World Travel Centre
Selective Travel Management

GDPR-Data
Protection Policy

Revision History

Version	Date	Revision Author	Summary of Changes
1.0	31/07/2017	Keith Raymond	Initial version
2.0	31/03/2018	Aidan Coghlan	GDPR compliant and approved version
3.0	30/04/2018	Aidan Coghlan	GDPR enhanced version
3.1	10/05/2018	Aidan Coghlan/Keith Graham	Further updates
3.2	21/05/2018	Aidan Coghlan	Further updates
3.3	22/05/2018	GDPR Team	GDPR pre May25th Final Version
3.4	05/11/2019	Keith Graham	Further updates

Contents

1 Introduction, Fundamental Approach & Definitions.

1.1 Introduction:

In its everyday business operations, World Travel Centre Group (WTCG) makes use of data about identifiable individuals. These categories of data subject include:

Travellers.
Prospective Travellers.
Current, past and prospective employees.
Website Users.

In collecting and using this data, the organisation is subject to a variety of legislation controlling how such activities may be carried out and the safeguards that must be put in place to protect it.

The purpose of this policy is to set out the relevant legislation and to describe the steps WTCG is taking to ensure that it remains fully compliant.

This control applies to all systems, people and processes that constitute the organisation's information systems, including board members, directors, employees, suppliers and other third parties who have access to WTCG systems.

In addition, we have developed a shorter GDPR FAQ document for Data Subjects and interested parties in clear and concise language.

1.2 Fundamental Approach to Data Capture, Processing & Control:

WTCG operates as a travel agent booking travel transactions for individuals personally or on behalf of other entities such as Employers, Travel Agencies, Schools, Clubs or other Corporate Bodies.

WTCG obtains, with the consent of the Data Subject, only the data required to facilitate the type of travel requested by the Data Subject or by the entities above on behalf of the Data Subject.

WTCG also obtains limited information about visitors to WTCG group websites in the ordinary course of browsing those sites. The information gathered is incidental and is not used for any data processing purpose, as outlined in section 2.4.15 Website Users

The type of data required to complete a travel transaction on behalf of a data subject is included in the list below and set out in both Summary and Detailed Form in the Appendices to this document.

Our preferred means of data capture is electronic, submitted securely by the data subject. We have procedures in place for data captured by email or telephone.

We will only seek to obtain data that is:

1. Required for travel by WTCG or other data controllers, for example Airlines, Hotels, Customs and Border Protection (CBP), Advance Passenger Information Systems (APIS) or to permit issuance of Electronic Travel Authority Visas (ETA).
2. Additional personal data such as airline frequent flyer numbers, FFNs, meal and seat preferences.
3. Contact information such as mobile telephone numbers and email addresses for the express and sole purpose of fulfilling our customer service obligations for a specific travel transaction undertaken by the Data Subject.

Personal data is not reproduced on any documentation generated by WTCG such as invoices, statements, itineraries etc.

We do not use this contact information for any marketing purposes unless the data subject expressly gives consent to do so.

We do not share this data with 3rd parties except where there is a legal or commercial requirement for the purposes of a travel transaction requested by the Data Subject.

We do not process special category and other more sensitive data on a routine basis, but only in the following specific exceptions:

- With their consent, we will process information about a Data Subject's health condition or disability as necessary for the purposes of arranging travel in accordance with their needs. Data Subjects can choose whether to save this information in their on-line traveller profile or provide it to us in relation to a specific travel transaction;

- With their consent, we will process information about a Data Subject's criminal record as necessary for the purposes of assisting them (at their request) with a visa application. Data Subjects can choose to apply direct to the visa provider rather than asking for our assistance with this.

We accept and understand that Privacy by Default is in the best interests of all our data subjects and clients. Our Corporate approach to GDPR and data generally is aligned with this.

Credit card information is at a high risk of fraud. We use 3rd party providers with the highest levels of encryption and security available.

The WTCG Board of Directors and Senior Management view GDPR as part of the wider corporate value of operating to the highest technical standards. Our compliance accreditations also include:

ISO9001.

Cyber Essentials Plus.

PCI Compliance.

