GRPR Frequently asked questions

General Data Protection Regulation - Handling customer data

Disclaimer: These FAQs are intended to provide a general guide to the GDPR for Travel Agents and Tour Operators and cannot be treated as definitive advice on specific circumstances. The Data Protection Commissioner's Office is the Irish Supervisory Authority and can be approached for more detailed guidance on the specific. **If in doubt, it is advisable to approach the Data Protecion Commissioner's Office at www.dataprotection.ie for further guidance.**

Overview

What is the GDPR?

The GDPR is the European Regulation (Regulation (EU) 2016/679) providing new rules on how to handle personal data. This Regulation is of particular importance in the tourism sector, as companies such as travel agents and tour operators are handling and processing the personal data of their customers on a daily basis (e.g. making bookings; marketing). The Regulation applies from 25 May 2018.

The Regulation applies to the **processing of personal data**. **Processing of personal data** is any operation performed on data, whether automatic or manual, such as the collection, storage, recording, use or sharing of the data.

It is important to remember that the Regulation applies to all data, not just customer data, so you should review your processes in relation to staff and other data that you hold as well as that relating to your customers. These FAQs however are intended to cover the most commonly raised questions about customer data.

How will it affect my business?

You will have to comply with several obligations which may require some modifications of your work processes when handling customers' personal data such as:

1. Awareness among staff

If you have not already done so you should raise awareness internally of the changes resulting from the GDPR. All staff need to appreciate the impact of the Regulation and identify areas that could give rise to compliance problems under the GDPR. The protection of data should be included in the company's risk register. *As stated above, you also need to consider your data handling processes in relation to the data you hold about your staff.*

2. Information management

You should document what personal data you hold, where it came from, why you hold it and for how long, and with whom you share it. You should organise an information audit, across the organisation, or within particular business areas for this purpose.

3. Review of privacy policies

You should review your current privacy notices and make any necessary changes for GDPR compliance. The GDPR requires the information to be provided in concise, easy to understand and clear language.

4. Individuals' rights

You should review your procedures to ensure you can comply with all the rights given to your customers under GDPR. *See below*

5. Subject access requests

You should establish how you will handle requests within one month and how you will provide any additional information. There are grounds for refusing to comply with a subject access request – manifestly unfounded or excessive requests can be charged for or refused. You will also need to establish system to deal with clients' other requests, such as the right to have inaccurate data corrected. It might be useful to consider establishing systems that allow individuals to access their information easily online.

6. Legal basis for data processing

You should look at the various types of data processing carried out, identify the legal basis for carrying it out and document it. *See below*

7. Consent

Where consent is relied on as the legal basis for processing data (and it is required when processing Special Category data) you should get an unambiguous agreement from your customer for you to collect and process the data. *See below*

8. Special category data

Special category data such as information relating to customers' racial or ethnic origin, religious beliefs, health or disability, or sexual orientation can be processed as long as it is required for completing the booking and providing that the customer's explicit consent has been collected.

9. Data Protection breaches

You should make sure that you have the right procedures in place to detect, report and investigate a personal data breach. This could involve assessing the types of data held and documenting which ones would fall within the notification requirement if there was a breach. In some cases you will have to notify the customers whose data has been subject to the breach directly, for example where the breach might leave them exposed to possible financial loss.

Larger organizations will need to develop policies and procedures for managing data breaches – whether at a central or local level. It is to be noted that a failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.

10. International transfers

It will be important to ensure that you have a legal basis for transferring personal data to jurisdictions that are not recognised as having adequate data protection regulations. This will generally require the consent of the data subject, particularly where the data consists of passport information, health and dietary information. *See below*

11. Documenting data protection processes

It is important that you keep records of your data protection processes and procedures. These will help you if questions are raised about any aspect of your management of data. You should particularly document decisions about whether or not to appoint a data protection officer; any assessments of the impact of your collection of data; any assessments of your ability to rely on a legitimate interest basis for processing data; and the consents obtained from data subjects.

