process, policy, and procedure in place which recognises the importance of security in each phase of development. The SDLC follows these standards and frameworks:

- Australian Government National Information Privacy Principles
- Data protection by design and default
- PCI-DSS
- Open Web Application Security Project (OWASP)
- ISO 27001/2
- ISO/IEC 27034

Where third party software development may be involved, these must also adhere to our SDLC process, policy, and procedure.

ARE SEPARATE ENVIRONMENTS MAINTAINED FOR DEVELOPMENT, TESTING, USER ACCEPTANCE TESTING (UAT), AND PRODUCTION?

Yes, development, test and production environments are physically separated on different servers. Further to this, live or non-anonymised data is never used in development or testing.

IS PRODUCTION DATA USED IN TESTING?

No. In line with best SDLC practices, FCTG does not use production or live data in testing and system development. Only testing, sample, and dummy data are used.

ARE CODE REVIEWS OR TESTS PERFORMED PRIOR TO RELEASE INTO PRODUCTION?

Yes. We rigorously test our application code according to OWASP security standards prior to release. Our dynamic and static analyses are used to find security issues caused by the code's interaction with other system components like SQL databases, application servers, or web services. Additional testing is also performed, such as penetration testing, validating server configuration, and source code reviews.

ARE CLIENT TRAVELLER PROFILES HOSTED IN A MULTI-TENANT OR SINGLE-TENANT ENVIRONMENT? WHAT CONTROLS ARE IN PLACE TO PREVENT CROSS-ENVIRONMENT DATA LOSS?

The travel portal is hosted in a multi-tenant environment with high availability. Client data is logically separated within the environment. Controls preventing cross-environmental data loss include access control whereby only authorised personnel is permitted to access the environment via user login and password, and audit trails to ensure file integrity management.

HOW DOES FCM ENSURE THE SECURITY OF FCM APPLICATIONS?

HUB is secured and protected in the cloud environment by virtual firewall appliance. Client data is logically separated with a unique customer ID/GUID and all data is encrypted at rest in AES 256. Data in transit is encrypted using TLS 1.2. Secure access to the portal can be implemented using Single Sign On via SAML for customer accounts. User passwords must align with PCI-DSS requirements. User passwords are encrypted and the portal stores hash and salt for each password.

DOES DATA REMAIN IN ARCHIVE IN THE PROFILE APPLICATION (HUB) AFTER TERMINATION OF THE TRAVEL MANAGEMENT AGREEMENT?

Yes. Traveller profile data is deleted from the live version of HUB during the de-implementation process and is thereby neither visible nor accessible by operational staff once the Travel Management Agreement ends. Nevertheless, these profiles will still exist within the HUB disaster recovery backups that are essential for our business continuity capabilities. These backups are maintained by the HUB development team and cannot be accessed, read or searched without first being restored.

Due to the risk of data corruption, we do not restore these backups and delete profile data when a client ceases trading. However, in the event we ever need to restore a backup for business continuity purposes we can run a script to delete redundant client profiles.

Data protection

IS FCM A "PROCESSOR" OR "CONTROLLER" OF DATA?

Where GDPR applies, when we process your employees' personal data for the purpose of providing contracted travel management services we do so as a "data controller".

WHAT DATA ARE COLLECTED?

We will only collect personal data in compliance with your local data protection laws. The types of data we collect include the following:

Personal data categories

Traveller profile data: Profiles can be created in HUB using the following three mandatory elements: first name, last name, and a unique email address. All other profile elements are controlled by the client, who can designate each data field as mandatory or voluntary during the implementation phase. These profile data elements can include residential address, telephone number, job title, office location, employee number, passport and visa information (including date of birth, nationality, place of birth, passport number and expiry date), driving licence number, mileage, and frequent flyer/guest card numbers.

Passenger Name Record ("PNR") Data: Master Data processed in PNR format associated with reservation data, including flight dates and routings, flight numbers, hotel reservations, car rental bookings, rail bookings, ticketing information, authorisation solutions and travel risk management.

Payment Data: Cardholder Data and bank details.

Emergency Contact Details: Name and telephone number of partners/emergency contacts.

