

GDPR and Travel Industry

John Kyriazoglou



JOHN KYRIAZOGLU

GDPR AND TRAVEL INDUSTRY

GDPR and Travel Industry

1st edition

© 2018 John Kyriazoglou & bookboon.com

ISBN 978-87-403-2591-1

CONTENTS

	Preface: GDPR, Travel and Tourism	6
1	Create Personal Data Inventory	12
2	Manage User Consent	15
3	Keep Users Informed	18
4	Upgrade Information Technology and Systems	21
5	Satisfy Personal Data Requests	24
6	Implement Data Protection Policies	29
7	Appoint Controller, Processor and DPO	34
	Appendix: Plans, Policies and Strategies	40
	Appendix 1: Travel and GDPR Definitions	41
	Appendix 2: Data Protection Team Improvement Plan	47



www.sylvania.com

**We do not reinvent
the wheel we reinvent
light.**

Fascinating lighting offers an infinite spectrum of possibilities: Innovative technologies and new markets provide both opportunities and challenges. An environment in which your expertise is in high demand. Enjoy the supportive working atmosphere within our global group and benefit from international career paths. Implement sustainable ideas in close cooperation with other specialists and contribute to influencing our future. Come and join us in reinventing light every day.

Light is OSRAM

**OSRAM
SYLVANIA** 

Appendix 3: Technical and Organizational Data Protection Measures	49
Appendix 4: Controller – Processor Agreement	52
Appendix 5: Personal Data Breach Incident Response Plan	58
Appendix 6: Data Protection Technology Strategy	60
Appendix 7: IT Security Strategy	64
Appendix 8: Data Protection Policy	65
Bibliography	68
About the author	70

PREFACE: GDPR, TRAVEL AND TOURISM

Introduction: Global travel and tourism environment

Most people at some point in their life will have an urge or a need to travel. This may be a two-week holiday to somewhere warm to top up your suntan or this could be a life changing year, or longer, trip. Everyone has their own reasons that they decide to travel but most people are triggered by something (personal or business).

On a personal level these reasons may include challenging yourself, learning new ways of doing things, gain awareness of new customs, cultures, people and places, expanding your perspective, getting in touch with yourself, appreciating your life, visiting family and friends, visiting religious places, etc.

On a business level these reasons may include finding new markets for your company's products and services, managing or consulting or executing other work away from your own home town or country, attending conferences, taking courses, etc.

The travel¹ services sector is made up of a complex web of relationships between a variety of suppliers, tourism² products and services providers, destination marketing organizations, tour operators, and travel agents, hotels, hostels, airline companies, travel agencies (online, classical), among many others.

These are termed TR (Travel) and TO (Tourism) Companies for the purposes of this book.

Travel and tourism (TR (Travel) and TO (Tourism) Companies), as one industry, is one of the world's largest industries with a global economic contribution (direct, indirect and induced) of over 7.6 trillion U.S. dollars in 2016. The direct economic impact of the industry, including accommodation, transportation, entertainment and attractions, was approximately 2.3 trillion U.S. dollars that year³.

Each year, the global traveler pool is flooded with millions of new consumers from both emerging and developed markets, many with rising disposable incomes and a newfound ability to experience the world.

Data and cybersecurity challenges for TR & TO Companies

For many years now, cybersecurity has been a primary concern of government-related organizations and the financial and banking sectors, but TR & TO Companies are beginning to acknowledge the importance of online security in their daily operations^{4, 5, 6}.

Each travel operator, hotel or transport company handles all kinds of sensitive data on their customers, as well as their own staff and suppliers. The consequences of companies and organizations experiencing online attacks and data breaches are now higher than ever before.

For instance, if a TR & TO Company like a travel operator is hacked, leaking thousands of personal addresses of customers, they face significant financial, legal and reputational ramifications. The loss of customer confidence in the operator and the legal costs of any resulting identity theft would hit any travel operator big or small right where it hurts – the profit and loss sheet.

TR & TO Companies also face many more data security challenges than other industries⁷, with multiple payment points, online electronic reservation systems, e-mails and faxes containing credit card data, and plenty of personal data and customer information.

All this makes TR & TO Companies easy for cyber criminals: in fact, according to recent reports and studies, the hospitality industry represented the second largest share of security breaches and personal data incidents in cyberspace last year (2017⁸).

The General Data Protection Regulation (GDPR)

On 14 April 2016, the EU Parliament adopted the General Data Protection Regulation (GDPR), and all companies and organizations now have to comply by 25 May 2018.

The GDPR applies to the personal data processing by the controller or processor establishment in the European Union, regardless of whether the processing takes place in the Union or not. Ultimately, the change applies to almost all travel companies that offer products and services in Europe and process personal data of EU citizens as well as other users, located within its borders.

Travel & Tourism Perspective

This will mean that global online travel agents or, for instance, US airlines, will be directly regulated by the GDPR. For example, when an Emirates-based hotel sells to EU travel agents or third-party wholesalers based in Europe, it falls under the Regulation. If you monitor the behavior of users who are located within the EU, such as flight destinations and hotel booking in France, you must comply with the requirements.

This approach affects the use of web analytics tools, data collection and tracking for personalization and retargeting purposes. It also applies to website visits from users located in the EU, regardless of whether they are EU citizens or not.

GDPR covers every kind of processing that can be done with personal data, whether by automated systems (e.g., IT applications) or non-automated means (e.g., manual systems) or whether it is active or passively retained (e.g., collecting, recording, storing, using, adapting, modifying, archiving and deleting data, etc.).

Data breaches may occur in all sectors of the economy.

Companies, customers and stakeholders need to ensure that personal data is protected, but also that there are strong policies and procedures in place to ensure the fair and legitimate processing of such data.

The General Data Protection Regulation (GDPR) is the modern answer to ensure the responsibility of all organizations (private companies, airline companies, travel agencies, hotels, etc.) to ensure the fundamental right to the protection of personal data. Serious violations of the law will be punishable by fines of up to € 20 million or 4% of the total annual turnover worldwide.

As we saw above TR & TO Companies are considered one of the most vulnerable sectors to data breaches and electronic attacks because these companies process a very large volume of transactions with payment cards every day. They also receive this information from many sources: third-party booking systems, point-of-sale systems, online reservation systems, their own web site, emails and faxes, telephone conversations and walk-ins, etc.

In addition, they generally store personal data from payment cards at different points. This data, from many sources, stored in so many sites, systems, files and media, must be protected. But before TR & TO Companies start to protect the data, they first need to know where all that personal data is (i.e., it is required to record personal data in a personal data inventory, etc.).

The GDPR, which is fully applicable now, requires all companies and hence all TR & TO Companies to:

- Properly train their human resources
- To implement the appropriate security measures and the necessary information protection policies
- Analyze the impact that may result from a privacy violation
- Design products and services with privacy considerations
- Inform competent authorities within 72 hours of system and data loss detection and customers whose data was lost
- Appoint a Data Protection Officer,
- Have an incident response plan for Incident Response Plan
- Compensate clients whose data was lost, etc.

In order to allow TR & TO Companies to maintain and increase their clientele and to avoid fines and downsizing from non-compliance with the new EU GDPR, they should invest in technology solutions and services to help them provide personalized services while taking care of the security of their customers' personal data.

This is achieved by executing the following steps:

- Step 1. Create Personal Data Inventory (Chapter 1)
- Step 2. Manage User Consent (Chapter 2)
- Step 3. Keep Users Informed (Chapter 3)
- Step 4. Upgrade Information Technology and Systems (Chapter 4)
- Step 5. Satisfy Personal Data Requests (Chapter 5)
- Step 6. Implement Data Protection Policies (Chapter 6)
- Step 7. Appoint Controller, Processor and DPO (Chapter 7).

The following chapters in this guide serve this specific purpose for TR & TO Companies and their management.

Notes

1. **Travel** is the movement of people between distant geographical locations. For more details, see:
<https://en.wikipedia.org/wiki/Travel>
<https://www.onetravel.com/travel/glossary.asp>
2. There are a number of ways tourism can be defined, and for this reason, the United Nations World Tourism Organization embarked on a project from 2005 to 2007 to create a common glossary of terms for tourism. It defines tourism as follows: Tourism is a social, cultural and economic phenomenon which entails the movement of people to countries or places outside their usual environment for personal or business/professional purposes. These people are called visitors (which may be either tourists or excursionists; residents or non-residents) and tourism has to do with their activities, some of which imply tourism expenditure (United Nations World Tourism Organization, 2008).
<http://www2.unwto.org/>
3. <https://www.statista.com/topics/962/global-tourism/>
4. Morgan, Steve. “Ransomware Damages Rise 15X in 2 Years to Hit \$5 Billion in 2017.” CSO Online, CSO, 23 May 2017, www.csoonline.com/article/3197582/leadership-management/ransomware-damages-rise-15x-in-2-years-to-hit-5-billion-in-2017.html
5. Morgan, Steve. “Top 5 cybersecurity facts, figures and statistics for 2018.” CSO Online, CSO, 23 Jan. 2018, www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html
6. http://www.idtheftcenter.org/images/breach/2017Breaches/DataBreachReport_2017.pdf
7. According to **Grant Thornton**:
http://www.grant-thornton.gr/globalassets/1.-member-firms/greece/insights/pdfs/surveys/gr_hotels_2020.pdf
8. For more details, see:
 - 8.1. 2017 U.S. State of Cybercrime www.CSOonline.com
 - 8.2. ‘Cybersecurity Tactics for a Hotel Industry that’s Under Siege’, 03/16/2017, <https://hospitalitytech.com/cybersecurity-tactics-hotel-industry-thats-under-siege>
 - 8.3. <https://ehotelier.com/insights/2016/05/19/5-key-issues-in-hotel-cybersecurity/>
 - 8.4. See ‘TRUST WAVE GLOBAL SECURITY REPORT’
<https://www.trustwave.com/home/>

Additional Resources

Douglas Quinby, Phocuswright Conference, Florida, November 9, 2017.

Deloitte Insights, “Deloitte Global Economic Outlook, Q3 2017,” <https://dupress.deloitte.com/dup-us-en/economy/global-economic-outlook/2017/q3.html>, last modified August 9, 2017.

Global Business Travel Association, https://www.gbta.org/foundation/pressreleases/Pages/rls_0711162.aspx, accessed October 12, 2017

<https://www.gbta.org/>

<https://www.wttc.org/-/media/382bb1e90c374262bc951226a6618201.ashx>

1 CREATE PERSONAL DATA INVENTORY

***Overview:** This chapter and its GDPR implementation actions is **the first step** in the proposed 7-step methodology for implementing appropriate controls to comply with the GDPR for your company.*

GDPR Requirements

All data about persons in the EU are covered under the GDPR.

This includes **TR & TO Companies** and their customers, passengers, hotel guests, website visitors and employees.

“Personal data” is any data about an identifiable person, such as: name, phone number, email address, reservation number, IP address, or any information that allows them to be uniquely identified.

