D-1017-246-MM

HOTREC guidelines on the General Data Protection Regulation

- **Preamble**: the Data Protection is one of the most complex Regulations ever adopted in the EU, which makes interpretation mandatory, reason why of this note;
- **Impact**: The General Regulation on Data Protection concerns the hospitality industry as all establishments' process personal data (e.g. e-mails; names; addresses of clients). The Regulation needs to be applied in all Member States from 25 May 2018 onwards;
- **Objectives**: This note provides a summary of the main outcome of the General Data Protection Regulation and how it should be applied by the hospitality sector (hotels, restaurants, cafés, national associations) under the understanding of HOTREC.

Context

All companies (hotels, restaurants, national associations) processing data will have to apply fully the General Regulation on Data Protection (Regulation (EU) 2016/679) from 25 May 2018 onwards.

Part I - Main content of the Regulation

(Applicable to all companies in the hospitality sector: hotels, restaurants, cafés, bars as well as national associations)

Scope

The Regulation applies to the processing of personal data wholly or partly by automated means and to processing that is part of filing (art.2).

Territorial scope

The Regulation applies to:

- Companies located in the EU which process personal data of clients (regardless of whether the processing takes place in the Union or not) – art 3/1;
- Companies which process personal data of clients who are in the EU, even if the company that processes the data is not established in the EU (this could be the case of hotel chains) – art.3/2.

What are the basic principles of the Regulation?

- **Fair, lawful and transparent processing (**art.5/1/a) - personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject (e.g. client);
- **The purpose limitation principle** (art. 5/1/b) - Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes;
- **Data Minimisation** (art. 5/1/c) - Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed;
- **Accuracy** (art. 5/1/d) - personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate are either erased or rectified without delay – integrity and confidentiality;
- **Data retention period** (art. 5/1/e) **-** Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- **Data security** (art.5/1/f) **-** Personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures;
- **Accountability (art.5/2) -** The controller is responsible for, and must be able to demonstrate, compliance with the Data Protection Principles.

When is it legal for hotels, restaurants, bars and national associations to process data under HOTREC's understanding?

- **When a client has provided consent (art.6/1/a).** Consent needs to be based on a freely given, specific, informed and unambiguous indication of the client. The controller (e.g. company) should be able to demonstrate that the client has consented to the processing (art. 7).

  HOTREC considers that processing with the data subject's consent is the safest way of processing information, therefore there will be no room for interpretation. If data subjects (e.g. clients) provide consent, the companies can legally process the data.

  But companies should also consider that clients might not be interested in providing consent – in this case, there is a potential risk for the companies to loose potential clients.

  Moreover, whereas it is reminded that one does not need to consider requesting consent where processing is based on legislation (e.g. passenger information under Schengen Agreement), one must also acknowledge that there is a risk that consent is withdrawn. If this happens, companies cannot process data on the basis of consent anymore.

Also, it is important to note that, if companies handle data based on a consent, data provided by the data subject should follow the right to data portability[1].

Apart from consent, the Regulation allows companies in the hospitality sector to process data on the following basis:

- **When processing is part of a contract - art 6/1/b**

  Example: when clients use the hotel services, it is usually under the framework of a contract – accommodation agreement between the hotel and a client.

  It is important to note that if companies handle data based on a contract, the data provided by the data subject should follow the right to data portability.

- **When processing is necessary to comply with legal obligation (art. 6/1/c);**

  Example: when a hotel is required to collect certain data from clients staying at the hotel on the basis of a national legislation. Many countries have this kind of legislation due to the Schengen Treaty.

- **When processing is necessary for the purposes of the legitimate interests pursued by the controller (company) – art.6/1/f;**

  HOTREC considers that it is practical for the hotels to process client data under a contract (6/1/b)[2] *and a legitimate interest (6/1/f) in addition to the requirements of legislation*[3].