BREXIT

WTCG Directors have considered the possible impact of Brexit on GDPR. We have assumed that GDPR will continue to apply to the United Kingdom. The UK Government has indicated it will implement an equivalent or alternative legal mechanism. In any event WTCG will remain compliant with our GDPR obligations and local legislation in all markets where we operate.

1.3 WTC Structure Definitions:

Name	Label	Entity / Business Division
World Travel Centre Group	WTCG	World Travel Centre Holdings Ltd and Subsidiaries.
World Travel Centre Ltd.	WTC IE	World Travel Centre Ltd. Reg No: 168612. Registered Office: 43 Pearse Street, Dublin 2 D02 W085
World Travel Centre Ltd.	WTC NI	World Travel Centre Ltd. Reg No: NI010853. Registered Office: Ground Floor, Murrays Exchange, 1 Linfield Road, Belfast BT12 5DR
World Travel Centre / WTC	WTC	Travel Trade and Retail Divisions
Selective Travel Management	STM	Business Travel / Travel Management / TMC Divisions

2 Privacy and Data Protection Policy

2.1 The General Data Protection Regulation

The General Data Protection Regulation 2016 (GDPR) is one of the most significant pieces of legislation affecting the way that WTCG carries out its information processing activities. Significant fines are applicable if a breach is deemed to have occurred under the GDPR, which is designed to protect the personal data of citizens of the European Union. It is WTCG policy to ensure that our compliance with the GDPR and other relevant legislation is clear and demonstrable at all times.

2.2 GDPR Key Definitions

There are a total of 26 definitions listed within the GDPR and it is not appropriate to reproduce them all here. However, the most fundamental definitions with respect to this policy are as follows:

Personal data is defined as:

any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

'processing' means*:*

any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

'controller' means*:*

the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law

WTCG is both a processor and a controller of data in different circumstances.

2.3 WTC IT System Definitions

Section below	Name	Description	Supplier
1	Galileo GDS	GDS Global Distribution System for booking flights, hotels and car-hire.	Travelport
2	Worldspan GDS	GDS Global Distribution System for booking flights, hotels and car-hire.	Travelport
3	Amadeus GDS	GDS Global Distribution System for booking flights, hotels and car-hire.	Amadeus
4	Boss	In-house Back Office system for invoicing, processing, quality control & accounting.	WTCG In-House IT
5	Mailchimp	Third party platform Mailchimp is used for Marketing Communications only	Mailchimp
6	Realex	Credit card payment processor	Realex
7	Micropay & Sage	Payroll Software	Micropay
8	Sage	HR Software	Sage
9	Microsoft Exchange & Outlook	Email System	Microsoft
10	Mail Store	Email Archive System	Mail Store
11	Clickatell	SMS System	Clickatell
12	Survey Monkey	Third Party platform 'Survey Monkey' used for Competition Data Collection and company feedback	Survey Monkey
13	CCTV	Office security system	ICRealtime
14	IP Phone System	Office phone system	Sangoma
15	Websites	WTCG public websites	WTCG In-House IT

Only systems processing personal data are listed above.
Explanatory notes are included in section 2.4 below.
The relevant data retention and deletion policy is set out in table 2 below.

2.4 WTC IT System Notes

2.4.1 Galileo GDS

STM Clients:
Data contained in PNRs (Passenger Name Record) is generally retained for a period of 11 months for customer service purposes.

WTC Clients:
Data contained in PNRs expires on completion of the travel transaction.

STM Clients:
Personal data may be stored in traveller profile records as requested by clients to facilitate current and future trips by clients. This data is expunged annually for clients who have not booked travel with STM in the preceding 3 years.

2.4.2 Worldspan GDS

Data contained in PNRs expires on completion of the travel transaction.

2.4.3 Amadeus GDS

Data contained in PNRs expires on completion of the travel transaction.

2.4.4 Boss

Boss is the WTCG in-house front, mid and back office processing system. We have identified the various tables and data sets where personal data may be stored. This data is retained securely for record keeping purposes only. Our data retention policy for personal data is 5 years post trip except where a traveller deletion request is received. The WTCG Directors consider this to be reasonable considering customer service and legal obligations.