The GDPR grants extra protections for “sensitive data.” This includes personal data that reveals any of the following:

- a) trade union membership, which may be revealed by event attendance,
- b) biometrics for the purpose of uniquely identifying someone, such as a fingerprint stored for opening doors,
- c) health status, which may be disclosed in guest requests,
- d) sex life or sexual orientation, which may also be disclosed in some guest requests,
- e) genetic data, racial or ethnic origin, political opinions and
- f) religious or philosophical beliefs.

Travel & Tourism Perspective: All online flight and accommodation reservation systems collect a broad spectrum of personal details, including names, travel purposes (leisure or work), travel with children, emails, payment data, etc.

The GDPR requires communicating clear purposes of information use. To achieve that, TR & TO Companies, especially those collecting data for sophisticated personalization, must organize a personal data audit and document their findings in a Personal Data Inventory, also taking into consideration the requirements of article 30 of GDPR.

The need for documenting the processing of personal data is specified in the following GDPR article: Article 30 (Records of processing activities).

As use cases grow in number and personal information is applied across various departments and services, it becomes difficult to track all the types of personal information collected.

What should TR & TO Company Managers do

Action 1. Create a Personal Data and Flows Inventory

Point 1. TR & TO Company managers should document what personal data they hold, where it came from and with whom it is shared. All of the above types of sensitive data can only be handled with explicit consent. If this kind of data is collected incidentally, it should be removed immediately to avoid undertaking new obligations for the protection of that data.

Point 2. Pay special attention to handling children's data. Within the EU/EEC, a "child" is defined as someone younger than a country-defined age between 13 and 16. For most cases, hotels, for example, will not need to rely on children's' or parent's consent to process guest information, since the primary basis for data processing is handling reservations.

However, in cases where consent is the basis for data processing, for example, for marketing purposes, children's data needs to be handled with extra care. You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity. Children's data can only be handled with explicit consent when consent is required.

Point 3. Best practice is to avoid collecting and storing data about children unless it is legally required or absolutely essential for handling a reservation.

Point 4. Review whether and how "sensitive personal data" is collected and held. If you are currently relying on consent for processing any type of data you should check whether there are other applicable grounds that you can rely on instead, and document these.

Point 5. Check that each individual (natural person, sole trader or unlimited liability partnership) on your marketing databases has either explicitly consented to receive electronic marketing, or, if they are existing customers, that they were given the opportunity to opt out from such marketing when their contact details were first collected and that their wishes have been respected.

Point 6. If personal data are out of date, update them. If personal data are no longer needed, delete them. This will minimise your risk and ensure that you are in compliance with the GDPR aim of personal data minimisation.

Action 2. Ensure Staff Understand Travel and other critical GDPR terms

In addition to understanding the nature of the personal data **TR & TO Companies** are holding and processing, **TR & TO** managers must also ensure that their staff understand the basic travel and the following relevant critical terms of GDPR, such as: Binding corporate rules, Consent, Data Subject, Encrypted Data, Enterprise, etc., for better implementation of GDPR.

For more details, see 'Appendix 1: Travel and GDPR Definitions'.

2 MANAGE USER CONSENT

Overview: *This chapter and its GDPR implementation actions is **the second step** in the proposed 7-step methodology for implementing appropriate controls to comply with the GDPR for your company.*

GDPR Requirements

- 1) **Consent for Adults.** GDPR requires (Article 7) controllers to follow the standard for **consent** when relying on **consent** as a legal basis for processing personal data (demonstrable consent) and sensitive personal data (explicit consent).
- 2) **Consent for Children.** GDPR requires (Article 8) controllers to follow the standard that where the legal basis of **consent** is being relied on in relation to offering information society services to minors under the age of 16 (or to younger **children** not younger than 13, if the age threshold is lowered by Member State law), consent must be given or authorised by the holder of parental responsibility over the child. The controller must also make reasonable efforts to verify consent.



Discover the truth at www.deloitte.ca/careers

Deloitte.

© Deloitte & Touche LLP and affiliated entities.

3) Consent for Sensitive Data. GDPR (Article 9) sets out a general prohibition on the processing of sensitive data, followed by legal grounds on which **sensitive personal data** can be processed. Sensitive data includes: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade-union membership; genetic data; biometric data; data concerning health or sex life; and sexual orientation. Grounds upon which sensitive data can be processed include: with explicit consent; for employment, social security, and social protection requirements; to protect vital interests of a natural person where consent cannot be obtained, etc.

Travel & Tourism Perspective: Processing of personal data for TR & TO Companies is based on consent. According to the regulation (GDPR), consent means the permission to process personal data given by the individuals (users, passengers, customers, guests, etc.).

The GDPR sets up conditions and rules for consent creation and TR & TO Companies must follow them to be in compliance with the act. New rules that apply to obtaining the consent:

- Consent must be freely given, specific, informed, and unambiguous.
- TR & TO Companies must present the consent in easily accessible form that is written in clear language.
- The consent can't be inferred from silence, visiting, and continuing to browse a website. It also needs to be separated from other terms and conditions. The user must complete an affirmative action. The best approach is to create a click with an opt-in box.
- If you gather information about users via cookies, you should give them the opportunity to accept or reject them.
- If a user changes their mind, they also must be able to access settings menus to update their preferences.

Personal information collected about users for one purpose can't be used for a different one.

All airline websites collect user email addresses so they can send an e-ticket. Usually, the purpose of acquiring these data is clearly articulated. But airlines must ask for the explicit consent again if they were to use this data for email campaigns.

The same with hotels, if a user gives the consent to collect data to make a hotel booking, the data can't be used for marketing purposes because the consent for such usage wasn't given. The best way to contact your customers for consent is to include multiple tick boxes for each type of consent you need.

What should TR & TO Company Managers do in terms of obtaining and managing user consent?

Action 1. Create and implement a procedure and a technical system to manage your consents.

Action 2. Develop, implement and maintain policies and procedures for collection and use of adults, children and minors' personal data.

Action 3. Update your consent procedure to ensure that all your contacts (users, customers, etc.) have confirmed their consents with a positive reply and that you have recorded all their particulars in a consent system.

Action 4. Update your consents, age verification and authorisation processes to comply with the stricter requirements for valid consent for processing children's personal data.

Action 5. You may need to speak with customers at check-in if explicit consent is required for any forms of data collection that require it, such as consent to marketing communications.

Action 6. All loyalty programs need to be examined for similar requirements if data is used in a way that requires consent.

3 KEEP USERS INFORMED

***Overview:** This chapter and its GDPR implementation actions is **the third step** in the proposed 7-step methodology for implementing appropriate controls to comply with the GDPR for your company.*

GDPR Requirements

Informing data subjects. According to GDPR (Recitals 13, 58 and articles 5, 12, 13 and 14): ‘The controller shall take appropriate measures to provide any **information** referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means, etc.’

Travel & Tourism Perspective: Providing information to users (customers, guests, passengers, etc.) by TR & TO Companies and being transparent about the processing of their personal data is very critical to their operations.

‘Transparency’ according to the business dictionary (Read more: <http://www.businessdictionary.com/definition/transparency.html>)

means:

1. See-through, clear piece of acetate used for projecting data, diagrams, and text onto a screen with an overhead projector.
2. Lack of hidden agendas and conditions, accompanied by the availability of full information required for collaboration, cooperation, and collective decision making.
3. Minimum degree of disclosure to which agreements, dealings, practices, and transactions are open to all for verification.
4. Essential condition for a free and open exchange whereby the rules and reasons behind regulatory measures are fair and clear to all participants.

Transparency requirements in GDPR for TR & TO Companies apply irrespective of the legal basis for the processing and throughout the processing life cycle.

This is clear from Article 12 which provides for transparency to be applied to the following stages of the data-processing cycle:

1. Before or at the commencement of the data processing cycle, ie when personal data is collected by the data subject or otherwise obtained,
2. Throughout the processing period, i.e., when communicating with the data subjects about their rights, and
3. At specific points during processing, such as when data breaches occur or when there is significant change in processing.

What does transparency mean?

Transparency is not defined in GDPR. Recital 39 of the GDPR is informative on the importance and impact of the principle of transparency in data processing:

Any processing of personal data should be legal and fair. It should be clear to natural persons that personal data relating to them are collected, used, taken into account or otherwise processed and to what extent personal data are or will be processed.

This principle requires that all information and communication concerning the processing of such personal data be easily accessible and understandable and that it uses clear and simple language.

This principle relates in particular to informing the data subjects about the identity of the controller and the purposes of the processing and further information to ensure fair and transparent treatment in relation to such natural persons and their right to receive confirmation and to obtain communication of the personal data relating to them that are processed.

What should TR & TO Company Managers do in terms of providing information to data subjects and promoting transparency?

Action 1. You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

Action 2. Develop, implement and maintain a data privacy notice that details, in clear language, your company's personal data handling practices.

Action 3. Develop, implement and maintain supporting guidelines indicating how and when privacy notices are communicated to individuals (special buttons, graphs, just in time notice, icons, scripts, etc.).

Action 4. Develop, implement and maintain a data privacy notice that details your company's personal data handling practices.

Action 5. Provide data privacy notice at all points (short form, condensed data privacy notice, hard copy, marketing communications, privacy notice in contracts and terms, scripts for providing notice via phone, etc.) where personal data is collected.

Action 6 . Ensure your company's data protection (privacy) policy is uploaded onto your website and contains the following paragraphs:

- Objective
- Purpose of this policy
- Commitment
- Opportunity to decline
- Personal information collection
- Use of information
- Credit reference checks
- Disclosure of information
- Protection of information
- Internet access
- Monitoring of communications
- Data Subject Access Requests
- Data Protection breaches
- Contact.

An example of a data protection policy is contained in 'Appendix 8: Data Protection Policy'.

4 UPGRADE INFORMATION TECHNOLOGY AND SYSTEMS

Overview: This chapter and its GDPR implementation actions is **the fourth step** in the proposed 7-step methodology for implementing appropriate controls to comply with the GDPR for your company.

GDPR Requirements

- 1) **Processing of personal data.** According to Article 5 (1, f) personal data shall be: 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').
- 2) **Security of processing.** Also, according to Article 32 (Security of processing):
 1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
 - a) the pseudonymisation and encryption of personal data;
 - b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
 - c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
 - d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing, etc.

Travel & Tourism Perspective

Personal and other corporate data of TR & TO Companies are collected, stored and processed by a variety of Information Technology Applications and Systems, both within the facilities and environment of the specific companies as well as in cloud computing platforms located outside the given TR & TO company.

There are also a set of critical trends to watch out for in 2018 that are bound to impact the Travel and Tourism Industry (according to <https://www.globaldata.com/top-6-technology-trends-watch-travel-tourism-industry-2018/>).

These are:

Trend 1. Augmented and Virtual Reality (AR and VR): The past few years have seen an increase in AR or VR popularity among travel and tourism companies, and the trend is set to continue. These technologies are being used either for content marketing or to enhance the customers' experiences.

Trend 2. Artificial Intelligence (AI): AI is behind many evolving technologies and innovations in the travel and tourism sector. The ways in which it helps the industry can be classified into three major categories: Machine Learning, ChatBots or TravelBots, and Robots.