Special category data

Sensitive Traveller Data: Dietary and medical information in connection with travel arrangements voluntarily provided by traveller.

WHY IS THIS DATA NEEDED?

The nature and categories of personal data we collect constitute the data necessary to facilitate your travel arrangements by allowing us to make bookings and arrange travel related services and products on your behalf. Without this data we would not be able to provide you the travel services you are contracting us to provide, and your employees would not receive the level of service they both deserve and rightly demand.

HOW DOES FCM RECEIVE PROFILES? IS INTEGRATION REQUIRED?

The travel portal (Hub) is a web application that clients can access via the Internet and where profiles of those individuals authorised to travel by the client are created. The receiving of profiles can occur through the following different channels: direct emailing and calling our consultants; csv files via email or SFTP; self-registration by the travel portal; xml file provided by Concur; or a direct HR feed from the client's HR database into Hub. As part of the implementation process, we will discuss these profile transfer and creation methods with the client in order to identify the most suitable method based on their needs. Of the five profile transfer and creation methods listed here, the last method (direct HR feed) constitutes integration.

IS THE DATA BEING USED BEYOND ITS ORIGINAL INTENT?

No. Our intent is to provide contracted travel management services in a safe and secure manner, that protects the personal data of your employees while meeting all the legal obligations of the countries we operate in. As such we will only process your information where:

- the processing is necessary to provide our contracted services to you;
- the processing is necessary for compliance with our legal obligations; and/or
- the processing is necessary for our legitimate interests (e.g. ensuring system security, maintaining back-ups for disaster recovery, service quality control, etc.).

WHO HAS ACCESS TO THIS DATA?

Access to personal data is role-based, with access split between staff who are providing business-as-usual travel services for existing clients, and those staff who only require access to data in order to provide specialised services. The following roles will have access to this data:

Day to Day Operations

- *The account management team:* day-to-day operations of the account which include bookings, travel assistance, and profile management
- *Finance:* managing invoicing and payments and providing financial reporting and management information reporting
- *Information Technology:* management and operation of all FCTG systems and databases that will contain client data, as well as the IT Service Desk.

On a Needs Basis

- *Out of hours help desk teams:* to assist the traveller when they contact the Out of Hours telephone support team
- *Data protection:* accessing personal data on a needs basis to support clients in meeting Subject Access Requests and addressing any data protection issues that may arise
- *Legal:* on a needs basis to address legal issues that may arise.
- *Implementation team:* during the implementation/on-boarding process

HOW IS DATA PROTECTED IN FCM SYSTEMS?

We implement and maintain appropriate technical and organisational measures (TOMs) to ensure a robust level of security when protecting the personal data of our clients and their employees from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal information transmitted, stored or otherwise processed. We regularly review our TOMs to confirm they appropriately address new and evolving threats, thereby ensuring we protect your personal data as fully as we protect our own confidential information. We will destroy or anonymise personal data once it is no longer required for our business purposes or to meet our legal requirements.

IN WHICH COUNTRIES WILL THE DATA BE STORED?

Data is hosted in the UK, Germany, Belgium, the Netherlands, and the USA. We use Microsoft Azure Cloud storage for profile and reporting data, hosted in the USA and the Netherlands. Our Azure data centres are ISO 27001 and ISO 9001 certified. Where we are required to retain all data in its originating market, we encrypt and store the data on local servers. International data transfers to our USA storage are covered under the EU-US Privacy Shield Framework.

WHAT ABOUT DATA LOCALISATION REQUIREMENTS?

FCM abides by all local data laws and requirements in the countries we operate in, as well as maintaining a global team of regional Data Protection Officers to oversee processing within their regions. Where localisation laws (and we include the GDPR as an example of a localisation law) require the implementation of storage, processing, operational and/or legal compliance measures, these are implemented. Should clients have specific concerns or localisation requirements, these can be discussed to examine and identify bespoke solutions subject to agreement on costs.

WILL CLIENT PERSONAL DATA BE SHARED WITH THIRD PARTIES?