- **If national legislation allows (art.6/2).**

  Example: Legislation based on the Schengen Agreement leaves it up to Member States to decide how the data from the hotel clients' is collected. For instance in Belgium, hotels might take a photocopy of the ID of the client in order to follow Schengen rules. Hotels in Belgium will legally continue to do so.

Nota bene: the above mentioned legal grounds to process data apply to the processing of **ordinary data**. The Regulation also foresees special rules for the processing of special categories of personal data (art.9). For instance, if the company uses biometric data (e.g. fingerprint) to identify a client, the processing of this data falls under art.9.

What are the rights of the data subjects (e.g. clients)?

- **Right to be informed** - the Regulation obliges the controller (e.g. hotel) to inform data

[1] See explanation of the right to portability on page 4.
[2] It is important to note, one more time, that if companies handle data based on a contract, the data provided by the data subject should follow the right to data portability – see more information on page 4.
[3] Please also see page 8.

subjects on certain issues – art.14[4].

- **Right of access** – art. 15 – clients have the right to know if personal data is being processed or not, and, if this is the case, be able to access the information (e.g. right to ask the erasure of the personal data by the controller);

- **Right to be forgotten** – art.17 - personal data of clients should be erased as long as the data is no longer necessary in relation to the purpose for which they were collected; the client withdraws consent; the client objects to the processing, amongst other cases);

  Note bene: under HOTREC's understanding, hotels, restaurants and bars are not obliged to delete completely data from former clients. HOTREC understands that at least a minimum of data can be processed, as the processing of personal data for direct marketing purposes can be regarded as carried out in the legitimate interest of the controller (art.6/1/f in conjunction with recital 47)[5] [6].

- **Right to rectification** – art. 16 – Clients shall have the right to obtain the rectification of inaccurate personal data without undue delay;

- **Right of data portability** – art. 20 – clients have the right to receive the data concerning him/her in a structured way and have the right to transmit that data to another controller, when the basis of the processing activities is consent or a contract (art.20/1/a). The right concerns only the kind of information that a data subject has provided to a controller.

  Data which is processed solely on the basis of a legitimate interest does not fall under the right of data portability.

  It is, therefore, important for companies to assess if they process the data on the basis of their legitimate interest. If this is the case, then there is no need for the controller to comply with right of data portability.

- **Right to object** – art.21 – the client has the right to object to the processing of the data (e.g.: when personal data is processed for direct marketing purposes, the data subject (e.g. client) shall have the right to object at any time of the processing. If this is the case, the company should immediately comply with the client's willingness).

What are the obligation for the controllers/processors (e.g. companies)?

- **Complying with the Risk Based approach**

  - The controller (e.g. hotelier) should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing

[4] Please see more information on section II of this paper regarding hotels.
[5] This was the interpretation of the Council during the negotiations of the Regulation with the European Parliament.
[6] Please also see HOTREC's explanation on page 8 of this document.

activities with the Regulation, including the effectiveness of the measures taken. The measures should take into account the nature, scope, context and purposes of processing and the risk for the rights and freedoms of individuals (recital 74 and article 24);

- The likelihood of the risk for the rights and freedoms of the data subject should be determined by the nature, scope, context and purpose of data processing. Risk should be evaluated based on an active assessment, by which it is established weather data processing operations involve a risk or a high risk (recital 76);
- Examples of high risk include cases of physical, material or moral damage, in particular where the processing can give raise to discrimination, identity theft or fraud, financial loss, damage to the reputation or any significant economic or social disadvantage; or where data subjects are deprived from their rights and freedoms (recital 75);

Impact to the industry: when processing personal data, companies will need to assess the risk (risk/high risk) of processing certain data and react accordingly[7].

HOTREC is of the opinion that companies processing data in the hospitality sector **do not**, **on a general basis**[8], **constitute a high risk**.