Trend 3. Internet of Things (IoT): IoT has a lot of potential to shape the future of the travel and tourism industry, and companies have started to realize that. An example of an industry player using IoT to reduce anxiety and stress levels associated with lost bags is Lufthansa. Passengers can track their baggage via a link found on their mobile boarding pass in the Lufthansa app.

Trend 4. Voice Technology: Voice technology is another digital novelty that is beginning to disrupt the travel and tourism sector, as more and more customers switch from typed-in search to voice interactions. More and more hotels have started experimenting with voice-activated devices.

Trend 5. Wi-Fi connectivity: When travelling, people want to always be connected, either to get destination ideas, options regarding places to visit or eat, find directions to points of interest, or share their experience with friends via social media or other connectivity platforms.

Trend 6. Wearable devices: Despite a sluggish start, travel and tourism companies are gradually using this technology to offer customers a more personalized and united experience.

Also, because TR & TO Companies, such as travel agencies, hotels, tour operators and airlines, etc., collect and store quite much of identifying personal data, from names to children's information, ensuring the right response to breaches becomes critical.

What should TR & TO Company Managers do

Action 1. Create and maintain an IT Assets Inventory.

Action 2. Hire an expert to carry out a security assessment and review of your IT risks and required measures and controls to mitigate all identified risks your company is faced with. Your company's hardware and software applications should be reviewed along with hard copy files. A series of encryption codes, passwords or limitations on access may need to be implemented to protect access to, and the integrity of the data.

Action 3. Study the technology trends (presented above) and prepare their company for their beneficial exploitation, as needed.

Action 4. Ensure that single vendor who receives personal data from their company must share a Data Processing Agreement (DPA) with the company (**TR & TO**) to confirm that the vendor is compliant with the rules of the GDPR.

Point 4.1. The DPA must dictate the purposes for which the processor is processing the data.

Action 5. For each software vendor that processes personal information of customers, guests, etc., the **TR & TO Company** needs to do the following:

Point 5.1. Determine the type of data the software vendor processes.

Point 5.2. Determine the purpose for which the processing is happening.

Point 5.3. Obtain a Data Processing Agreement.

Point 5.4. If the vendor is outside the EU, sign the standard contractual clauses (usually part of the Data Processing Agreement mentioned above), or confirm that the vendor is a member of the Privacy Shield or other relevant privacy certification mechanism.

Point 5.5. Mention the vendor in the **TR & TO Company's** privacy policy, along with the purpose of the vendor and how the data will be used.

5.6. Confirm that the vendor can handle data rights requests within the time period set by GDPR, etc.

Action 6. Maintain data privacy protection and information security policies and procedures. See also Appendices 3, 6, 7 and 8.

Action 7. Establish a protection incident and breach response process. See also Appendix 5.

Action 8. Integrate data protection into corporate IT application systems and infrastructure.

Point 8.1. Add a privacy policy to your website, if you have not done so already, to make clear how you use data collected on your website, and also to make it clear to users how their personal data will be used.

Point 8.2. Add privacy controls, such as encryption, masking and pseudonymization to your computerised applications processing personal data, as required.

5 SATISFY PERSONAL DATA REQUESTS

Overview: This chapter and its GDPR implementation actions is **the fifth step** in the proposed 7-step methodology for implementing appropriate controls to comply with the GDPR for your company.

GDPR Requirements

- 1) Rights of access to data subjects.** Individuals (consumers, customers, users, patients, passengers, employees, employees, partners, citizens, etc., referred to as data subjects under GDPR terms) will have different rights, under the GDPR (articles 15 to 22) to ask companies (such as **TR & TO Companies**, etc.) and organizations for processing of their personal data and which must be met by companies (such as hotels) and organizations.
- 2) Data subject definition.** According to the GDPR (Article 4 definitions), a “data subject” is an identifiable natural person that can be identified, directly or indirectly, in particular by reference to an identifier such as name, identification number (VAT number, Social Security Number, etc.) location data, electronic identifier (e-mail, IP address, etc.) or one or more factors related to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

Travel & Tourism Perspective

This EU regulation gives data subjects (tourists, passengers, hotel guests, etc.) a wide range of rights that can be imposed on companies and organizations processing personal data. These rights may limit the ability of **TR & TO Companies** to legally process the personal data of data subjects, and in some cases these rights may have a significant impact on the business, operations, and operational model of a business or organization.


All companies (such as **TR & TO Companies**) and organizations that act as controllers are directly affected by the rights granted to data subjects. Companies and organizations acting as processors are less likely to be affected, but they must be aware of these rights.

These rights are summarized as follows:


- 1. The right to basic information:** A basic principle of EU data protection law is that data subjects should be entitled to a minimum set of information about the purposes for which their personal data will be processed (Preamble 58, 60 and Articles 12 to 14).
- 2. The right of access:** the right of individuals to have access to their personal data (Article 15).
- 3. The right to rectification:** individuals have the right to correct their personal data if it is inaccurate or incomplete (Article 16).
- 4. The right to erasure ('right to be forgotten'):** allowing a person to request the deletion or removal of his or her personal data if there is no good reason to continue processing (Article 17).
- 5. The right to restrict processing:** when processing is limited, personal data may be stored but not further processed (Article 18).
- 6. The right to be informed of the rectification, erasure or limitation:** data controllers must notify any beneficiary whose data is disclosed, any correction, deletion or limitation of the processing carried out in accordance with Article 16, Article 17 (1) and Article 18, unless this proves impossible or involves a disproportionate effort (Article 19).

SIMPLY CLEVER

ŠKODA



We will turn your CV into an opportunity of a lifetime



Do you like cars? Would you like to be a part of a successful brand? We will appreciate and reward both your enthusiasm and talent. Send us your CV. You will be surprised where it can take you.

Send us your CV on
www.employerforlife.com



7. **The right to data portability:** allows individuals to acquire and re-use their personal data for their own purposes in various services (Article 20).
8. **The right of objection:** the right of individuals to refuse the use of their data for direct marketing, including profiling (Article 21).
9. **The rights related to automated decision making and profile creation:** individuals have the right not to be subject to a decision when it is based on the automated processing of their data (Article 22).

What should TR & TO Company Managers do?

Action 1. Enable access to personal data by data subjects (users, customers, guests, passengers, etc.)

Point 1.1. Develop and install the technical platform and tools to ensure all access requests aspects (as described next).

Point 1.2. Develop, implement and maintain a procedure for responding to access requests by data subjects.

Point 1.3. Develop, implement and maintain data subject access request forms.

Point 1.4. Develop, implement and maintain template letters for responding to requests by data subjects.

Point 1.5. Develop, implement and maintain a data subject access requests log.

Point 1.6. Develop, implement and maintain forms for the supply of additional data required for access requests by data subjects.

Action 2. Enable rectification of personal data by data subjects (users, customers, guests, passengers, etc.)

Point 2.1. Develop, implement and maintain data quality and rectification procedures.

Point 2.2. Develop, implement and maintain procedures for responding to customer or user (data subjects) requests and needs.

Point 2.3. Install and maintain customer or user or data subject portal to update personal data.

Point 2.4. Train staff to handle rectification requests.

Point 2.5. Keep training records.

Action 3. Enable erasure of personal data by data subjects (users, customers, guests, passengers, etc.)

Point 3.1. Develop, implement and maintain procedure for responding to right to be forgotten requests.

Point 3.2. Develop, implement, install and maintain customer or data subject or user portal to erase or update personal data.

Point 3.3. Monitor the operation of the portal.

Point 3.4. Evaluate results for portal functionality

Action 4. Enable restriction of processing of personal data by data subjects (users, customers, guests, passengers, etc.)

Point 4.1. Develop, implement and maintain procedure for responding to requests to restrict processing of data.

Point 4.2. Develop, implement, install and maintain customer or data subject or user portal to update personal data.

Point 4.3. Monitor the operation of the portal.

Point 4.4. Evaluate results for portal functionality.

Action 5. Enable disclosure notification on personal data updates

Point 5.1. Develop, implement and maintain procedures to respond to requests.

Point 5.2. Develop, implement and maintain procedure a mechanism for individuals to update or correct their personal data.

Point 5.3. Maintain procedures to respond to requests to be forgotten or for erasure of data

Point 5.4. Develop, implement and maintain a personal data holdings inventory.

Point 5.5. Develop, implement and maintain a data flow map.

Point 5.6. Develop, implement and maintain agreements with third parties regarding notification of any requests for rectification, erasure or restriction of personal data.

Action 6. Enable personal data portability

Point 6.1. Develop, implement and maintain procedures to respond to requests for data portability.

Point 6.2. Develop and implement technical solution for processing data portability requests.

Point 6.3. Ensure technical solution is tested effectively to validate that data is being exported properly.

Action 7. Enable objection to processing of personal data by data subjects (users, customers, guests, passengers, etc.)

Point 7.1. Develop, implement and maintain procedures to respond to requests to opt-out of, restrict or object to processing

Point 7.2. Develop, implement and maintain data privacy notices at all points where personal data is collected

Point 7.3. Integrate data privacy into research practices

Point 7.4. Integrate data privacy into direct marketing practices

Point 7.5. Issue guidance for analysing and responding to data subject objections to processing (e.g. operating procedures or technical processes)

Point 7.6. Develop, implement and maintain procedures for responding to customer requests and preferences

Point 7.7. Develop, implement and maintain procedures for customer or user portal to update data

Point 7.8. Develop, implement and maintain procedures for responding to requests to restrict processing of data in a timely manner

Action 8. Enable right of data subjects (users, customers, guests, passengers, etc.) related to automated decision making and profiling

Point 8.1. Develop, implement and maintain procedures to review processing conducted wholly or partially by automated means

Point 8.2. Develop, implement and maintain a personal data processing register that identifies automated processing and states a legal basis for such processing.

Point 8.3. Develop, implement and maintain a personal data holdings inventory.

Point 8.4. Develop, implement and maintain a checklist for automated processing.

6 IMPLEMENT DATA PROTECTION POLICIES

*Overview: This chapter and its GDPR implementation actions is **the sixth step** in the proposed 7-step methodology for implementing appropriate controls to comply with the GDPR for your company.*

GDPR Requirements

- 1) **Personal Data Processing Principles.** According to Article 5 (Principles relating to processing of personal data) of GDPR, personal data shall be:
- a) processed lawfully, fairly and in a transparent manner in relation to the data subject (**‘lawfulness, fairness and transparency’**);
 - b) 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’**);
 - c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**‘data minimisation’**);
 - d) 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’**);
 - e) 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’**);
 - f) 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’**).
1. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (**‘accountability’**).

- 2) Security of processing.** GDPR requires (Article 32) that controllers and processors, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
- a) the pseudonymisation and encryption of personal data;
 - b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
 - c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
 - d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed, etc.
- 3) Data Transfers.** GDPR requires (Chapter V, Articles 44 – 50) that any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined, etc.
- 4) Member State Laws.** GDPR (Articles 85 - 90) state that Member State national law shall address the balance between the Freedom of Expression, Freedom of Information, and Right to Protection of Personal Data. Exemptions may be provided from some of the obligations for processing for journalistic, academic, artistic or literary expression, etc.