2.4.5 Mailchimp

Where you have explicitly consented at the time we collected your personal information or where we otherwise have a right to do so, we may also use your personal information to send you our Monthly Newsletters, Travel Alerts and other Marketing Communications, using third party email platform, MailChimp. If you choose to unsubscribe from Selective Marketing Communications your personal data will be deleted after 30 days of Selective Travel receiving this request.

Opting-in to Marketing Communications. When you opt-in to marketing communications we will ask you for the following personal details: name and email address. This information is then used to, where you have opted- in to receiving email newsletters and travel alerts.

2.4.6 Realex

WTCG use Realex for the credit card payment collection via a re-direct to a secure payments page. We do not store personal credit card info on behalf of clients.

2.4.7 Micropay & Sage Payroll

We store personal data for staff members for the purposes of payroll processing. Data for former staff members is archived following the completion of the last tax year of service of that employee.

2.4.8 Sage HR System.

We store personal data for staff members in accordance with standard HR practice. Data for former staff members is archived on completion of their employment.

2.4.9 Microsoft Exchange & Outlook

Personal data may be submitted to us by or on behalf of clients by email. Our staff are trained to use this data for the express purpose of fulfilling a travel request and to store this data in the relevant systems above. We have procedures in place to delete this data immediately on completion of the travel transaction.

2.4.10 Mail Store

WTCG emails are generally archived after 12 months. We endeavour to ensure that personal data is not archived and is deleted from the primary email system above.

2.4.11 Clickatell

We periodically send promotional SMS mailshots to clients who have booked with us in the previous 3 years. From May 25th 2018, clients will be asked to specifically opt in to such mailshots.
The subject matter of these mailshots is strictly related to the travel service previously purchased from us. All SMS mailshots contain an opt-out facility.
Clients with bookings older than 3 years have their details removed from these SMS marketing lists.

2.4.12 Survey Monkey

Selective Travel Management run competitions where subscribing to email marketing is a condition of entry. You can unsubscribe to these communications using the link in the email at any time. When entering a competition Selective Travel Management will ask you for the following personal details: name, email address, mobile phone number (not compulsory). This information is collected and stored on a third party platform called Survey Monkey. Your information will be held for 30 days post competition before being deleted.

Selective Travel Management will occasionally ask for feedback and send corporate survey questionnaires. Selective Travel Management will ask you for the following personal information: name and email address. Information is collected and stored on third party platform Survey Monkey. Your personal information will be held for 12 months before being deleted from Survey Monkeys data base.

2.4.13 IP Phone System

All telephone calls to/from our organisation are recorded for quality control and training purposes. Data Subjects may supply personal data to us by telephone. We securely retain recorded audio files for a period of 18 months in accordance with good business practice.

2.4.14 CCTV

Data Subjects may be personally identifiable from CCTV recordings which are part of our overall security measures. CCTV recordings are overwritten approximately every 2 months.

2.4.15 Website Users.

Data Subjects who access our various websites may in theory be identifiable from IP addresses used. We do not collect, collate or use this data in any way and the log files containing this data are periodically deleted.

2.5 Principles Relating to Processing of Personal Data

There are 7 fundamental principles upon which the GDPR is based.

Personal data shall be:

1 *processed lawfully, fairly and in a transparent manner in relation to the data subject **('lawfulness, fairness and transparency');***

2. *collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes **('purpose limitation')**;*

3. *adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed **('data minimisation');***

4. *accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay **('accuracy');***

5. *kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject **('storage limitation')**;*

6. *processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures **('integrity and confidentiality')**.*

7. *The controller shall be responsible for, and be able to demonstrate compliance with 1-6 above **('accountability')***

WTCG complies with all of these principles both in the processing it currently carries out and as part of the introduction of new methods of processing such as new IT systems. The operation of an information security management system (ISMS) that conforms to the ISO/IEC 27001 international standard is a key part of that commitment. World Travel Centre Limited is currently aligning its ISMS processes with a view to being ISO 27001 compliant.

2.6 Rights of the Individual

The data subject also has rights under the GDPR. These consist of:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Each of these rights must be supported by appropriate procedures within WTCG that allow the required action to be taken within the timescales stated in the GDPR.

These timescales are shown in Table 3.