12. For how long can I keep my customers' personal data?

There is no explicit time limit in the GDPR. The GDPR states that "personal data shall be kept for no longer than is necessary for the purposes for which it is being processed". National limitation periods and other statutory periods will apply to certain data and so it is important to keep data securely so that it is available for these purposes. However, it is likely that much of the booking data (e.g. passport and payment details) will not be needed for the purposes of any litigation or complaint handling so where possible such data should be deleted as soon as it is no longer needed.

13. What are the risks if I do not comply with the new rules of the GDPR?

The consequences of non-compliance could be severe. A failure to comply with the provisions of the GDPR could attract a fine of up to 4% of annual worldwide turnover or 20 Million €, whichever is greater.

Data controller and data processor

The GDPR identifies two roles when handling data, the data controller and the data processor.

What is a data controller? What is a data processor? What is my role as a travel agent or tour operator?

- The data controller determines how personal data is processed and the purposes for which it is processed. This may be the role of a travel agent or tour operator. The data controller may use other companies to carry out processing services for them. In that case, the controller remains responsible for the processing of the data.
- Data processors are the entities processing the data on behalf of a data controller. The GDPR also holds processors liable for breaches or non-compliance. It's possible, then, that both your company and processing partner will be liable for penalties even if the fault is entirely on the processing partner.
- As a travel agent or tour operator, you can be, depending on the situation, either a data controller or a data processor. Usually, as a trader directly in contact with customers, it is likely you will be a data controller.

What about the data passed on to trade partners such as airlines and hotels)?

Business partners can also be a data controller as the GDPR foresees the possibility of joint controller. You should formalise your relationships with your different business partners. Therefore:

- You need to agree beforehand on the type of relations you will have with your business partners with regards to the processing of personal data,
- You should inform your customers about the fact that their data will be processed by third parties and provide their identity in your Privacy Notice.
- GDSs are considered to be data controllers for the purposes of the CRS Code of Conduct but will also act as processor for other data handling purposes.

Data Protection Officer (DPO)

What is the Data Protection Officer?

Data protection officers are responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements.

Do I need to appoint a DPO?

If a business' core activities comprise the large - scale processing of special category data or the regular and systematic monitoring of data subjects, then it is mandatory to appoint a DPO. Nonetheless, even if it is not mandatory for your business to appoint a DPO, it is recommended that all companies should consider whether or not they should appoint a DPO and, if they decide not to, the reasons for that decision should be documented so that they are available for reporting to the relevant supervisory authority where necessary.

Individuals' Rights

The main rights for individuals under the GDPR are:

• the right to be told that their data is being processed;

• access to their personal data

You cannot charge for providing this information and you must provide the information within one month of receipt of the request.

In addition, customers are entitled to have personal data rectified if it is inaccurate or incomplete.

Customers can also request the deletion or removal of personal data where there is no compelling reason for its continued processing (this is known as the right to erasure or the right to be forgotten). This applies where:

• the personal data is no longer necessary for the purpose which you originally collected or processed it for;

• you are relying on consent as your lawful basis for holding the data, and the individual withdraws their consent;

• you are relying on legitimate interests as your basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;

• you are processing the personal data for direct marketing purposes and the individual objects to that processing;

- you have processed the personal data without a proper legal basis;
- you have to do it to comply with a legal obligation; or
- you have processed the personal data to offer services online (information society services) to a child.

The right to erasure does not apply if processing is necessary for one of the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation;
- for the establishment, exercise or defence of legal claims.

There is a right to data portability where the customer can ask for their data to be provided to another data controller. This applies when processing is carried out by automated means; and is based on consent or because the processing is necessary for the performance of a contract; and where the data has been provided to the data controller by the customer. "Provided by" would include data generated by observing the customer's activity, e.g. past bookings and expenditure.

This right allows customers to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way. You will need to provide the information in a structured, commonly used and machine readable format that can be easily transferred to another controller and you cannot charge for it.

Legal Basis for Processing

You must have a legal basis to process personal data. The legal basis relied on for processing data must be one of the following:

1. you have obtained the consent for data processing from the person, or, if a child, their parent or guardian; or

2. the processing is necessary in relation to a contract which the person has entered into for a holiday or other arrangement or because they have asked for something to be done so they can enter into a contract; or

3. you must process the data because of a legal obligation that applies to you (not an obligation under a contract); or

4. the processing is in accordance with the legitimate interests condition (this is interpreted narrowly so cannot be used to simply describe the ordinary business interests a company may have to override the need for other legal bases).