Travel & Tourism Perspective

The GDPR applies to the personal data processing by the controller or processor establishment (a TR & TO Company) in the European Union, regardless of whether the processing takes place in the Union or not. Ultimately, the change applies to almost all travel companies that offer products and services in Europe and process personal data of EU citizens as well as other users, located within its borders.

This will mean that global online travel agents or, for instance, US airlines, will be directly regulated by the GDPR. For example, when an Emirates-based hotel sells to EU travel agents or third-party wholesalers based in Europe, it falls under the Regulation. If you monitor the behavior of users who are located within the EU, such as flight destinations and hotel booking in France, you must comply with the requirements. This approach affects the use of web analytics tools, data collection and tracking for personalization and retargeting purposes. It also applies to website visits from users located in the EU, regardless of whether they are EU citizens or not¹.

What should TR & TO Company Managers do?

Action 1. Review legal bases for processing

Point 1.1. Review your legal bases for processing (i.e. understanding the purpose(s) for which your company uses personal data and ensuring you are complying with one of the lawful processing conditions in doing so.

Point 1.2. Updating your company's privacy notices in line with the new higher GDPR standards.

Action 2. Craft and implement GDPR organizational and technical policies and procedures (measures)

Point 2.1. You will need to review all current data protection policies such as their privacy policy, SARs (subject access request) policy, retention policy and other policies like shredding and breach management policy.

Point 2.2. Also policies relating to third party data contractors should be reviewed and consideration given to the appointment of a data protection officer (DPO).

Point 2.3. On the basis of above implement and maintain appropriate technical and organisational security measures to meet the requirements of article 32, such as:

- (1.1) physical access controls
- (1.2) personnel management controls
- (1.3) encryption and pseudonymisation/anonymisation
- (1.4) Information Security policies and procedures
- (1.5) Data breach response plans

Point 2.4. Comply with any approved codes of conduct or certification mechanisms regarding security

Point 2.5. Conduct regular compliance checks to verify the effectiveness of such measures (including resilience/ penetration testing), particularly if there has been a data breach

Point 2.6. Train staff on IT and cybersecurity techniques

Point 2.7. Keep training and testing records.

Point 2.8. Issue reports on company's data protection management issues.

For more details, see '8.3. Appendix 3: Technical and Organizational Data Protection Measures'.

Action 3. Manage international data transfers

Point 3.1. Put in place appropriate data transfer agreements including EU Model Clauses, BCRs or other approved mechanisms

Point 3.2. Review derogations relied on to ensure these remain lawful and appropriate, in particular regarding consent

Point 3.3. Ensure processor/sub-processor contracts include protections against unauthorised transfers/onward transfers

Point 3.4. Exercise audit and inspection rights to verify compliance by processors with their obligations

Action 4. Train company staff on travel and GDPR terms and data protection requirements

Point 4.1. Ensure your training strategy focuses on preparing everyone better on privacy issues.

Point 4.2. Ensure your training engages all staff (board, management and employees).

For more details, see 'Appendix 1: Travel and GDPR Definitions' and 'Appendix 2: Data Protection Team Improvement Plan'.

Action 5. Implement Data Protection by Design and Default and DPIAs

Point 5.1. When introducing new products, services, or processes, data controllers will need to show that the impact of such products, services or processes has been considered, and that steps have been taken to minimise any negative impact on individuals' rights and freedoms.

Point 5.2. Data should be pseudonymised where possible and should not be collected unless it is really needed.

Point 5.3. For new projects, do not collect personal data unless you can justify your purposes for doing so and you have conducted, and documented, privacy impact assessments.

Point 5.4. Determine how you will keep personal data safe and how high risk the proposed project is to individuals' privacy.

Point 5.5. Make sure that your data protection policies are up to date and that your data processing is transparent.

Action 6. Integrate Data Protection into Business Functions

Point 6.1. Integrate data protection in all **TR & TO** business functions

Point 6.2. Maintaining GDPR awareness with staff is an ongoing process.

Point 6.3. **TR & TO** Companies should provide regular refresher training for all staff to ensure an awareness culture exists to protect against possible breaches.

Point 6.4. **TR & TO** Management should incorporate data privacy into operational training such as induction, HR and security, and conduct regular access request drills to ensure staff efficiency.

Point 6.5. Integrate data protection in practices related to monitoring **TR & TO** company employees' communications.

Point 6.6. Ensure **TR & TO** data subjects (guests, customers, etc.) are aware of their right to demand full details of the information held on them. .

More examples and details on all aspects (plans, policies, strategies, controls, questionnaires, etc.) of designing, implementing, reviewing and improving your own Data Privacy and Protection System may be found in my books listed in the Bibliography part of this book.

Notes

1. For more details, see:

<https://www.altexsoft.com/blog/business/how-to-comply-with-gdpr-recommendations-for-travel-industry/>

7 APPOINT CONTROLLER, PROCESSOR AND DPO

*Overview: This chapter and its GDPR implementation actions is **the seventh step** in the proposed 7-step methodology for implementing appropriate controls to comply with the GDPR for your company.*

GDPR Requirements

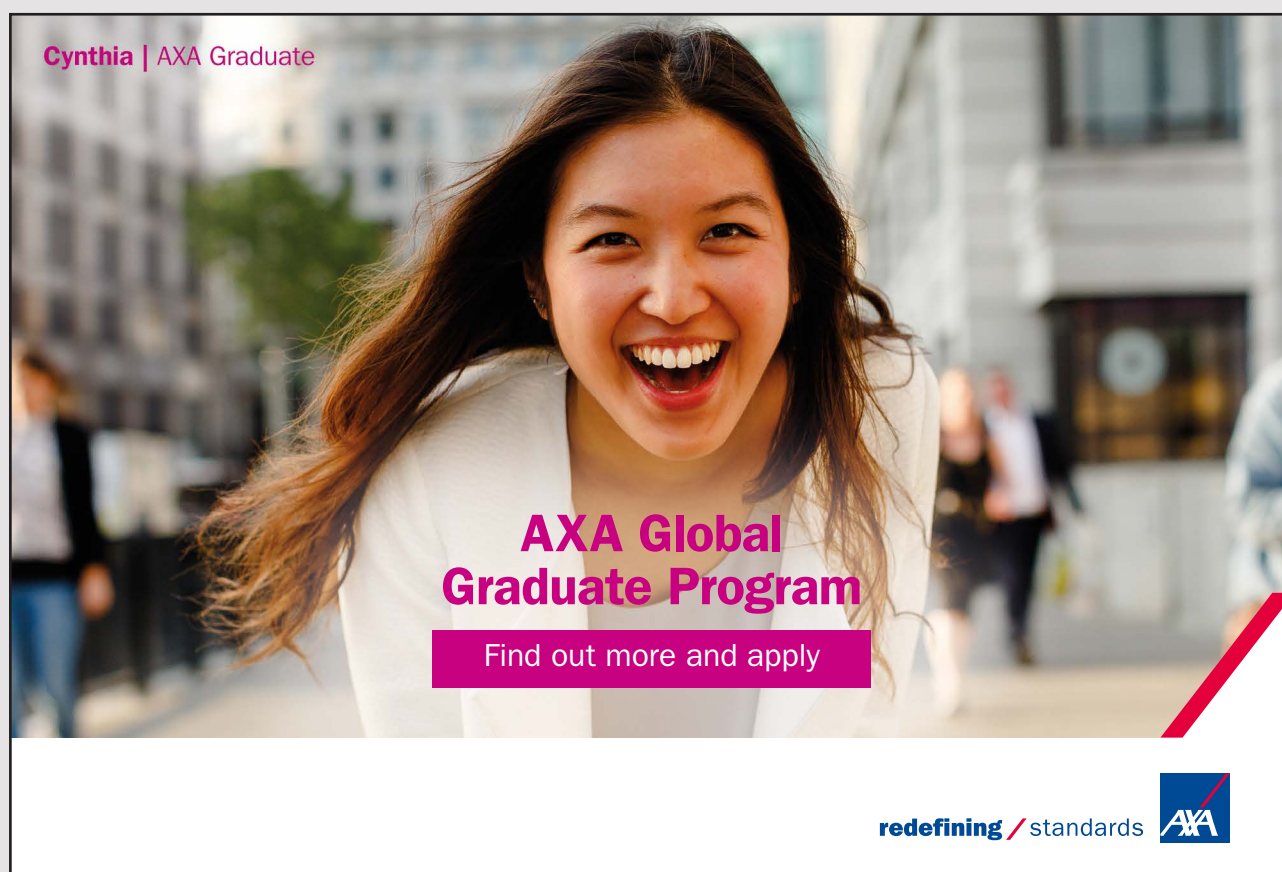
- 1) **Controller.** The role and duties of the data controller are specified in the following GDPR articles: Article 24 (Responsibility of the controller), Article 26 (Joint controllers), Article 27 (Representatives of controllers or processors not established in the Union), Article 29 (Processing under the authority of the controller or processor) and Article 31 (Cooperation with the supervisory authority).

- 2) **Processor.** Article 28 defines the responsibilities of the Processor:
 1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.
 2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes, etc.

- 3) **Data Protection Officer (DPO).** The role and duties of the data protection officer are specified in the following GDPR articles: Article 37 (Designation of the data protection officer), Article 38 (Position of the data protection officer) and Article 39 (Tasks of the data protection officer)
In general terms:
 1. The controller and the processor shall designate a data protection officer in any case where:
 - a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

- b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
 - c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.
2. A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment, etc.


4) Member State Laws. GDPR (Articles 85 - 90) state that Member State national law shall address the balance between the Freedom of Expression, Freedom of Information, and Right to Protection of Personal Data. Exemptions may be provided from some of the obligations for processing for journalistic, academic, artistic or literary expression, etc.



Cynthia | AXA Graduate

AXA Global Graduate Program

Find out more and apply

redefining / standards 

Travel & Tourism Perspective

Note that the GDPR applies to the personal data processing by the controller or processor (TR & TO Company) established in the European Union, regardless of whether the processing takes place in the Union or not. Ultimately, the change applies to almost all travel companies that offer products and services in Europe and process personal data of EU citizens as well as other users, located within its borders.

The details of the controller are noted in the Personal Data Inventory, in The Privacy Notice and other relevant documents and must be communicated to the Data Protection Authority. Also understand that a company's appointed data controller must notify privacy regulators and affected individuals in the event of certain data privacy breaches within 72 hours, etc.

Contracts between data controllers and data processors are already mandatory. The GDPR prescribes specific new clauses which must be included in such contracts, for example, an obligation on the data processors to act only on the documented instructions of the data controller, to impose confidentiality obligations on the staff who will be processing the data and to delete or return all of the personal data at the end of the provision of services related to the processing.

Travel companies also use data in marketing new promotions to people, as well as sharing large volumes of data with overseas suppliers, such as accommodation and excursion providers. All related activities must be reviewed and brought in line with the new regulations.