Yes. Providing global travel management services necessitates the sharing of certain personal information from individual travellers with third parties in order to deliver their required services. For example, it is a requirement for booking hotels, airlines, and rental cars that personal information of the individual making use of these services is passed to the third-party provider at the point of booking. FCTG will only disclose your personal information to third parties in the ways set out in our Privacy Policy and in accordance with your local data protection laws. We do not and will not sell, rent out, or trade your personal information.

WILL PERSONAL DATA BE PROCESSED OUTSIDE THE EU?

Yes. At a technology/system level, a number of third-party service providers relied upon by FCTG conduct their data processing activities outside of the EU. These third parties are set out in our processor list shared with our clients. At a practical level, any time a client's employees travel outside the EU elements of their personal data will be transferred to the country they are travelling to in order to book hotels, airline tickets, rental cars, transfers, etc.

WHEN AND HOW IS DATA DELETED?

The client can request deletion of their data at any time during the provision of our services to them. We will also promptly delete and procure the deletion of client personal data upon termination of the Travel Management Agreement. Data will be deleted in such a manner such that it is irretrievable by ordinary commercially available means. Where it is not possible to delete personal information, data will be irreversibly anonymised by erasing unique identifiers which would otherwise allow data to be linked back to an individual. Clients can request a written certificate confirming that client personal information has been deleted. Where FCM is under a legal obligation to process client personal information beyond the contracted period for services, all security measures outlined herein with continue to apply.

WHAT ARE THE PROCEDURES FOR REGULAR TESTING, ASSESSMENT AND EVALUATION FOR DATA PROTECTION BY DESIGN AND DEFAULT?

We have the following processes in place, in line with GDPR and other relevant data protection legislation to help assure assessment testing and data protection by design and default:

- We use an internally developed data protection by design and default evaluation mechanism that is integrated into an upstream stage gate of our software development process. This is overseen by the relevant Data Protection Officer (DPO) who assesses the software and application to identify new changes to functionality, thereby ensuring all software meets data protection by design and default best practices.
- Downstream in the design process, the DPO has sign-off to ensure data protection requirements have been met before moving to the production environment.
- For third party software applications, we conduct a third-party security questionnaire to ensure appropriate data protection by design and default principles have been applied before the system is integrated into FCTG systems. These software applications are subject to annual audits and reviews.

WHAT IS THE PROCESS FOR SUBJECT ACCESS REQUESTS?

As per GDPR, FCM acts as controller. Any Subject Access Requests received by FCM will be actioned and completed within one month of receipt. To enable this process, we use the OneTrust application to log all Subject Access Requests and have mapped our systems to enable the effective completion of such requests.

IS FCM REGISTERED WITH THE INFORMATION COMMISSIONER'S OFFICE?

Yes, Flight Centre (UK) Limited is registered with the ICO. Our reference number is Z7994553.

Human Resources & Training

DOES FCM CARRY OUT BACKGROUND SCREENING FOR POTENTIAL EMPLOYEES?

Yes, our HR department conducts background screenings for all new hires and re-hired employees, including prior employment, criminal background checks, and references.

ARE EMPLOYEES CONTRACTUALLY OBLIGATED TO ENSURE SECURITY?

Yes, confidentiality agreements and Non-Disclosure Agreements are required for employment at FCTG. All new employees must also review and sign our IT security policies during orientation.

HAS FCM IMPLEMENTED A DATA CLASSIFICATION SYSTEM?

Yes, we have an Information Sensitivity and Classification Policy designating restricted and private information assets. This helps employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of the organisation without proper authorisation. This policy is annually reviewed.

ARE FCM EMPLOYEES AWARE OF WHAT THEY NEED TO DO TO KEEP THE ORGANISATION SAFE?

All new starters undergo initial security awareness training and all current employees must refresh this security training on an annual basis. Training is provided through an online training tool known as Compass which includes modules covering GDPR and PCI compliance as well as a wide variety of job-specific training. These training programmes are enforced by Human Resources. Participation, progress and test scores are recorded on each Compass user's dashboard. Managers can run reports to monitor progress. Compliance to security policies is also regularly audited and reviewed.