Legitimate Interest Assessment

In order to rely on this reason for processing the data you must be able to show that certain requirements apply (i.e. you should undertake a Legitimate Interest Assessment (LIA) :

1. The first requirement is that you need to process the information for the purposes of your legitimate interests or for those of a third party to whom you disclose it. GDPR says that the processing of personal data for direct marketing purposes may be regarded as being carried out for a legitimate interest (but nb. Electronic marketing).

2. The second requirement, once the first has been established, is that the legitimate interests must be balanced against the interests of the individual(s) concerned.

3. Finally, the processing of information under the legitimate interests condition must be fair and lawful and must comply with all the data protection principles such as transparency, accuracy, relevance and security

The Information Commissioner has created a template for carrying out Legitimate Interest Assessments https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests.

Consent

Under the GDPR, consent will require a clear affirmative action.

The consent should be:

- **Unambiguous**: Consent requires either a statement or clear affirmative action in order to be valid. (e.g. ticking a box). Silence, pre-ticked boxes and inactivity will not suffice.
- **Freely given**: There should be a possibility to refuse. For example you cannot impose that a booking will be finalized only if the customer agrees to receive a newsletter/marketing correspondence.
- **Specific**: Consent must relate to specific processing operations (e.g. booking a flight, marketing purposes). Consequently, a general broad consent to unspecified processing operations will be invalid.
- **Right to withdraw**: Customers should have the opportunity to opt-out at any time. Therefore, if not done yet, you should consider adding an "unsubscribe" option in your correspondence and on your website.
- **Formal**: You should be able at any time to prove that you have received an explicit consent from your customer. Any written proof will work. It is possible to collect oral consent (via phone) although that will be up to the company, as a data controller, to prove that the consent had been collected (e.g. by recording the phone conversation).

Therefore it is strongly recommended to check your internal processes and verify if you fulfil the conditions listed above. If not you should amend your methods accordingly.

Is it consent if no answer is given?

No, it will not be considered as an explicit consent and you should not use the customer's data.

How to collect consent when organising a school trip?

If you are organising school trips, you should ensure that the minor's parents/tutors are duly informed that the children's data will be handled and used by you in order to organise the trip. The responsible teacher or staff member should also be authorised by the parents to collect the minor's data and forward them to you. This will mean that the form to be signed by the parents should contain a privacy notice informing them of the above. Consent should be obtained from the parents for the children's data to be collected by the teacher; passed to the travel company; and then passed to the travel service suppliers. Preparing a model form to be signed by the parents/tutors would be advisable.

Privacy Notices

What should be included in the Privacy Notice?

As we have seen, individuals have the right to be informed that their data is being processed. You should give this information through the use of Privacy Notices. There is a list of information that must be included in a Privacy Notice and this must be given in a concise, transparent, intelligible and easily accessible form; in clear and plain language; and free of charge.

As well as the full form of Privacy Notice, you should ensure that customers are told at each point that you collect their data why you are collecting the data and what the data will be used for. Where you must obtain the customer's consent in order to process the data, for example where you are passing special category data to a supplier, you must tell the customer who you will be sharing the data with.

A link to the company's full Privacy Notice should be provided at an early stage of the booking process.

The full Privacy Notice should include the following information:

Where you collect the data directly from the data subject you must provide them with the following information:

- The identity and contact details of the data controller or the data controller's representative.
- The contact details of the data protection officer where one is appointed.
- Why you are processing the data and the legal basis on which you are processing it.
- Where you are relying on the legitimate interest condition, what those legitimate interests are.
- Who you will be sharing the data with. This will be a list of suppliers where that is possible or the categories of suppliers e.g. airlines, hotels etc.
- When your sharing and the subsequent use of data is based on consent, data subjects must be informed of the identity of data controllers relying on that consent.
- Where applicable, the fact that you intend sending the data outside of the EEA and what safeguards are in place.
- How long you will be holding the data for or the criteria that you use to determine what any retention period will be.
- The fact that the data subject has the right to request access to the data held about them; rectification of any errors; erasure of the data where appropriate; as well as the right to data portability.
- Where the data is processed due to the consent of the data subject, their right to withdraw their consent.
- The data subject's right to complain to the relevant supervisory authority.
- Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data.