2.7 Consent

All data collected and processed is necessary for a reason allowable in the GDPR. In the case of children below the age of 16 data is collected from a parent usually travelling in the same booking as the child.

This statement contains transparent information about our usage of personal data and is available to data subjects at any time, including rights regarding their data explained, such as the right to withdraw consent or have data permanently deleted.

We only collect data directly from the Data Subject or through a connected party such as an Employer or an entity contracting with us to supply travel services.

2.8 Privacy by Design

WTCG has adopted the principle of privacy by design and will ensure that the definition and planning of all new or significantly changed systems that collect or process personal data will be subject to due consideration of privacy issues, including the completion of one or more data protection impact assessments.

2.9 Transfer of Personal Data

Transfers of personal data outside the European Union must be carefully reviewed prior to the transfer taking place to ensure that they fall within the limits imposed by the GDPR. This depends partly on the European Commission's judgement as to the adequacy of the safeguards for personal data applicable in the receiving country and this may change over time.
Personal data may be transferred outside the EU for the expressed purpose of fulfilling a travel request on behalf of a data subject. For Example: Non-EU airlines, hotel providers and governments. WTCG takes all reasonable steps to ensure secure data transfer to reputable third parties.

Intra-group international data transfers must be subject to legally binding agreements referred to as Binding Corporate Rules (BCR) which provide enforceable rights for data subjects.

The following table outlines where and why data may be transferred to third parties.

Data Sharing	WTC Group	Third Party
Sensitive Data	Yes	Yes, but only in two known and specific circumstances where it is required by a service provider under 1.2.3.
Marketing Purposes	Yes	**Yes**. Third Party platform Mailchimp is used for our own marketing purposes. Data is only stored on Mailchimp server and not shared.
EU Travel Purposes	**Yes**	**Yes.** Only where we are required to do so to complete a travel request such as when requested by airlines, hotels, and car hire companies or for visa purposes i.e. only where it is necessary to enable the data subject to avail of the travel service booked.
Non EU Travel Purposes	**Yes**	**Yes.** Only to a verified travel supplier or service provider who may be situated outside the EEA and only for the expressed purpose of enabling a travel transaction. For example, non-EU airlines or US government for APIS purposes.
Other Purposes	**Yes.** Only where the data subject has submitted the data to us and consents to its retention for future use.	No

2.10 Data Protection Officer

A defined role of Data Protection Officer (DPO) is required under the GDPR if an organization is a public authority, if it performs large scale monitoring or if it processes particularly sensitive types of data on a large scale. The DPO is required to have an appropriate level of knowledge and can either be an in-house resource or outsourced to an appropriate service provider.

Based on the above criteria WTCG does not require a Data Protection Officer to be appointed.