What should TR & TO Company Managers do?

Action 1. Appoint Data Controller

Point 1.1. Ensure the details of the controller are noted in the Personal Data Inventory, in The Privacy Notice and other relevant documents and must be communicated to the Data Protection Authority.

Point 1.2. If required, duly appoint an EU representative.

Point 1.3. Sign an agreement that sets out your EU representative's appointment and obligations

Point 1.4. Provide information about your EU representative to data subjects.

Point 1.5. Provide information about your EU representative to the DPA.

Action 2. Monitor State Laws

Point 2.1. Monitor Member State laws relating to specific processing situations (i.e., freedom of expression; employment; public access to official documents; archiving in the public interest, scientific/ historical research or statistics; and secrecy, etc.).

Point 2.2. Monitor relevant DPA guidance (and review when published).

Action 3. Manage supervisory authority requests

Point 3.1. Implement and maintain effective data governance processes.

Point 3.2. Ensure processors/subcontractors are contractually obliged to refer any notices from DPAs.

Point 3.3. Train relevant staff on data protection compliance best practice and dealing with regulators.

Point 3.4. Keep training records.

Action 4. Notify data breaches to DPA

Point 4.1. Implement procedures to ensure personal data breaches are notified to the DPA within 72 hours of knowing of breach (e.g., data breach response plans)

Point 4.2. Document all personal data breaches, including the relevant facts, effects and remedial action

Point 4.3. Ensure your processor contracts require processors to inform you of data breaches promptly so you can notify the DPA in time.

Action 5. Notify data subjects of breaches

Point 5.1. Implement procedures to ensure personal data breaches communicated to affected data subjects promptly where required/ appropriate (e.g., data breach response plans)

Point 5.2. Ensure technical measures such as encryption are used, where appropriate

Point 5.3. Ensure any orders by the DPA to communicate data breaches to affected data subjects are complied with

Point 5.4. Ensure your processor contracts require processors to inform you of data breaches promptly so you can communicate the breach to affected data subjects without delay, if appropriate.

Action 6. Select and manage processors

Point 6.1. Carry out comprehensive due diligence (or audits) to ensure you only engage processors that maintain appropriate security processes and standards

Point 6.2. Put in place processing contracts that oblige processors:

- to implement appropriate technical and organisational measures (including regarding security and transfers);
- to ensure that personal data is processed only on the controller's documented instructions;
- to ensure that your (Cloud) processor legal contract: processes the personal data only on documented instructions from the controller;
- to ensure that persons authorised to process the personal data observe confidentiality;
- to take appropriate security measures;
- respects the conditions for engaging another processor;
- assists the controller (your company) by appropriate technical and organisational measures;
- assists the controller (your company) in ensuring compliance with the obligations to security of processing;
- deletes or returns all the personal data to the controller (your company) after the end of the provision of services;
- makes available to the controller (your company) all information necessary to demonstrate compliance with the Regulation, etc.

Point 6.3. Exercise audit and inspection rights to verify compliance by processors with their obligations

See also Appendix 4 (Controller – Processor Agreement).

Action 7. Select and appoint DPO

Point 7.1. You should designate someone (within your **TR & TO Company** management or from an outside entity) to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements, even if you are not formally required to have a Data Protection Officer.

Point 7.2. The role and the responsibilities of the corporate Data Protection Officer (DPO), in general terms, are to:

- 1. Data protection and privacy program:** Develop, initiate, maintain, and revise policies and procedures for the general operation of the Data protection and privacy program and its related activities to prevent illegal, unethical, or improper conduct. Also run and manage the day-to-day operation of the Program.
- 2. Data Privacy Standards:** Develop and periodically review and update Standards of Conduct to ensure continuing currency and relevance in providing guidance to management and employees on Data Privacy issues, according to the current national and local data privacy laws and practices.
- 3. Collaboration:** Collaborate with Corporate Data protection and privacy Committee and other departments of the enterprise (e.g., Risk Management, Internal Audit, Human Resources, etc.) to direct data privacy issues to appropriate existing channels for investigation and resolution. Consult with the Corporate legal function as needed to resolve difficult legal data privacy issues.
- 4. Data Privacy Investigation:** Respond to alleged violations of rules, regulations, policies, procedures, and Standards of Data Privacy by evaluating or recommending the initiation of investigative procedures. Develop and oversee a system for uniform handling of such violations.
- 5. Data Privacy Monitoring:** Monitor, and as necessary, coordinate data protection and privacy activities of other departments to remain abreast of the status of all data privacy data protection and privacy activities and to identify trends. Also to identify potential areas of data privacy vulnerability and risk.
- 6. Data Privacy Reporting:** Ensures proper reporting of existing or potential data privacy violations to duly authorized enforcement agencies as appropriate and/or required.

More examples and details on all aspects (plans, policies, strategies, controls, questionnaires, etc.) of designing, implementing, reviewing and improving your own Data Privacy and Protection System may be found in my books listed in the Bibliography part of this book.

APPENDIX: PLANS, POLICIES AND STRATEGIES

Appendix 1: Travel and GDPR Definitions

Appendix 2: Data Protection Team Improvement Plan

Appendix 3: Technical and Organizational Data Protection Measures

Appendix 4: Controller – Processor Agreement

Appendix 5: Personal Data Breach Incident Response Plan

Appendix 6: Data Protection Technology Strategy

Appendix 7: IT Security Strategy

Appendix 8: Data Protection Policy

APPENDIX 1: TRAVEL AND GDPR DEFINITIONS

Summary

This appendix contains a set of indicative definitions of terms for the travel industry and for GDPR.

Part A: TRAVEL INDUSTRY GLOSSARY

AGENT: A business that is mainly focused on reselling tours and activities in exchange for commission fees.

APP: An app is a small software program that can be downloaded to a smart phone or tablet. It allows users to interact with businesses, play games and perform tasks on their mobile device. Apps are typically available either for free or for purchase on the Apple App store or the Android App Market.

ARTIFICIAL INTELLIGENCE: Artificial intelligence is defined as technology that can complete thought processes for itself, without human interaction, manipulation or control. Artificial Intelligence technology can perform a variety of tasks, ranging from communicating with a device user, translating a language or making a decision.

AUTOMATED PAYMENTS: Automated payment is a service where commission fee payments between tour operators and agents are automatically managed.

AUTOMATION: The creation and application of technology to monitor and control the production and delivery of products and services.

CHANNEL MANAGER: This is software that allows a company to give access to their inventories of hotel room or tours availability to distributors.

CHARTER: Chartering a tour, a bus, a boat or other means that an individual or group will make one booking for exclusive use of that vehicle, vessel or service. Many tour operators offer daily tours that can be chartered for a fixed price and include a maximum of persons.

CHATBOT: A chatbot is a computer program that can be synced with your website to provide your site visitors with real-time information in a way that mimics a human conversation. The program launches a customer service chat box when a visitor arrives on your site, providing them with an opportunity to ask questions or offer feedback.

CLOUD COMPUTING: Cloud computing is a way of managing a computer's data. Previously most data were stored on a local server, but using cloud computing all different types of data can be managed on a remote server that can be accessed by a desktop, laptop or mobile device.

GOOGLE ANALYTICS: Google Analytics is a tool that is used to help understand the functionality of your website and to make improvements in the future. This tool is designed to track the visitors that you receive, identify where those visitors came from and monitor what they are doing on your site. **GLOBAL DISTRIBUTION SYSTEM:** A global distribution system is a computer reservation system that allows a travel company to manage its reservations while at the same time communicate with its customers. GDS are used by travel agent to access flight, accommodations, car rental, tours and activities.

HOTEL: A popular accommodation choice made by travelers across the globe. Hotels typically offer one-room accommodations but many also have upgrades to suites available. They are often larger places to stay that offer more amenities such as pools, gyms and restaurants.

HOSTEL: Known as an inexpensive place to stay while traveling abroad, hostels are often geared toward the young crowd. Many people bunk with other people that they do not know in order to keep the costs down.

SECURE SOCKETS LAYER (SSL): SSL is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral.

SOCIAL MEDIA: The term used to describe the vast amounts of social networking sites available today. Social media is one of the main ways that people communicate.

TOUR OPERATOR: A person or company who operates a tour for travelers who are visiting. The operator often points out local points of interest as well as answers questions to their customers. The term is broadly use in the industry and can include dive centers, surf schools, bike rental and all sort of activity providers.

For more terms, see: <https://www.onetravel.com/travel/glossary.asp>
<https://www.rezdy.com/resource/travel-tourism-glossary/>

PART B: GDPR TERMS

Binding corporate rules (Reference: GDPR article 4(20), 47, 49, 57, 58, 64 and recitals 107, 108, 110 and 168)

Definition: ‘binding corporate rules’ means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

Biometric data (Reference: GDPR article 4(14) and recital 51 of GDPR)

Definition: ‘biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data. This includes photographs, finger-prints, facial recognition, iris scans, etc. The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person.

Consent (Reference: GDPR articles 4(11), 6, 7, 8, 9, 22, 49 and recitals 32, 33 and 38)

Definition: ‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Controller (Reference: GDPR articles 4(7) and recital 18)

Definition: ‘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;

Data concerning health (Reference: GDPR article 4(15))

Definition: ‘data concerning health’ means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

Data protection officer (Reference: GDPR articles 37 to 39, recital 97 and ARTICLE 29 DATA PROTECTION WORKING PARTY , Website: http://ec.europa.eu/justice/data-protection/index_en.htm, 16/EN WP 243 rev.01, Guidelines on Data Protection Officers ('DPOs'), Adopted on 13 December 2016, as last Revised and Adopted on 5 April 2017)

Definition: '...a person with expert knowledge of data protection law and practices should assist the controller or processor to monitor internal compliance ...'.

Data Subject (Reference: GDPR Articles 3 to 5, etc., and recitals 11, 23, 24, 28, 33, 39, etc.)

Definition: a natural person whose data is processed by a controller or processor.

Encrypted Data (Reference: GDPR Articles 6 and 32)

Definition: personal data that is protected through technological measures (encryption software and related procedures, etc.) to ensure that the data is only accessible/readable by those with specified access

Enterprise (Reference: GDPR article 4(18))

Definition: 'enterprise' means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity.

Genetic data (Reference: GDPR article 4(13))

Definition: 'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

Personal data (Reference: GDPR article 4(1) and recital 26)

Definition: 'personal data' means 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;

Personal data breach (Reference: GDPR articles 4(12))

Definition: ‘personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

Processing (Reference: GDPR articles 4(2))

Definition: ‘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;

Processor (Reference: GDPR articles 4(8))

Definition: ‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;



- The number 1 MOOC for Primary Education
- Free Digital Learning for Children 5-12
- 15 Million Children Reached

About e-Learning for Kids Established in 2004, e-Learning for Kids is a global nonprofit foundation dedicated to fun and free learning on the Internet for children ages 5 - 12 with courses in math, science, language arts, computers, health and environmental skills. Since 2005, more than 15 million children in over 190 countries have benefitted from eLessons provided by EFK! An all-volunteer staff consists of education and e-learning experts and business professionals from around the world committed to making difference. eLearning for Kids is actively seeking funding, volunteers, sponsors and courseware developers; get involved! For more information, please visit www.e-learningforkids.org.