Where you have not collected the data directly from the data subject you must provide them with the additional following information:

- The categories of personal data that you hold. You should explain what types of data you hold
- about individuals where the individuals have not given you this information themselves.
- The source from which the data has been obtained.

Where should the Privacy Notice be displayed and at what stage of the booking process?

Customers should be informed throughout the booking process about your collection and use of their data. This is in addition to the need to give clear and easy access to your full Privacy Notice.

As part of the booking process, whether online or offline in a shop or on the telephone a statement should be provided along the lines of:

We are collecting your personal information for the purposes of booking the travel services that you have requested. This information, including any information about any health or medical issues that you tell us about and your passport details will be sent to the suppliers who will be providing your

travel services. These suppliers may be based outside of the EU where the protection of personal data may not be as strong as it is in the EU.

By *signing this booking form/ticking this box/giving your consent* you agree to us passing on your personal details for the purposes of your booking. Our full Privacy Notice can be found on our website.

We will also use your details to notify you of travel offers that we think might be of interest to you. *Tick here/tell us now* if you do not wish to receive such offers.

For telephone sales a script could be developed along the lines above which could be turned into a recorded message to be played whenever a customer contacts the call centre. Consent should be obtained by email or post following the telephone call.

International Transfers

As travel agents and tour operators, you will work with commercial partners not established in the EU/EEA. Therefore, it is important to clarify your relationships with these partners. You should ensure that you have a correct legal basis for transferring personal data in the first place and then that you have the ability to transfer the data to countries that do not ensure an adequate level of protection as determined by the Commission. *At the time of writing, only the following countries, outside of the EEA, have an adequate level of protection: Andorra, Argentina, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland, and Uruguay. Canada and the USA are also considered to have adequate levels of protection in limited circumstances.*

Where there are regular transfers of data to a supplier or other partner located in a country that does not have an adequate level of protection, you will need to make sure that there are adequate safeguards in place. This will usually be achieved by including in your contract with the supplier the standard data protection clauses adopted by the Commission or your supervisory authority. The European Commission has so far issued two sets of standard contractual clauses for data transfers from data controllers in the EU to data controllers established outside the EU or European Economic Area (EEA). It has also issued one set of contractual clauses for data transfers from controllers in the EU to processors established outside the EU or EEA https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en

If the transfer of data is not a regular process you can transfer data on the basis of the necessity to transfer the data for the performance of a contract or, and particularly where special category data is involved, the consent of the data subject. The transfer by travel agents of personal data concerning their individual clients to hotels or to other commercial partners that would be called upon in the organisation of these client's stay abroad has been cited by the Article 29 Working Party paper of 6 February 2018 paper as an example of when the arrangements for non-regular transfers might occur.

Direct Marketing

Can I use the data I collect to do direct marketing?

For the purposes of GDPR, in the appropriate circumstances you will be able to rely on legitimate interests as the legal basis for processing data for direct marketing. A Legitimate Interest Assessment (***see above***) should be carried out but, if the marketing is restricted to travel services and the data subject is given a clear method of opting out of future marketing, it is likely that such an Assessment should show the necessary balance of interests.

With regard to electronic marketing however, the provisions of the e-Privacy Directive apply meaning that the data of individual persons, including employees of sole trader or partnership businesses (as opposed to employees of limited companies and PLCs) can only be used for direct marketing purposes where the data subjects has given their consent.

However, electronic marketing can also be carried out by way of what is known as the soft opt-in where:

1. the data has been collected from the data subject through the previous sale of the company's services; and
2. where the data subject was given the opportunity to opt out of receiving marketing communications from the company and did not do so; and
3. where the marketing relates to similar services to those which the data subject had previously expressed interest in; and
4. where the customer is given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details on the occasion of each subsequent message.

What should I do with my old database of email addresses?

This depends on how the data was collected in the first place. If it was collected in the course of the sale of your services and the data subjects were given the option of opting out of future mailings and did not do so, you should be able to continue using that data under the e-Privacy Directive and on the basis of legitimate interest under GDPR.