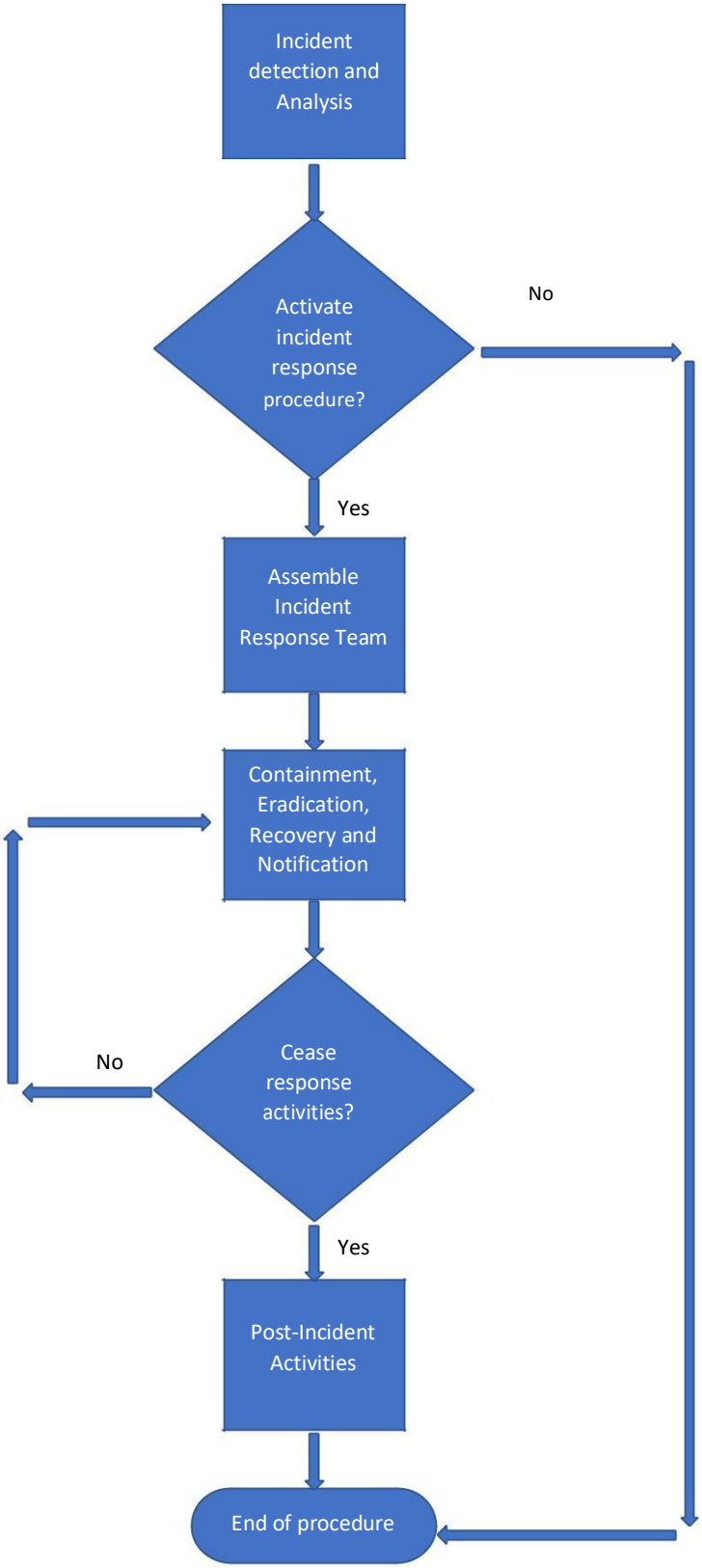
2.11 Breach Notification

It is WTCG policy to be fair and proportionate when considering the actions to be taken to inform affected parties regarding breaches of personal data. In line with the

GDPR, where a breach is known to have occurred which is likely to result in a risk to the rights and freedoms of individuals, the relevant Data Protection Authority (DPA) will be informed within 72 hours. This will be managed in accordance with our *Information Security Incident Response Procedure* which sets out the overall process of handling information security incidents.

The Personal Data Breach Notification Form is included in Appendix 5 of this document.

Information Security Incident Response Procedure:



2.12 Addressing Compliance to the GDPR

The following actions are undertaken to ensure that WTCG complies with the accountability principle of the GDPR:

The legal basis for processing personal data is clear and unambiguous

All staff involved in handling personal data understand their responsibilities for following good data protection practice

Training in data protection has been provided to all staff

Where applicable, Rules regarding consent are followed

Routes are available to data subjects wishing to exercise their rights regarding personal data and such enquiries are handled effectively

Regular reviews of procedures involving personal data are carried out

Privacy by design is adopted for all new or changed systems and processes

The following documentation of processing activities is recorded:

- Organization name and relevant details ○

Purposes of the personal data processing

- Categories of individuals and personal data processed
- Categories of personal data recipients
- Agreements and mechanisms for transfers of personal data to non-EU countries including details of controls in place
- Personal data retention schedules
- Relevant technical and organisational controls in place

These actions will be reviewed biannually as part of the management review process of the information security management system.

2.13 Data Deletion

Hard Copy Data.

We aspire to operate as a paperless business. We do however receive some paper records from third parties and these may contain personal data. All paper documentation is shredded and disposed of.

Soft Copy / Electronic Data.

Subject to the data retention policy set out in table 2 below, we have a thorough and complete approach to deleting data from all data sources including but not limited to database tables, temporary files, log files and any other locations where personal data may exist.

