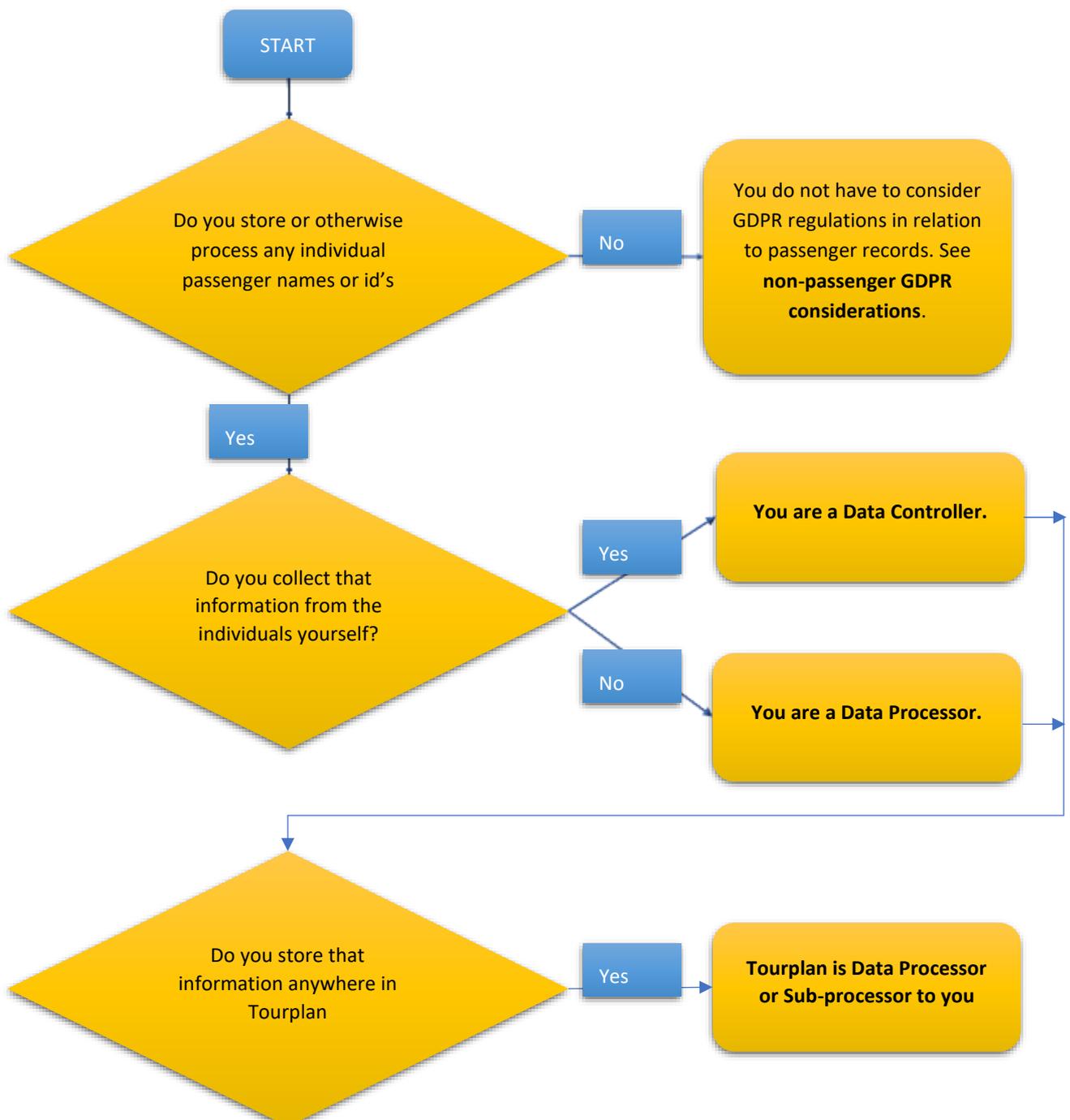


Version 1.00 - Tuesday, 30 July 2019

Tourplan is fully supportive of and in full compliance with GDPR. In this document we discuss Tourplan's and your own responsibilities in achieving compliance with GDPR. We provide our guarantees and commitments in respect of GDPR.

Two key GDPR legal definitions are the roles of **Data Controller** and **Data Processor**. Each role has important responsibilities, and potential liabilities under GDPR. There are several contexts to consider. The most relevant in the context of our industry concerns passenger information.



GDPR COMPLIANCE IN RELATION TO PASSENGER INFORMATION

By definition in GDPR, if you “**determine the purposes and means for processing personal data**” then you are a Data Controller.

The simple act of providing hotels with rooming lists probably places you into either a “Data Controller” or a “Data Processor” role assuming that any one of those individuals happens to be an EU citizen.

The rooming list example in detail:

- 1) Purpose: You have determined the purpose for recording those names e.g. assisting groups and hotels by providing rooming lists or passenger details in advance of arrival.
- 2) Means: You have determined to use an email, spreadsheet, or Tourplan to achieve the purpose.
- 3) Processing: Recording and transmitting that data are forms of processing.
- 4) Personal Data: Travellers names – Names are enough data to qualify as personal. As of course are deeper details such as Date of birth/passport number/ethnicity/contact details etc.