What about list of contacts I bought from other traders or a specialised company?

Subject to national laws, you can use lists obtained from other trade partners as long as the listed persons have given their explicit consent and are aware of your identity as a trader and for what purpose you collected their data.

What about events where guests/visitors gives business cards or enter in competitions by giving their personal detail (e.g. email address)?

If your company organises an event to collect emails, it is possible to use the data collected under the GDPR. You should make it clear what the data collected will be used for. If it is intended to be used for purposes other than the competition (e.g. marketing), then, under GDPR, it is likely that you could rely on legitimate interests as the legal basis for processing. However, if that marketing is to be done electronically, then the rules of the e-Privacy Directive apply and the consent of the data subjects will be needed where they are personal subscribers

It might be difficult to distinguish between the data collected for personal and corporate subscribers and so it might be advisable to treat all data subjects as personal subscribers. Consent could then be obtained at the time of collection or, where national law permits, by sending a follow-up email without any marketing content, seeking the consent to send further marketing.

Should I take particular precautions with photos of customers used for marketing purposes?

When you use photos for marketing purpose (brochure, website, social media) which involve individuals, it is necessary to collect the explicit written consent of all those featured in the picture.

The best way to achieve this is via a photography release form. This must be signed and include a clear indication of how the photos are going to be used. If photos feature children under the age of 18, full written parental consent must be given.

Moreover you should keep in mind that, even after collecting the explicit consents, the individuals featured can always assert the following rights

- The right to be informed: you should clearly inform about the context of how the photos are being used (e.g. social media, website, brochure). It also means that you should not use a photo for a purpose which had not been previously agreed on.
- The right to access: Individuals have the right to access their personal data (photos) on request, and receive confirmation regarding how these are being used.
- The right to be forgotten/right to erasure: Individuals have the right to request photos be removed from websites, social media and/or future versions of printed materials.

It is therefore advisable to keep track of:

- how the photos are being used and for what purpose,
- who are the individuals identifiable on the photo
- where are stored the photos and the release forms

For how long can I keep my customers' personal data?

There is no explicit time limit in the GDPR. The GDPR states that "personal data shall be kept for no longer than is necessary for the purposes for which it is being processed". For the purposes of direct marketing, if this is based on legitimate interests and the soft opt-in under the e-Privacy Directive, as long as you are providing a clear method of opting out of future mailings, your continued use of the data should not be a problem where you are sending mailings on a regular basis. If you have not sent such mailings for more than 12 months, you probably cannot assume that the soft opt-in or legitimate interest bases will suffice. In practice, you will probably want to refresh any data from subjects that have not responded to any mailings for more than, perhaps, 24 months by way of an email asking them to update their details and confirm that they consent to receiving future mailings.

Security

What steps need to be taken in order to fulfil the security requirements under the GDPR:

You should carry out a detailed and objective audit of the data that you hold; where you hold it; who it is shared with and the purposes for which it is held. An assessment should be carried out setting out the type of personal data being processed and the processing operations and evaluating the risks.

Based on the assessment, appropriate technical and organizational measures should be implemented such as:

- The pseudonymisation and encryption of personal data.
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services (e.g.: strong password, regular update of software and firewall, anti-virus, anti-malware).
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident (e.g. regular backup).
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.
- Vetting and training of staff, contractors, vendors and suppliers on continuous basis
- Provide training to staff on data processing obligations, identification of breaches and risks. Even with state of art security software you may not be able to prevent some breaches without having appropriately trained staff
- Restrict staff access to personal data to those who need to know (also referred to as the "*principle of least authority*")
- Ensure physical security on premises (e.g. policy for staff to lock away their documents overnight in secure cabinets, and destroy any sensitive printouts, which are no longer needed, by putting them in a confidential bin or through a cross cut shredder)
- Put in place a BYOD (bring your own device policy) if you allow use of personal devices for work

- Implement a strict ban on the use of personal email for work purposes.

Does ISO 27001 implementation satisfy EU GDPR requirements?

The implementation of ISO 27001 covers most of the requirements of the EU GDPR; however, some controls should be adapted to include personal data within the Information Security Management System.

Date: 30th April, 2018