Appendices and Forms

1. Traveller Profile Data
2. Data retention timeframe
3. Data Subject request timeframe
4. Data Access request form
5. Personal Data Breach Notification Form

Table 1. Traveller Profile Data.

Data Record	Record Type	Mandatory	Notes
Title	ClientRecord	N	
FirstName *	Client Record	Y	
MiddleName	Client Record	N	
Surname *	Client Record	Y	
Phone Number Type	Client Record	N	
Phone Number Value	Client Record	Y	
Email Addresses	Client Record	N	
Mobile Numbers	Client Record	N	
Postal Addresses Type	Client Record	N	
Description	Client Record	N	
Line 1	Client Record	Y	
Line 2	Client Record	N	
Line 3	Client Record	N	
City	Client Record	N	
County	Client Record	N	
Country	Client Record	Y	
Post Code	Client Record	N	
Gender	Client Record	N	
Date Of Birth	Client Record	N	
Organisation (TradeClient) *	Client Record	Y	
Position in Organisation	Client Record	N	
Name is as per passport verification	Client Record	N	
Allow Marketing Contact flag	Client Record	N	
Marketing Group Membership	Client Record	N	
Seat Preference	ClientProfile	N	
Meal Preference	ClientProfile	N	
TSA Redress Number	ClientProfile	N	
Frequent Flyer Programme name/airline	ClientProfile	N	
Frequent Flyer Numbers	ClientProfile	Y	
Special Service Requests	ClientProfile	N	
Special Service Requests Code	ClientProfile	N	
Airline (if applicable)	ClientProfile	Y	
Extra Info (if applicable, as prescribed by GD	ClientProfile	Y	
Travel Documents (e.g. passport, driving lice	ClientProfile	N	
Reference Number *	ClientProfile	Y	
Country of Issue	ClientProfile	N	
Issue Date	ClientProfile	N	
Expiry Date	ClientProfile	N	
Name as per document	ClientProfile	N	
Emergency Contact Name	ClientProfile	N	
Emergency Contact Telephone	ClientProfile	N	
Emergency Contact Email	ClientProfile	N	
ProfileExportTarget (PCC),	ClientProfile	Y	
Key	ClientProfile	Y	
Last Export date/time	ClientProfile	Y	

Table 2. Data Retention and deletion timeframe.

Data Type	Internal Ref	IT System	Data Retention Period	Rationale
Corporate Traveller Profile Data*	STM	GDS Passenger Name Record (PNR)	11 Months post trip except where client or traveller deletion request received.	To enable post trip customer service, refunds etc.
Corporate Traveller Profile Data*	STM	GDS Profile System. Boss Profile System.	5 years post trip except where client or traveller deletion request received.	To facilitate current and future bookings from Clients.
Consol Traveller Data	WTC	GDS Boss	48 hours post trip. 5 years post trip except where client or traveller deletion request received.	To enable booking completion, APIS, ETA etc. For record purposes only.
Retail Traveller Data	WTC	GDS Boss	11 months post trip. 5 years post trip except where client or traveller deletion request received.	To enable booking completion, APIS, ETA etc. For record purposes and for specific marketing of relevant products to existing customers
Personal Traveller Data	WTCG	Microsoft Exchange	Emails older than 12 months are archived.	Reasonable timeframe to retain data / records in live system.
Personal Traveller Data	WTCG	Mail Store	Emails are retained for 6 additional years.	To comply with all legal and customer service obligations
Employee Data	WTCG	Sage / Micropay	Data is archived after every tax year.	To comply with legal and taxation obligations
Telephone Call recordings	WTC STM	PBX System	18 Months	For quality control and training purposes. To deal with customer service issues.
CCTV Recordings	WTC STM	CCTV System	Approx. 2 months	For office security purposes.

Table 3. Data Subject request timeframe.

Data Subject Request	Timescale
The right to be informed	When data is collected (if supplied by data subject) or within one month (if not supplied by data subject)
The right of access	One month
The right to rectification	One month
The right to erasure	Without undue delay
The right to restrict processing	Without undue delay
The right to data portability	One month
The right to object	On receipt of objection
Rights in relation to automated decision making and profiling.	Not applicable

4. Data Subject Request Form

This form should be used to submit a data subject request under the provisions of the European Union General Data Protection Regulation (GDPR).