Pseudonymisation (Reference: GDPR articles 4(5))

Definition: ‘pseudonymisation’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

Special categories of personal data (Reference: GDPR article 9 and recitals 51 to 56)

Definition: Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited.

Third party (Reference: GDPR article 4(10))

Definition: ‘third party’ means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

For more definition of GDPR terms, see:

<http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>

APPENDIX 2: DATA PROTECTION TEAM IMPROVEMENT PLAN

Objective of this plan

The main objective of the Data Protection (DP) Team Improvement Plan is to improve the organizational and operational aspects of the people working in the data protection teams that are working in implementing efforts of GDPR for the specific **TR & TO Company**.

Action 1: Scope the TR & TO DP problem

- You have to know what the DP performance problem is with your team.
- Assess their environment and concerns against your business requirements for GDPR and DP issues.
- Identify the general and specific DP issues involved in solving the specific GDPR implementation problem.
- Document the problem and the solution, in terms of specifications, needs, expectations, demands and resources required for GDPR implementation.

Action 2: Organize the TR & TO DP team

- Assign DP project manager or team manager or function manager.
- Develop terms of reference.
- Define each detail team and the roles within that DP team.
- Assign specific DP responsibilities.
- Develop and issue DP project schedule and DP reporting mechanisms.

Action 3: Link TR & TO DP team to strategy

- Set clear vision, mission and values; establish targets for the DP project, team, function, etc., and its expectations.
- Inform DP team members of the desired outcomes and measures of success.
- Invite each member to be a part of the DP team and communicate the goals and why they were selected.

Action 4: Enable TR & TO DP team culture

- Build commitment and trust by valuing the contribution of each member of the DP team.
- Build sympathy for each person's challenges.
- Ensure the competence of the whole DP team, as well as each member.
- Empower the DP team by allowing the members to work within the prescribed guidelines with each other to accomplish the goals.
- Resolve conflicts.

Action 5: Establish TR & TO DP communications

- Craft and implement DP communication policy and associated procedures.
- Ensure clarity and accountability for all types of DP communications.
- Ensure DP team shares information and develops an open mind.

Action 6: Monitor TR & TO DP activities

- Establish regular DP monitoring.
- Review progress.
- Identify issues, and resolve problems.
- Close the DP project when all DP project activities have been concluded successfully.

Action 7: Manage TR & TO DP team performance

- Develop DP performance policy for DP manager and team members.
- Link this policy with corresponding corporate performance system.
- Award DP manager and team members when performance targets are met.
- Manage DP performance issues.

APPENDIX 3: TECHNICAL AND ORGANIZATIONAL DATA PROTECTION MEASURES

These measures include organizing, designing, developing implementing, monitoring and improving a set of measures for your **TR & TO Company** to comply with the data protection principles (article 5) and with articles 32 to 34 of GDPR.

1. TR & TO Organizational data protection measures

These measures include organizing, designing, developing, implementing, monitoring and improving:

- 1) Security and privacy responsibilities of the Board of Directors
- 2) Security and privacy responsibilities of Senior Management
- 3) Appointment and responsibilities of Controller
- 4) Appointment and responsibilities of Data Protection Officer
- 5) Personnel Management System (Security and privacy aspects)
- 6) Contracts with third-party software providers
- 7) Data protection specifications with third-party data processing companies
- 8) Instructions for the security and safeguarding of confidential information
- 9) Information Systems Security and privacy Rules
- 10) Cyber Security Insurance Program
- 11) Reporting mechanisms for security incidents and privacy violations
- 12) Certification (ISO, PCI, SOX, ITIL, etc.)
- 13) Provision of controller and data protection officer details to data protection authority

2. TR & TO Technical data protection measures

2.1. Methodologies (DPIA, Data Protection by Design and by Default)

- 1) Methodology of Security and Privacy Integration in Information Systems Development
- 2) Methodology for the Development of Hotel Security Strategy for IT
- 3) Methodology for analyzing and managing information and privacy risks (DPIA)
- 4) **Methodology for integrating data protection into products and services**

2.2. Plans

- 1) Information Security Strategic Plan
- 2) Business Continuity Plan
- 3) Data Protection and Security Plans
- 4) Data Protection Program
- 5) Data Protection Awareness, Communication and Training Plan
- 6) Personal Data Requests, Complaints and Correction Plan
- 7) Third Party Risks Management Plan
- 8) Data Protection Integration Plan
- 9) Data Quality Improvement Plan
- 10) Data Security Management Plan
- 11) Social Media Governance Plan
- 12) Information Security Management Plan
- 13) Information System Security Development Plan
- 14) Privacy Complaints Plan
- 15) **IT Disaster Recovery Plan**

2.3. Data Protection Policies and Procedures:

- 1) Data Protection Policy
- 2) Encryption Policy
- 3) Pseudonymization Policy
- 4) Data Minimization Practices Policy
- 5) Minimum Personal Data Definition Policy
- 6) Continuous Evaluation of Personal Data Collection Policy
- 7) Personal Data Transformation Techniques Policy
- 8) Personal Data Documentation Procedure
- 9) Corporate Files and Records Retention Policy
- 10) Data Classification Policy
- 11) Data Quality Policy
- 12) Information Security Manual
- 13) Web Site Policy
- 14) Data Protection Guidelines
- 15) Cookies Policy

2.4. IT Security Policies and Procedures

- 1) IT Security Policy
- 2) Backup and Recovery Policy and Procedures
- 3) IT security events and breaches monitoring Procedure

2.5. Procedures for Evaluation and Improvement of Data Protection Measures

- 1) Procedure for Implementing the Data Privacy Policy
- 2) Procedure for executing internal audits for data protection
- 3) Procedure to support the implementation of external audits
- 4) Procedure for carrying out specific assessments and studies
- 5) Procedures for the implementation of Data Protection Impact Assessments
- 6) Procedures for the implementation of Data Protection by Design and by Default

2.6. Physical and Environmental Protection

- 1) Physical Security Measures
- 2) Environmental protection measures

2.7. Software and Technical Infrastructure

- 1) Data loss prevention (DLP) software
- 2) Software tools for aggregation, data masking, pseudonymisation, or anonymization
- 3) Encryption software technology
- 4) Intrusion Detection and Prevention System
- 5) Consent technical infrastructure
- 6) Technical infrastructure for enabling rights of data subjects (access, portability, rectification, deletion, etc.).

APPENDIX 4: CONTROLLER – PROCESSOR AGREEMENT

Overview

This appendix describes the GDPR requirements of processors that process personal data and details an example of such a Controller-Processor contract for **TR & TO Companies**.

Introduction

Any enterprise (private company, public organization, non-profit, etc.) that is subject to the EU General Data Protection Regulation (GDPR) as a Controller will need to have in place an appropriate contract (Controller – Processor Agreement) with any third party that it shares data with where that third party is a Processor as defined under GDPR.

GDPR is quite specific about the duties of the Controller and the Processor. Article 28 (3) of GDPR stipulates that there must be a contract in writing between the Controller and Processor which clearly sets out:

1. The subject matter of the processing and its duration;
2. The nature and purposes of processing;
3. The types of personal data, any particular special categories of data and the obligations and rights of both parties, etc.

Failure to have in place a suitable Controller – Processor Agreement is a breach of the law under GDPR.

This means that Controllers:

1. Should be carrying out an audit of their existing contracts with Processors to establish if those contracts already comply with GDPR; and
2. Should be putting in place due diligence and procurement requirements in respects of contracts that are going to be entered into to which GDPR will apply.

GDPR Requirements

Articles 28 to 36 set out issues that must be addressed in the Controller – Processor Agreement which include that the Processor:

1. Must cooperate with the relevant Data Protection Authorities in the event of an enquiry;
2. Must report data breaches to the Controller without delay;
3. May need to appoint a Data Protection Officer;
4. Must keep records of all processing activities;
5. Must comply with EU trans-border data transfer rules;
6. Must help the Controller to comply with data subjects' rights;
7. Must assist the Controller in managing the consequences of data breaches;
8. Must have adequate information security in place;
9. Must not use sub Processors without consent of the Controller;
10. Must delete or return all personal data at the end of the contract at the choice of the Controller; and
11. Must inform the Controller if the processing instructions infringe GDPR.

An example of such a contract is detailed next.

Hotel Controller – Processor Agreement Example

1. Parties to the agreement

Between:

- 1) 'TR & TO XYZ' Private Corporation ('The Company') *<complete details, such as: incorporated by xxx, address, etc.>* named the 'Controller', and
- 2) 'Processor-xyz company' *<complete details, such as: incorporated by xxx, address, etc.>* named the 'Processor')

2. Scope of the agreement

- 2.1. 'Personal data' shall include all data relating to individuals and which is processed by the Processor on behalf of 'The Company' in accordance with this Agreement.
- 2.2. 'The Company' uses the services of the Processor to process personal data *<describe what data and what processing to be done>*.
- 2.3. Both parties have agreed to enter into this Agreement to ensure compliance with the European Union General Data Protection Regulation (EU GDPR, termed 'the Act') in relation to all such processing.

3. Terms of Agreement

It is agreed as follows:

- 3.1. Processing.** The terms of this Agreement are to apply (a) to all forms and types of data processing carried out for ‘The Company’ by the Processor and (b) to all personal data held by the Processor in relation to all such processing whether such personal data is held at the date of this Agreement or received afterwards.
- 3.2. Services.** The Processor is to carry out *<describe services in detail – as per Annex 1>* and provide ‘The Company’ with the Deliverables as set out in Annex 2 and process personal data received from ‘The Company’ only on the express written instructions of designated persons of ‘The Company’.
- 3.3. Support.** The Processor shall comply at all times with the Act and shall not perform its obligations under this Agreement in such way as to cause ‘The Company’ to breach any of its applicable obligations under the Act.
- 3.4. Confidentiality.** All personal data provided to the Processor by ‘The Company’ or obtained by the Processor in the course of its work with ‘The Company’ is strictly confidential and may not be copied, disclosed or processed in any way without the express written authority of ‘The Company’.
- 3.5. Compliance.** The Processor agrees to comply with any reasonable measures required by ‘The Company’ to ensure that its obligations under this Agreement are satisfactorily performed in accordance with all applicable legislation (EU GDPR, other national laws, etc.) from time to time in force and any best practice guidance issued by the Data Protection Authority.
- 3.6. Security.** The Processor agrees to implement appropriate technical and organizational security measures (as detailed in Annex 3) and take all steps necessary to protect the personal data against unauthorized or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure, and promptly supply details of such measures as requested from ‘The Company’.
- 3.7. Data breaches - reporting.** In the event of a suspected or actual data breach or breach of security measures or breach of the confidentiality obligation or loss of confidential data, the Processor shall notify ‘The Company’ immediately, but no later than 24 hours after the incident was first discovered.