- **Data protection by design** – art 25/1 – the company shall implement technical and organisational measures to integrate the necessary safeguards into data processing. To do this, nature, scope, context and purpose of the processing should be taken into account;
- **Data protection by default** – art 25/2 – companies can only process data which are necessary for each specific purpose of the processing;
- **Communication of the data breach to the supervisory authority** shall be done without undue delay, and where feasible no later than 72 hours, unless the personal data breach is unlikely to result in a risk for the rights and freedoms of individuals (art.33)[9];
- **Records of processing activities –** art 30 **–** each controller and processor (e.g. hotel) shall maintain a record of processing activities under its responsibility. The record should contain, amongst others, the name and contact details of the controller; the purposes of the processing; if possible, the envisaged time limits for erasure of the data.

  According to HOTREC's understanding, companies should record information per category: client's data; data on potential clients, data processed on the basis of legislation (e.g. Schengen Treaty); data on personnel, etc., in order to facilitate the recording.

[7] The European Data Protection Authorities will probably work on a more precise definition of risk and will identify and characterise the different types of risk.
[8] Please see HOTREC comments on Impact assessment (page 9)
[9] The original Commission proposal made reference to a 24 hours deadline.

- **Data Protection Officer**

  - Under HOTREC's understanding/interpretation, **the Data Protection Officer (DPO) is not compulsory neither for SME's, nor for hotel chains,** because the hospitality sector companies' core business is not data processing (art.37). Under HOTREC's point of view, the core business of an hotel/restaurant is to provide a service to client.

  - The DPO is only mandatory in the following cases (art. 37/1):

    - The processing of the data is carried out by a public authority, or

    - The core activities of the company consist of processing operations, which by virtue of their nature, scope or purposes require regular and systematic monitoring of data subjects on a large scale (e.g. Facebook; Google), or;

    - The core activities of the company consist of processing special categories of data on a large scale (e.g. criminal convictions or revealing political opinions, etc.)

    - The DPO is also mandatory where required by Union or Member State Law (37/4)

Impact to the industry: Estimates show that the DPO could cost 12.000€ in the first year for companies. But, it is up to the companies to decide whether to have a DPO or not.

It is to note that under the interpretation of the European Institutions (Council of the European Union, European Parliament (EP) and European Commission), hotels and restaurants do not have to hire a DPO on a mandatory basis[10]. But both the Commission and the EP recommend that companies have the DPO in order for the Regulation to be implemented correctly and in order for companies to avoid the payment of heavy fines.

A DPO can be hired by a group of undertakings, as long as the DPO is easily accessible from each establishment (art.37/2).

- **Standardised icons**

Standardised icons produced by the controller (company) with the objective of providing certain information to the data subject (clients) are voluntary (and not compulsory, as it was the European Parliament's intention) – art.12/7;

Impact to the industry: it is up to the companies to decide whether they are willing to invest on standardised icons to provide information to clients on how the data is processed.

Other important topics:

[10] HOTREC obtained this information by phone from the three institutions, right after the text had been adopted.

- **Impact assessments[11] (art.35) and prior consultation**[12] (art.36) shall only be done in case there is a high risk for the rights and freedoms of the individuals[13]. HOTREC is of the opinion that, on a general basis, data processed in an hotel/restaurant does not constitute a high risk. Therefore, HOTREC considers that companies in the hospitality sector, usually, do not need to develop impact assessments or prior consultations. But there might be few exceptions[14].

- **Transfer of personal data to third countries or International Organisations – companies** (e.g. hotel chains) might transfer data to a third country when:

    - The Commission has decided that the third country ensures an adequate level of protection (art.45); or

    - If the third country has adduced appropriate safeguards (e.g.: binding corporate rules; legally binding instruments; standard data protection clauses; approved codes of conduct or certification mechanisms) – art.46.

- **Remedies**

    - **Right to lodge a complaint with a supervisory authority –** art. 77/1 – every client shall have the right to lodge a complaint with a supervisory authority;

    - **Right to an effective judicial remedy –** art. 78 - each client shall have the right to an effective judicial remedy if they consider their rights have been infringed.

- **One-stop-shop mechanism** - art. 4/16 + 4/23; recital 124; 62/2 - when the processing of personal data takes place in more than one member state (example of an hotel chain), one single supervisory authority should be competent for monitoring the activities of the controller or processor throughout the Union and taking the related decisions. The main establishment of a company in the E.U. is usually the place of its central administration in the Union.