ANY DISCIPLINARY ACTIONS FOR NON-COMPLIANCE?

We notify all employees (both during hire and regularly through refresher training) that disclosure of protected information by our employees is considered gross misconduct and will be subject to dismissal at management discretion. Legal action will be taken as necessary to protect and preserve this principle.

There is a formal process for removal of duties, access rights, and privileges after verification of a breach. The employee is either terminated or provided a written warning letter of notice, depending on the circumstances. The letter is signed by the employee, their supervisor, and HR and placed in the employee's HR file. In either case, access is either removed or restricted.

LEAVER PROCESS - HOW IS INFORMATION KEPT SAFE WHEN PEOPLE LEAVE?

We expect privacy and confidentiality in respect to our company, our clients, and our supplier relationships to be observed at all times, both during and after employment with us. All employees, contractors, and third-party users are required to return their information and information assets to the organisation upon termination of their employment, contract, or agreement. All documents, information and promotional property always remain the property of FCM and must be returned by our employees upon termination of employment, or at any time when a specific request is made.

ARE PRIVILEGED ACCOUNTS CHANGED WHEN A PRIVILEGED USER CHANGES ROLE?

In line with roles-based access control and "need-to-know" principles, users' privileges are promptly changed in accordance when their roles change. Steps are undertaken to revoke any and all access, privileged or otherwise, upon the final day of employment in a particular role.

Physical Security

ARE THERE SECURITY MEASURES FOR FCM SITES?

Yes, in line with our internal policies and appropriate risk assessments, all sites have appropriate procedures. These include the use of reception, 24/7 security monitoring, and visitor policies, such as recording and supervising access of all visitors as required.

All sites have a swipe card, token, or keypad access control for staff. There are surveillance systems including alarms and, as appropriate, CCTV monitoring in the building foyer and loading areas but not within customer data processing areas. There is also a centralised key and code management which outlines card-key procedures.

Business Continuity & Disaster Recovery

A security incident can come in many forms: a malicious attacker gaining access to the network, a virus or other malware infecting computers, or even a stolen laptop containing confidential data. A well-thought-out Incident Response Policy is critical to successful recovery from an incident. Our Business Continuity and Disaster Recovery policy covers all incidents that may affect the security and integrity of the company's information assets, and outlines steps to take in the event of such an incident.

IN THE EVENT OF A SECURITY INCIDENT, HOW ARE CLIENTS NOTIFIED?

In the event of a security incident affecting client personal data, including incidents at our processors, the affected clients will be notified without undue delay, and in any event within 72 hours of the incident. Should any client information be subject to an incident or breach, communication of the event would be through the appropriate account manager unless otherwise agreed.

IS THERE A VALIDATED BUSINESS CONTINUITY PLAN OR DISASTER RECOVERY PROCEDURE? ARE THESE PROCEDURES TESTED?

Our ISO 27001:2013 certified Business Continuity Plan is designed to provide guidance in the event of a major business disruption impacting critical resources (i.e. buildings, equipment, technology, human resources and third parties) where a loss may affect the continuity of critical business functions. Our BCP is updated annually or whenever there is a major change, such as enhancements during the normal course of business or a significant organisational restructure occurs. The plan is regularly tested in both “test” and “live” environments, such as desktop exercises and physical tests.

Our focus on Business Continuity is to ensure 24X7 operations and availability of the following six critical applications/systems:

- Internet access for our consultants
- Phones access for our consultants
- Email access
- FCM Portal
- GDS access
- FCM ClientBank

We undertake the necessary risk assessments and model the outcomes to ensure that no unnecessary risks are taken. These Risk Assessments are centrally stored such that any unique records that could be vital in a post incident review would not be destroyed as part of an incident.

The strategies documented in this plan are based on the following loss scenarios, to ensure the business functions are recovered within the required Maximum Acceptable Outage:

- Loss of Building
- Loss of Staff
- Loss of Technology
- Loss of Dependencies

Appendices

GOVERNANCE: http://www.fctgl.com/investors/governance/

PRIVACY NOTICE: https://www.fcmtravel.com/en-uk/privacy-notice