- 3.8. Data breaches - measures.** The Processor shall take all measures reasonably necessary to prevent or limit unauthorized examination, change, and provision or otherwise unlawful processing and to stop and prevent any future breach of security measures, breach of the confidentiality obligation or further loss of confidential data, without prejudice to any right ‘The Company’
- 3.9. Audit.** Without any prior notice, permit persons authorized by ‘The Company’ to enter into any premises on which personal data provided by ‘The Company’ to the Processor is processed and to inspect the Processor’s systems to ensure that sufficient security measures are in place.
- 3.10. Data subjects.** The Processor agrees to provide ‘The Company’ with full co-operation and assistance in relation to any complaint or request made by data subjects.
- 3.11. Data transfers to third parties.** The Processor agrees not transfer any personal data provided to it by ‘The Company’ to any third party without the written consent of ‘The Company’.
- 3.12. Data transfers to ‘The Company’.** The Processor shall transfer all personal data to ‘The Company’ on the Controller’s request in the formats, at the times and in compliance with the specifications agreed with ‘The Company’.
- 3.13. Liability.** The Processor shall be liable for and shall indemnify ‘The Company’ against each and every action, proceeding, liability, cost, claim, loss, expense, including reasonable legal fees and disbursements on a solicitor and client basis and demand incurred by ‘The Company’ which arise directly or in connection with the Processor’s data processing activities under this Agreement.
- 3.14. Deletion.** The Processor agrees that in the event that it is notified by ‘The Company’ that it is not required to provide any further services to ‘The Company’ under this Agreement, it, at the Controller’s request, shall destroy all such information using a secure method which ensures that it cannot be accessed by any third party and shall issue the ‘The Company’ with a written confirmation of secure disposal.
- 3.15. Monthly reporting.** The Processor shall compile a monthly report on security management within two working days after the beginning of the next calendar month, which will include the following aspects in relation to the processing of personal data of ‘The Company’: Number of transactions processed; Number

of personal data breaches; Number, status, progress and analysis of security incidents; Measures taken in the area of security management in connection with security breaches and incidents; and General measures taken in the area of personal data security.

3.16. Measures by Supervisory Authority. If the supervisory authority imposes a measure or fine on ‘The Company’ and if the cause of the measure or fine being imposed is attributable to the Processor’s failure to comply with the arrangements made in the Processor Agreement, ‘The Company’ can recover all costs for this measure or fine from the Processor. Furthermore, ‘The Company’ has the right to terminate the Agreement with immediate effect in the above situation without ‘The Company’ being entitled to any form of damages.

3.17. Copyright. All copyright, database rights and other intellectual property rights in any personal data processed under this Agreement shall belong to ‘The Company’. The Processor is licensed to use such data only for the term of and in accordance with this Agreement.

3.18. Laws. This Agreement shall be governed by the laws of *<add country>*.

SIGNED for and on behalf of ‘The Company’ by:

Print Name:
 Position:
 Signature:
 Date:

Company Seal:

SIGNED for and on behalf of The Processor by:

Print Name:
 Position:
 Signature:

Date:

Company Seal:

Annex 1: Description of services. The Processor is to carry out *<describe services in detail – as per Annex 1>* and provide ‘The Company’ with the Deliverables as set out in Annex 2, etc.

Annex 2: Description of deliverables.

<describe services in detail1>

Annex 3: Security Measures to be adopted by the Data Processor

1. The Processor will ensure that in respect of all personal data it receives from or processes on behalf of ‘The Company’ it maintains security measures to a standard appropriate to: the harm that might result from unlawful or unauthorized processing or accidental loss, damage or destruction of the personal data; and the nature of the personal data.
2. *<Provide a list of security measures, for example:>*.
 - 2.1. Security policy.
 - 2.2. Implementation of appropriate standard security safeguards (such as NIST SANS, etc.).
 - 2.3. Implementation of Physical and Environmental Security Control Actions
 - 2.4. Implementation of Data Communications Security Control Actions
 - 2.5. Implementation of Personal Computers and Office Equipment Security Control Actions
 - 2.6. Implementation of Security Administration Control Actions .

For more details, see: ‘Chapter 2: Data Security Controls’ in my book ‘Data Protection Specialized Controls: Data Protection and Privacy Guide – Vol IV’ <http://bookboon.com/en/data-protection-specialized-controls-ebook>

APPENDIX 5: PERSONAL DATA BREACH INCIDENT RESPONSE PLAN

Objective

The objective of this plan is to provide guidelines for improving the responses to potential or actual breaches to your personal data and information of your **TR & TO Company**.

Description

A personal data breach is usually defined as ‘a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service’. A personal data breach may mean that someone other than the data controller gets unauthorized access to personal data. But a personal data breach can also occur if there is unauthorized access within an organization, or if a data controller’s own employee accidentally alters or deletes personal data.

In contrast to the typical Security Incident Response, which concerns a broader range of incidents affecting information security, this control uses the term Personal Data Breach Incident to describe only those incidents that relate to personal data.

An example of such a plan is described next.

Action # 1: Maintain TR & TO personal data breach register

1. Ensure that your data controller maintains an internal personal data breach register for your hotel enterprise.

Action # 2: Establish TR & TO personal data breach organization

1. Ensure the establishment and operation of a cross-functional Personal Data Breach Incident Response Team.
2. Ensure this team reviews, approves, and participates in the execution of the Personal Data Breach Incident Response Plan.

Action # 3: Establish TR & TO data protection risk assessment process

1. Ensure the implementation of a data protection risk assessment process to determine the extent of harm, embarrassment, inconvenience, or unfairness to affected individuals.
2. Ensure the execution of the required steps to mitigate any such risks by the Personal Data Breach Incident Response Team or other corporate function (e.g., IT, Legal, etc.).

Action # 4: TR & TO Breach Notification

1. Implement procedures to report a data breach incident to the supervising authority.
2. Implement procedures to report a data breach incident to the data subject(s).
3. Ensure that the breach notification referred to above shall at least:
 - 3.1. Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
 - 3.2. Communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
 - 3.3. Describe the likely consequences of the personal data breach; and
 - 3.4. Describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
4. Implement a process to determine whether notice to oversight organizations or affected individuals is appropriate and to provide that notice accordingly.
5. Implement internal procedures to ensure prompt reporting by employees and contractors of any data breach incident to information security officials and the DPO.
6. Implement internal procedures for reporting noncompliance with organizational data protection policy by employees or contractors to appropriate management or oversight officials.
7. Include data protection clauses in tender documentation and contracts with suppliers to require suppliers to proactively notify breaches to them; and to put a great emphasis on the duty to cooperate between both parties;

APPENDIX 6: DATA PROTECTION TECHNOLOGY STRATEGY

The primary objective of the Data Protection Technology Strategy is to provide strategic guidelines for the data protection technology issues related to personal data collected and processed by information systems and information collection activities of your **TR & TO Company**.

An example of such a policy is described next.

Company ‘TR & TO Company XYZ-Fictitious Enterprise Corporation’ Data Protection Technology Strategy

1. Introduction

‘**TR & TO Company XYZ-Fictitious Enterprise Corporation**’ staff, in today’s business operating environment, may not be fully aware of the data protection and privacy as well as other cyber risks facing their data and information systems.

These risks are caused by malicious attackers: insiders and external entities or people.

Both of these types of attackers alike love to steal the enterprise’s (**‘TR & TO Company XYZ-Fictitious Enterprise Corporation’**) sensitive information and data such as customer records, employee health records, research data, intellectual property, financial records, and personal information, etc., because these data have a very high value.

In addition to this, enterprise data are also at risk due to careless and negligent employees and other trusted users with elevated levels of access such as partners and consultants.

All these make it paramount for the enterprise (**‘TR & TO Company XYZ-Fictitious Enterprise Corporation’**) to craft its own effective data protection and privacy strategy and implement it with specific technical solutions to mitigate the above-mentioned risks.

These integrated data protection strategic solutions are purpose-built to address these security risks and also streamline the process of enabling and facilitating data protection and privacy controls for the specific enterprise.

These solutions include: Using encryption; Implementing data loss prevention solutions; Monitoring database activity; Managing portable and removable storage devices; and Using personal data de-identification techniques.

These are described next.

2. Using encryption

Encryption is the process of encoding messages or information or data in such a way that only authorized parties can read it.

Encryption reduces the usefulness of any lost or stolen enterprise data of ‘**TR & TO Company** XYZ-Fictitious Enterprise Corporation’ to a large degree and even makes them, in most cases, totally useless to the hackers or other attackers who have performed a data breach.

Encryption may be used in files, folders, network transmission and files, data bases, USB drives, etc.

By using encryption solutions that are centrally managed with the information protection controls previously outlined, deployments, administration, and policy creation can be more efficient and add a better level of protection to the enterprise’s data.

3. Implementing data loss prevention solutions

Data loss prevention (DLP) is a strategy and a set of instructions and software tools (solution) for making sure that end users do not send sensitive or critical information (such as personal data, emails, files, etc.) outside the corporate network of the enterprise (‘**TR & TO Company** XYZ-Fictitious Enterprise Corporation’).

Designated DLP solutions detect and prevent unauthorized attempts to copy or send sensitive data, intentionally or unintentionally, without authorization.

An effective DLP solution will combine controls to protect the enterprise from careless or intentional data loss. Examples include uploading information, sending information outside the organization via instant messaging, or email, or even copying information to a removable media device, etc.

4. Monitoring database activity

Database activity monitoring (DAM) is the observation of actions in a **TR & TO** corporate database.

DAM software tools monitor, capture and record database events in near-real time and provide alerts about policy violations.

Database activity monitoring (DAM) operates independently of the database management system and helps enterprises address various regulatory mandates, such as: PCI DSS, HIPAA, SOX, U.S. government regulations, and EU data protection regulation, etc.

Finding sensitive data and discovering all of the databases within the enterprise ('**TR & TO Company** XYZ-Fictitious Enterprise Corporation') is a difficult task. Database activity monitoring (DAM) solutions should be able to identify databases and provide database-specific protection for all systems.

These DAM solutions should leverage a combination of virtual patching, protection from specific, known attacks, as well as the ability to terminate sessions that are seen as violating security policies, as in the case of zero-day attacks. These controls should work across physical databases as well as in virtualized and cloud computing environments.

Database activity monitoring and prevention (DAMP) is an extension to DAM that goes beyond monitoring and alerting to also block unauthorized activities.

5. Managing portable and removable storage devices

Portable and removable storage devices and media like laptops, jump drives, personal audio players, tablets, USBs, MP3 players, DVDs, and others give enterprise (i.e., '**TR & TO Company** XYZ-Fictitious Enterprise Corporation') users easy access to business and personal data on request.

As their use increases, however, so do the associated risks. The properties that make these portable and removable storage devices and media to have easy and immediate connection to various networks and hosts also make them vulnerable to losses of physical control, network attacks and data security breaches.

Using portable and removable storage devices can increase various risks, such as: the risk of data exposure (when sensitive data are exposed to the public or a third party without consent of the enterprise); the risk of data loss (when a physical device is lost); the risk of exposure to network-based attacks to and from any system the device is connected to (both directly and via networks over the internet), etc.