Impact to the industry: businesses will be supervised by one single supervisory authority, instead of several. Businesses will need to produce less notifications, which means a cut in red tape.

- **Administrative fines –** art.83 – non-compliance with the Regulation might be subject to administrative fines up to 20 000 000 EUR, or in case of an enterprise up to 4% of the total worldwide annual turnover of the preceding financial year.

---

[11] The controller (the company) might need to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. In this case, the controller shall seek the advice of a data protection officer (35/2);

[12] The controller (company) shall consult the supervisory authority prior to the processing of personal data where a data protection impact assessment indicates that the processing would result in a high risk in the absence of the measures taken by the controller to mitigate the risk.

[13] The original Commission proposal referred to any operation presenting specific risks. The fact that the Regulation only requires companies that pose a high risk to comply with the impact assessment and prior consultation was a lobbying victory for HOTREC.

[14] Please see page 9.

Impact to the industry: businesses shall comply very well with the Regulation in order to avoid the need to pay for any penalties.

Part II - Special guidelines to Hotels/restaurants/cafés

- **Processing data on the legitimate interest of the hotel**

As already mentioned before, HOTREC considers that it is easy (in the sense of practical) for the hotels to process client data under a contract (6/1/b) and a legitimate interest (6/1/f) in addition to the requirements of legislation.

In fact, it is easy for the hotels to have a legitimate interest as a legal basis even though processing of client's data is based on a contract (accommodation agreement between a hotel and a client). Legitimate interest allows data to be processed as long as there is a relationship between the hotel and the client. The challenge is to determine when a client's relationship begins and ends. It can be considered that the relationship begins when a client makes a reservation in a hotel, leading to an accommodation. It can also be argued, that if there is no activity between a hotel and a client for a certain period of time after the last visit that the relationship has come to an end.

When using legitimate interest as a legal basis, the hotels should create criteria to determine when the relationship begins and ends. If the hotel processes data under a legitimate interest, than it has the right to process more comprehensive data on clients compared to a contractual basis. Moreover, processing can continue between the hotel and the client until when the hotel considers that that there is a relationship with the client. Under these circumstances, the processed data does not have to be limited to what is necessary for contract purposes.

- **Is direct marketing possible?**

Under HOTREC's understanding direct marketing is possible – meaning that hotels and restaurants can contact former clients, as they can become customers again, as long as the company only processes the data that is necessary for direct marketing purposes (e.g. promotions, newsletters, etc.).

Explanation in detail:

Under HOTREC´s interpretation and understanding, a hotel has a legitimate interest to process data of former and new potential clients for direct marketing purposes without consent (art.6/1/f + recital 47).

Recital 47 also specifies that: "Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller".

Nevertheless, companies should then, under HOTREC's opinion, access the client's data and comply with the data minimisation principle to keep only the information that is necessary for direct marketing purposes (also taking into account that personal data of clients should be erased as long as the data is no longer necessary in relation to the purpose for which they were collected (art. 14)). In any case, if the client objects to the processing, the company needs to take immediate measures to eliminate the client's data from its database (art.21).

In any case, hotels should keep the data of former clients, if the EU or national legislation says so and limited to the requirements of the legislation.

Nevertheless, it is to take into account that the European Commission recommends companies to ask in the contract signed with the clients' whether they are allowed to contact old clients for the purposes of promotions, newsletters, etc., or not - basically, the Commission recommends companies to ask for client's consent, in accordance with art. 6/1/a + art.7.

It must be noted that if a hotel has a loyal customer program, it is common practise that customers who have joined it, have given consent to data processing for various purposes. This is a clear demonstration of the sector's specific needs.

Do hotels represent a high risk, as they deal with credit cards on a daily basis? Do they need to do impact assessments?