Submitter Details

Title:	
Name:	
Address:	
Customer/Account Number:	

Type of Request

Please select the type of request you are making:

- ☐ *Consent Withdrawal*
- ☐ *Access request*
- ☐ *Rectification of personal data*
- ☐ *Erasure of personal data*
- ☐ *Restriction of processing of personal data*
- ☐ *Personal data portability request*
- ☐ *Objection to processing of personal data*
- ☐ *Request regarding automated decision making and profiling*

Personal data involved

Request details

Request reason/justification

Signature:	
Name:	
Date:	

Once completed, this form should be submitted via email to compliance@worldtravelcentregroup.com or posted to:

Republic of Ireland / Worldwide Residents:
GDPR Compliance
World Travel Centre / Selective Travel Management
43 Pearse Street
Dublin 2
D02 W085

Northern Ireland / United Kingdom Residents
GDPR Compliance
World Travel Centre / Selective Travel Management
Ground Floor
Murrays Exchange
1 Linfield Road
Belfast
BT12 5DR

5. Personal Data Breach Notification Form

World Travel Centre Selective
Travel Management

Notification Details

Name:	
Title:	
Organisation Name:	
Organisation Address:	
Phone number:	
Email Address:	
Date and Time Notification Submitted:	
Date and Time of Detection of the Data Breach:	
Elapsed Time Between Detection and Notification:	

a. Description of the Nature of the Personal Data Breach

b. Likely Consequences of the Data Breach

c. Measures Already Taken to Address the Breach

d. Measures Proposed to be Taken to Further Address the Breach

e. Reasons for Delay in Notification, if applicable

f. Guidance Notes for Completion

This form is intended to be used by an employee of [Organization Name] to notify the supervisory authority of a breach of personal data for which [Organization Name] is a controller, in accordance with the requirements of the European Union General Data Protection Regulation (GDPR).

Correct use of this form, including where it should be sent to and how, is described in the document *Personal Data Breach Notification Procedure*.

Name

The name of the person that is officially submitting the personal data breach notification to the supervisory authority. This may be the Data Protection Officer or another (usually senior) employee of the organisation.

Title

The role title of the submitter e.g. Data Protection Officer, Chief Information Officer

Organisation Name

The official name of the organisation submitting the notification.

Organisation Address

The main address of the organisation, to which correspondence about the personal data breach should be directed.

Phone number

The phone number(s) of the main contact point concerning the breach.

Email Address

The email address(es) of the main contact point concerning the breach.

Date and Time Notification Submitted

The date and time at which the notification is recorded as having been submitted. This should be completed shortly before the actual submission and maybe be overruled by the actual date and time of receipt by the supervisory authority.

Date and Time of Detection of the Data Breach

The date and time at which it was reasonably recognised by the organisation that a breach affecting personal data occurred, or was highly likely to have occurred.

Elapsed Time between Detection and Notification

The elapsed time, in hours, between the data breach having been recognized or detected by the organisation and the personal data breach notification being submitted to the supervisory authority.

g. Description of the Nature of the Personal Data Breach

Describe the nature of the personal data breach, including, where possible:

h. Categories and approximate number of data subjects concerned

i. Categories and approximate number of personal data records concerned

The description should include the current understanding of how the breach occurred (e.g. unauthorised access, accidental) and any supporting information.

j. Likely Consequences of the Data Breach

A description of what the likely effects on data subjects may be of the breach and the risks they may face, including potential timescales.

k. Measures Already Taken to Address the Breach

Describe the actions that have been taken prior to the notification to lessen the impact of the breach, stop any further breaches and otherwise address the risk to data subjects.

l. Measures Proposed to be Taken to Further Address the Breach

Describe the further actions that have been identified, but not yet taken, that may help to lessen the impact of the breach, stop any further breaches and otherwise address the risk to data subjects.

m. Reasons for Delay in Notification, if applicable

The GDPR requires that breaches of personal data that may result in a risk to the rights and freedoms of natural persons are notified to the supervisory authority without undue delay and, where feasible, not less than 72 hours after having become aware of it. If this timescale has not been met, the reasons for this should be stated here