These risks can be mitigated by a portable and removable storage devices solution that includes a device and media control policy, various software tools and a set of management controls.

These solutions must: enforce the types of devices that can and cannot be used as well as the type of information that can be transferred via physical or wireless connections; implement procedures to handle all aspects of managing portable media and devices; scanning tools to ensure that no malicious software gets into the enterprise systems from portable media and devices; transparent and automatic encryption of data when approved information is transferred to an approved device, USB drive or network connection, etc.

6. Using personal data de-identification techniques

There are two personal data de-identification techniques that can be used by ‘**TR & TO Company** -Fictitious Enterprise Corporation’: Anonymisation and Pseudonymization.

Anonymization, in general, refers to the process of removing identifying information such that the remaining data does not identify any particular individual.

Anonymisation therefore refers to the conversion of personal data into data that cannot be used to identify an individual whether from that data itself, or from that data and other information to which the organisation has or is likely to have access. Generally, anonymisation of personal data is carried out to render the resultant data suitable for more uses than its original state would permit under data protection regimes. For example, anonymised data may be used for research and data mining where personal identifiers in the data are unnecessary or undesired. Anonymised datasets could also be a protection measure against inadvertent disclosures and security breaches.

Pseudonymization is a technique by which the most identifying fields within a data record are replaced by one or more artificial identifiers, or pseudonyms, and render the data record less identifying for potential abuse. This way, the enterprise, where feasible and within the limits of technology, locates and removes or transforms specified personal data to permit use of the retained information while reducing its sensitivity and reducing the risk resulting from disclosure. This technique (‘Pseudonymization’) reduces the risk to privacy of using personal data for research, testing, or training.

APPENDIX 7: IT SECURITY STRATEGY

The primary objective of the IT Security Strategy is to provide strategic guidelines for the control, protection and security over your **TR & TO Company's** critical information assets, such as: Information systems; Information technology and application software; Software; Data, etc.

An example of a typical **TR & TO Company's** IT security strategy is:

'Our **TR & TO Company's** IT Security Strategy will include:

- 1) Administrative controls, which aim to ensure that our entire control framework is instituted, continually supported by management, and enforced;
- 2) Physical protection of our data center;
- 3) Controls over personnel access to the data center;
- 4) Control over our operations personnel;
- 5) Control over our computer and telecommunications equipment maintenance;
- 6) Control over our archival media and storage facilities;
- 7) Logical access controls for the operating system, data base system and application software;
- 8) Network and local access security;
- 9) Identification and authentication of our users including firewalls, encryption, hashing and message transmission controls; and
- 10) A security incident monitoring and resolution mechanism'.

APPENDIX 8: DATA PROTECTION POLICY

Objective

The primary objective of this Data Protection Policy is to provide general guidelines for the data privacy issues related to the collection, use, processing, disclosure, monitoring, etc., of the personal data of our **TR & TO Company**.

An example of such a policy is described next.

Company 'TR & TO Company XYZ-Fictitious Enterprise Corporation' Data Protection Policy

1. Purpose of this policy

This policy explains how 'TR & TO Company XYZ-Fictitious Enterprise Corporation' (hereby termed the company) may collect personal data of individuals (customers, employees, partners, etc.) and use them in order to satisfy particular data protection and privacy regulatory requirements. It also outlines some of the data protection and security measures that the company is taking in order to protect data privacy and provide certain assurances on things that the company will not do.

2. Commitment

The Company considers the protection of the privacy of personal data to be of utmost importance and is committed to providing all people with a personalized service that meets the requirements of the specific individuals in a way that safeguards their privacy in accordance with the data protection and privacy regulations in force.

3. Opportunity to decline

When the company obtains personal information from you, or when you take a new service from the company, we will give you the opportunity to indicate if you do or do not (as applicable) wish to receive information from the company about other services or products.

Normally this will be done by way of a tick box on an application form or contract. You may revise the choice that you have made at any time by writing to the company informing us of the change.

4. Personal information collection

Some of the personal information the company holds about you may be sensitive personal data within the meaning of the Data Protection Act and other relevant laws. The company may collect personal information about you from a number of sources, including: (a) from you when you agree to take a service from us in which case this may include your personal and/or business contact details, (b) from you when you contact the company with an enquiry or in response to a communication from the company, in which case this may tell us something about your preferences, and (c) from publicly available sources.

5. Use of information

Information you provide to the company or the company holds about you may be used by the company to:

- a) identify you when you make enquiries,
- b) help administer, and contact you about improved administration of, any accounts, services and products provided by the company previously, now or in the future,
- c) carry out marketing analysis and customer profiling and create statistical and testing information,
- d) help the company to prevent and detect fraud or loss, and
- e) contact you by any means (including mail, email, telephone, etc.) about other services and products offered by the company, and authorized selected partners.

6. Credit reference checks

The company, in some circumstances, may do certain credit checks with licensed credit reference agencies when you apply to take a service or product. If this is applicable, then it will be stated in the terms and conditions of doing business between you and the company.

7. Disclosure of information

The company may disclose information only where legitimately requested for legal or regulatory purposes, as part of legal proceedings or prospective legal proceedings.

8. Protection of information

The company maintains strict data protection, privacy and security measures and controls in order to protect personal information. This includes following certain administrative and security policies, procedures, and data protection practices to check your identity when you telephone us, encrypting data on our websites, backing up data to offsite locations, etc., in order to ensure data protection and privacy with all applicable legal requirements.

9. Internet access

If you communicate with the company via the internet then we may occasionally use e-mail to contact you about our services and products. Please be aware that communications over the Internet, such as emails, are not secure unless they have been encrypted. The company cannot accept responsibility for any unauthorized access or loss of personal information that is beyond the company's control. We may use 'cookies' to monitor website user traffic patterns and site usage. You can normally alter the settings of your browser to prevent acceptance of cookies. However, rejecting cookies may affect your ability to use some of the products and/or services at the company's web site.

10. Monitoring of communications

All Company communications with you (including phone conversations, emails, Fax, etc.) may be monitored and recorded by the company for security, quality assurance, legal, regulatory and training purposes.

11. Data Subject Access Requests

The Company is required to permit individuals to access their own personal data held by the Company via a subject access request. Any individual wishing to exercise this right should do so in writing to the Company Data Protection Officer.

A standard form is available on the Company's data protection web pages.

The Company aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within the time limit set out in the Data Protection Act or other privacy regulation in force.

Individuals will not be entitled to access information to which any of the exemptions in the privacy regulation applies. However, only those specific pieces of information to which the exemption applies will be withheld and determining the application of exemptions will be made by the Company.

12. TR & TO Data Protection breaches

Where a Data Protection breach occurs, or is suspected, it should be reported immediately in accordance with the Data Security Breach Management Policy of the Company.

13. Contact

Queries regarding this policy or the Data Protection Act at large or any other privacy issue should be directed to the **TR & TO** Company Data Protection Officer (provide <phone....Fax:...e-mail: xxxabc@the company.com> and other details).

BIBLIOGRAPHY

1. Books by John Kyriazoglou:

- 1.1. DATA PROTECTION AND PRIVACY MANAGEMENT SYSTEM
DATA PROTECTION AND PRIVACY GUIDE – VOL I
<http://bookboon.com/en/data-protection-and-privacy-management-system-ebook>
- 1.2. DP&P STRATEGIES, POLICIES AND PLANS DATA PROTECTION
AND PRIVACY GUIDE – VOL II
<http://bookboon.com/en/dpp-strategies-policies-and-plans-ebook>
- 1.3. DATA PROTECTION IMPACT ASSESSMENT DATA PROTECTION
AND PRIVACY GUIDE – VOL III
<http://bookboon.com/en/data-protection-impact-assessment-ebook>
- 1.4. DATA PROTECTION SPECIALIZED CONTROLS DATA PROTECTION
AND PRIVACY GUIDE – VOL IV
<http://bookboon.com/en/data-protection-specialized-controls-ebook>
- 1.5. SECURITY AND DATA PRIVACY AUDIT QUESTIONNAIRES DATA
PROTECTION AND PRIVACY GUIDE – VOL V
<http://bookboon.com/en/security-and-data-privacy-audit-questionnaires-ebook>
- 1.6. ‘IT Strategic & Operational Controls’, 2010, IT Governance
<https://www.itgovernance.co.uk/shop/product/it-strategic-and-operational-controls>
- 1.7. ‘Business Management Controls: A Guide’, 2012
<http://www.acfe.com/products.aspx?id=4294984471>
<https://www.itgovernance.co.uk/shop/product/business-management-controls>
- 1.8. The CEO’s Guide To GDPR Compliance: The guide for C-Suite Members
to ensure GDPR compliance, bookboon.com, 2017
<https://bookboon.com/en/the-ceos-guide-to-gdpr-compliance-ebook>

2. Article 29 Working Party documents

- 2.1. Press release Privacy Shield
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610170
- 2.2. Guidelines on the right to „data portability“ (wp242rev.01)
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233
- 2.3. Guidelines on Data Protection Officers (‘DPOs’) (wp243rev.01)
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048
- 2.4. Guidelines on the Lead Supervisory Authority (wp244rev.01)
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611235

- 2.5. Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01)
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236
- 2.6. Guidelines on Personal data breach notification under Regulation 2016/679 (wp250)
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052
- 2.7. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251)
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053
- 2.8. Guidelines on the application and setting of administrative fines (wp253)
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237
- 2.9. Guidelines on Consent (wp259)
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611232
- 2.10. Guidelines on Transparency (wp260)
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611232

ABOUT THE AUTHOR

John Kyriazoglou, Editor-in-Chief of TheIIC Internal Controls e-Magazine.

John is a Business Thinker, Consultant and an Author. He is also a graduate of the University of Toronto (B.A. Honors), a Certified Internal Controls Auditor (CICA) and Management Consultant with over 45 years global experience on IT Auditing, IT Security, IT Project Management and Data Privacy issues.

He has written several books on Business Management Controls, IT Strategic and Operational Controls, and Ancient Greek Wisdom.

More details at: <https://www.linkedin.com/in/johnkyriazoglou/>

<https://twitter.com/jkyriazoglou>

<https://flevy.com/author/jkyriazoglou>

<https://bookboon.com/en/search?q=author%3A%22John%20Kyriazoglou%22>

Blog posts: <http://www.blogster.com/jkyriazoglou>

Disclaimer

The material, concepts, ideas, plans, policies, procedures, forms, methods, tools, etc. presented, described and analyzed in all chapters and appendices, are for educational and training purposes only. These may be used only, possibly, as an indicative base set, and should be customized by each organization, after careful and considerable thought as to the needs and requirements of each organization, taking into effect the implications and aspects of the legal, national, religious, philosophical, cultural and social environments, and expectations, within which each organization operates and exists.

Every possible effort has been made to ensure that the information contained in this book is accurate at the time of going to press, and the publishers and the author cannot accept responsibility for any errors or omissions, however caused. No responsibility for loss or damage occasioned to any person acting, or refraining from action, as a result of the material in this publication can be accepted by the publisher or the author.