- If supervisory authorities at national level argue that hotels/restaurants might represent a high risk, as they deal with credit card data on a daily basis, national associations might argue that there are strict security rules regarding card payments, namely PCI-DSS-rules by Visa and Mastercard. According to HOTREC's information hotel chains don't handle online card payments directly in their own systems[15]. Therefore, impact assessments and possible prior consultations are not necessary. In case companies ask for the client's credit card data over the phone, it is crucial that they don't store sensitive authentication data or the card verification code which can be used for fraudulent transactions. If they store these data, there might be a need to run impact assessments (and possible prior-consultations)[16]. But in this last case, companies would be in breach of the Visa/Mastercard PCI-DSS rules. If the data falls in the wrong hands, large fines would be charged to credit card companies and hotels would probably face a lock-out from the credit card schemes (which could lead to the hotel bankruptcy). HOTREC considers that this practice is illegal.

[15] The card payment service is normally handled by a PCI-DSS compliant PSP – Payment Service Provider, and no personal information regarding the card holder is forwarded to the reservation office of the chain (or to the hotels).

[16] If an hotel processes and stores sensitive card holder data contrary to PCI – standard and especially in a large scale, one has to asses whether impact assesment is needed or not, even though sensitive card holder data does not fall under article 9(1). WP 29 guidelines on the impact assessment (link) states that beyond provisions (referring to art 9(1) and 10 of the GDPR), some categories of data can be considered as increasing the possible risk to the rights and freedoms of individuals because their violation clearly involves serious impacts in the data subject's daily life (such as financial data that might be used for payment fraud).

- National Associations should also be alerted to the fact that often OTAs forward card numbers by mail or unencrypted means directly to the hotel where the reservation is made (which is against the PCI-DSS rules). If this happens, hotels need to handle these personal data from clients. On this particular point, one can argue that it is the OTA that is not complying with the legislation. But in order to be accurate, and in case hotels store sensitive data (e.g.: authentication data or card verification code), HOTREC wonders whether impact assessments would not be necessary[17].

- Hotel chains will need to access the risk of their databases (e.g. hotel loyalty programmes). Depending on the type of data stored and the total amount of data stored, there might be a need to develop a risk assessment (and possibly a prior-consultation afterwards);

- National Associations should be aware of the lists developed by the supervisory authorities in each Member State stating the kind of processing operations which are subject to the requirement for an impact assessment. If hotel/restaurant activities are included in the lists, then an impact assessment is needed (art. 35/4). HOTREC recommends national associations to contact their supervisory authorities and explain them why an hotel does not represent a high risk to the rights and freedoms of natural persons.

How does the right of information apply to hotels?

As already mentioned, the Regulation obliges the hotel to inform data subjects on certain issues – art.14.

Information obligation applies to situations where the data is collected from the data subject but also when data is not obtained from the data subject.

For instance, in an hotel´s reservation site, where a client is required to fill his/her personal data in order to make a reservation, data is collected from the data subject. The information should be available for the data subject at the same time as the data is collected. In HOTREC´s opinion this obligation can be fulfilled by notifying the data subject (e.g. client) in a reservation phase or in a reservation confirmation on how this information can be accessed and by providing a link to an information document or a website where information can be found.

In any case, clients must be informed actively. For instance, if a client asks through a website, how his/her data is processed, the hotel should actively provide the required information.

How can companies/restaurants process information on special diets/allergens?

Companies in hospitality industry process information concerning special diets and allergens.

[17] Please see footnote number 15.

Especially in (large) events and conferences, information of special diets can be required and collected in advance from the event organiser or directly from the participants. Information is necessary for preparing and serving the right amount of normal and special diet meals in an event.

Under HOTREC's understanding, processing of health data is possible if data subjects have given an explicit consent for processing or if there is special legislation foreseen in article 9/2. The legal basis for the hospitality industry to process health information can be consent. The processing of health information should also be necessary.