It is entirely legitimate that you do so, but to comply with GDPR you need to “**implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation**”.

These measures include ensuring your **Data Processor** or **Sub-Processors** provide “**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.**”

NON-PASSENGER GDPR CONSIDERATIONS

Other elements that are discussed in the GDPR context:

- 1) Names and Contacts of business contacts – typically email, phone details of Agents and Suppliers held in phonebooks and message history.
- 2) Sales and Marketing mailing or similar lists.
- 3) Tourplan's records of your staff contact details used for technical support, accounting, CRM or general business contact.

Our most recent research based on expert commentary indicates that these instances fall outside the gamut of GDPR personal privacy information.

As such, this document focuses on passenger based information.

TOURPLAN'S GDPR COMMITMENTS

Tourplan acts as your Data Processor or sub-processor in two contexts.

- 1) **Platform:** Tourplan provides a technical infrastructure on which you run your Tourplan Software – either Tourplan Cloud Platform, Tourplan Custom Cloud Platform, or CCL Hosted Platform. Through these platforms Tourplan provides data storage facilities that will contain personal data that you store and otherwise process in Tourplan. This context does not include on-premises systems.
- 2) **Support:** For the purposes of providing technical system support, implementation, upgrades and enhancements Tourplan staff may connect to your system, regardless of platform, and have access to the data in your system.

PLATFORM CONTEXT SECURITY

- Tourplan Cloud Platform – access to personal data is protected
 - through Microsoft Azure's GDPR compliance commitments
 - through login/password control into the Tourplan application – managed by the client (Data Controller)
 - against direct access to the SQL database containing the data – such access is restricted to need-to-know Tourplan technical support staff through login/password known only to those technical staff.
- Tourplan Custom Cloud Platform– access to personal data is protected
 - through Microsoft Azure's GDPR compliance commitments
 - through login/password control into the Tourplan application – managed by the client (Data Controller)
 - against direct access to the SQL database containing the data - such access restricted to system security setup designed by the client (Data Controller)
- CCL Hosted Platform – being phased out in 2019 so not considered.

SUPPORT CONTEXT SECURITY

Tourplan Technical Support teams at all escalation levels are aware of the GDPR commitments they must undertake, and all Tourplan employment contracts are being updated to include the following:

“The employee agrees that in relation to all personal information they are required to:

- a. *recognise the employer's clients' data as personal information, confidential, and subject to the confidentiality clauses in the employee's employment agreement; and*
- b. *take appropriate measure to ensure the security of any processing or data transfer; and*
- c. *only act on the data with written instruction from the client (support ticket or email); and*
- d. *not disclose personal information outside the employer's procedures, or use personal information held on others for your own purposes; and*
- e. *escalate to the employee's manager:*
 - i. *if the employee is considering engaging sub-processors to handle the data*
 - ii. *if the client requires assistance in providing subject access*
 - iii. *if data subjects attempt to involve the employee to exercise their rights under GDPR*
 - iv. *if asked to do something the employee is infringing GDPR*
 - v. *if the employee becomes aware of any data breach, being “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.”*

TOURPLAN APPLICATION COMPLIANCE WITH GDPR

Tourplan software application itself has no GDPR-inherent obligations. The application does not determine if, what and where you may store personal data. In a similar way MS-Excel is not required to provide GDPR guarantees for personal data stored in a worksheet.

In response to your requests we will offer data tools if they will assist your compliance with GDPR – for example in deleting specific booking notes records once a specific time period has elapsed after travel. Under GDPR it is incumbent on you to direct Tourplan as your Data Processor or Sub-processor on how any personal data that you have collected is to be managed.

TOURPLAN'S FURTHER COMMITMENTS IN RELATION TO GDPR:

In addition to the primary data security assurances covered in preceding sections, Tourplan commits;

- to assist you in your obligations to respond to data subjects' requests to exercise their GDPR rights;
- to meet GDPR's breach notification and assistance requirements;
- to assist you with data protection impact assessments and consultation with supervisory authorities;
- to delete or return personal data at the end of provision of services; and
- to support you with evidence of compliance with GDPR.

FORMAL AGREEMENT

A formal "Data Processor Agreement" framed as an addendum to your Tourplan NX Subscriber agreement is available at <https://www.tourplan.com/agreements/>. This agreement covers the same ground as discussed above in more detail and precision.

SUMMARY

Tourplan is committed to its own compliance with GDPR, as well as working to assist you to meet your own compliance obligations. We are wholeheartedly supportive of the individual personal privacy rights embodied in GDPR. And we are determined to provide you with the re-assurances you require to fulfil your own commitments in this area.

Please let us know of any further steps you feel we can take in this regard. (Email DPO@tourplan.com).

We consider this (evolving) document, alongside our formal agreement, to embody our complete GDPR commitments to all our clients, customers and subscribers. For the sake of clarity and consistency the commitments contained here-in supersede all prior GDPR and privacy related commitments and contracts between Tourplan and our clients, customers and subscribers.