Taking into account a justified need to collect and process information on special diets in restaurant and catering business' and the fact that there is strict regulation towards processing data on a person's health, it is advisable to create practices where information collected in a register or processed by automatic means, concern only data of served food (for example gluten free or lactose-free meal or nut free meal etc.) and where processing information of person's health is avoided (for example celiac disease or allergy to certain food items). It is not necessary to collect data on why a special diet is chosen. It is sufficient to have information about the food.

When information is collected and processed in a way that special diet requirement can be identified to relate to a particular customer, it is advisable to inform the customer, when requesting meal preferences that the given information is not used for other purposes than to prepare and serve food to a customer and ask for consent. In this way processing of customer's special diet information, would be based on a given consent.

Part III - Special guidelines for HOTREC National Associations

- HOTREC National Associations are encouraged to develop codes of conduct for their own members (art 40), although codes of conduct must be monitored by a body which has been accredited by a competent supervisory authority which brings costs to associations or its members;

- According to HOTREC's opinion, HOTREC National Associations are allowed to process the data of their contacts (e.g. old and new contacts of the databases), <u>even without explicit consent</u> (arts. 6/1/f) – legitimate interest of the controller + art. 9/2/d;

  In this sense, HOTREC is of the opinion that old and new contacts can be legally kept and do not need to be deleted;

  Nevertheless, HOTREC would also recommend national associations to prepare a general written statement/e-mail/newsletter article to be sent to all respective members to make sure that they agree that their data is processed and published, for instance, in the members site (if this is the case). If someone opposes, then the Association needs to follow the person's willingness without delay;

  Also, with regard to new contacts, if Associations are able to put in place an automatic procedure for contacts to provide consent before being part of the data base, this would

be even better – in accordance with art. 6/1/a + 7;

- With regard to future members of Associations (prospect members), HOTREC believes that their data can be kept, even if there is no explicit consent, as it is the legitimate interest of the Association to do so (again: 6/1/f). But of course, it would be recommendable to ask the prospect member to provide consent for the data to be kept;

- HOTREC recommends national Associations to check with an IT specialist whether all systems and software are complying with the General Data Protection Regulation. Members of national associations should probably be recommended to do the same;

- All data processed in the Associations needs to comply with the Regulation. All unstructured data needs to be sifted through (e.g. if a contact mentions that he/she does not want to receive a newsletter, but wishes to continue receiving information on other topics, the association should comply without undue delay to the person's wish);

  For this reason, is recommended that national associations, when sending newsletters/general e-mails, etc., allow the possibility to the user to choose not to receive those messages again (art. 15/1/e) – e.g. by using an unsubscribe option;

- Data Protection Officer; impact assessment and prior consultation are not mandatory for National Associations according to HOTREC's line of interpretation as explained before;

- HOTREC believes that internal contracts of an Association (e.g. contracts with employees) do not need to be updated – Art 6/1 f + 9/2/d;

Part IV – Checklist for all companies

- ✓ Appoint a person responsible for data protection issues in your company;
- ✓ Identify what personal data is processed in your company and why this data is processed;
- ✓ Make an assessment of what are the legal basis for the treatment of the processed information;
- ✓ How are you managing the rights of the data subject (e.g. client)?
- ✓ How are you registering all the processed information?
- ✓ What information shall you provide to your contacts / clients regarding the personal data that is being processed? Review and update information texts;
- ✓ Provide a routine for the managing of data breach incidents;
- ✓ Train your staff;
- ✓ Review and update contracts with external data processors.

Nota bene:

HOTREC would like to highlight that the current note is the result of HOTREC's interpretation of the Regulation.

The legislators left an ample room for interpretation on the matter, in an attempt to conciliate the interests of stakeholders and consumers.

HOTREC would recommend to all National Associations to contact their respective supervisory authorities at national level (e.g. privacy commission in Belgium) to obtain an interpretation of the Regulation that is favourable to the sector.

HOTREC also recommends to national associations to read the guidelines of the Working Group Party Article 29, which will continue being uploaded on a systematic basis (link).[18]

***

[18] The Working Group Party of Article 29 has an advisory status and acts independently. The reflection of the working group does not reflect the position of the European Commission.