ericsoft

GDPR

New software features introduced for European privacy legislation

Introduction

This guide summarizes all measures undertaken by Ericsoft to adjust the software to GDPR regulations (General data protection regulation) in force starting May 25th 2018.

The new legislation, by regulating the collection, storage, processing and sharing of personal data, wants to guarantee that this data is managed correctly and in full respect of data holders. GDPR is applied in all states of the European Union to protect the data of European citizens (even if this data is managed by companies that reside outside the EU). The regulation did not provide specific procedures on how to collect, manage and store data, but it is mandatory to follow the principles and guidelines introduced by the new regulation anytime a company handles personal data of its customers.

The present document specifies how **to configure the PMS** in accordance with GDPR based on **internal privacy policies undertaken by each property that uses the software together with a legal consultant. Please note that all companies must be advised by their own legal consultant.** For example, the data retention period (that needs to be configured within the PMS) has to be decided by the hotel or restaurant manager together with his consultant.

It is the responsibility of the software user, not of Ericsoft, to enable the parameters which allow the correct management of guests' data inside the PMS.

What are the responsibilities of hotel and restaurant managers?

The **hotel** or **restaurant manager** (*Data Controller*) is the one who manages guest data: **it is his responsibility to ensure confidentiality and act in compliance with GDPR by activating all parameters within the software that allow proper handling of guests' data.** Management must also be able to **demonstrate to have adopted all technical and organizational measures necessary** to be in line with the principles of the new regulation.

Below is a list of precautions that the software user should implement in order to be able to adapt to the legislation, **which are NOT Ericsoft's responsibility:**

1. Contact **a legal advisor or a privacy expert** for an analysis of the data that is managed within their company and the access granted to each operator to ensure security and control.
2. Entrust **the analysis of the IT infrastructure** (servers, computers, operating systems, antivirus, firewall, Cloud) to a **hardware technician or IT consultant** that guarantees the security of the company's computer system. For example, an operating system has to be constantly updated in order to be in line with GDPR regulations, otherwise the company may be subject to sanctions because it does not own a computer system compliant with legal standards.
3. Define together with the legal adviser the retention **period of guests' data** to be configured in the PMS.
4. Prepare **clear information sheets** and **consent requests** in line with GDPR in order to prove that an explicit consent from the data holder has been given.
5. Provide adequate **training to staff on GDPR** to ensure that management instructions are acknowledged and adopted by staff in all daily operations.

What are the responsibilities of the software producer?

Ericsoft is the *Data Processor*, the company providing the PMS, the tool with which data is collected and managed. **The legislation requires that software complies with the GDPR "by design" e "by default"**, meaning that in the development phase new standards and new regulations are taken into account. With **Version 2.1.1.0, Ericsoft is able to guarantee its customers the adequacy of its software to the principles and guidelines of GDPR.**

How much does the software adaptation to GDPR cost?

Adjustment to GDPR **for Ericsoft customers is free of charge.** Unlike other companies that sell additional modules to be compatible with GDPR, Ericsoft has fully embraced the principle of compatibility of the software " by design " and " by default " by adding necessary functionalities directly within the software.

How to proceed with the software update and the configuration of the GDPR compliant version

The **upgrade** to the GDPR compliant version can be done in either of two ways listed below, **remember that in BOTH cases the figures to be entered within the PMS to activate necessary configurations** (such as the data retention period) **must be defined by the software user with his privacy consultant.**

a. **Autonomously (without the intervention of Ericsoft)**
   The software update is available in the control panel (**version 2.1.1.0** and following releases) and includes specific parameters which, if configured, allow data processing in compliance with the law. **It is mandatory to make a backup copy of the database before proceeding with the update** (full procedure is described in the online manual portal.ericsoft.com in the section "**upgrade procedure**"). For any doubt, before proceeding, please contact our customer care department, dialling 0541 604894 (Extension 4). While the configuration of parameters that need to be activated within the software can be carried out by following the procedures contained in this guide (pag 5, 6, 7).

b. **Technically supported (with the technical intervention of Ericsoft)**
   Ericsoft offers a paid configuration service for customers that wish to be supported by the helpdesk during the software update process and the configuration of the necessary parameters (according to privacy policies adopted by each property together with his consultant). This Service has a cost of **150 euro** (excluding VAT) and has to be **scheduled with our helpdesk department.**

Below are listed the new parameters that have been introduced by Ericsoft which, if configured, allow to make the software compatible with GDPR. For simplicity, the term "company" will be used to indicate the hotel or restaurant using the software. Some examples are related specifically to hotel guest data treatment while others, more in general, refer to data storage and email marketing activities.

1.Acquisition of customer data

1.1. Data required to make a reservation

Each guest to stay in a property (hotel, B&B, apartment, etc) must be able to provide consent for sensitive data treatment according to GDPR legislation (regardless of the method used to make the reservation). The acquisition of customer data by a restaurant, instead takes place when the guest requests an invoice. In this case, in order to obtain the fiscal document, the customer has to receive a copy of the privacy treatment terms according to GDPR legislation. In both cases the guest can't, by law, refuse to accept data processing.

1.2. Consent to send marketing communications (if the company use the CRM module)

While requesting consent for data treatment (necessary for the reservation or to issue an invoice) the company may also ask for guests' consent to receive promotional emails. In the PMS, based on customer's will, the "authorizes marketing communications" flag can be enabled and the system will automatically record the date/time the consent was given.

- **Positive consent:** the customer will receive promotional emails from the hotel or restaurant;
- **Negative consent:** in addition to not being able to send marketing communications to the customer, the software will maintain only the data necessary to fulfil law obligations. In the case of hotel reservation, all sensitive data will be cancelled at guest's check out, if the property has pre-configured this automatic operation in the PMS. In order to set this process as automatic, the "cancellation at check out" flag needs to be enabled.

1.3. Withdrawal of consent to marketing communications (if the company uses the CRM module)

End of consent may take place if:

- The guest, during his next stay in the property, decides not to renew the consent previously expressed (in case of a hotel);
- The guest sends a communication to the company with which he exercises his right to no longer receive promotional emails.

In both cases listed above, in addition to not being able to send marketing communications to the customer, all sensitive data will be cancelled from existing reservations. Sensitive data means racial or ethnic origin, political views, religious or philosophical beliefs, trade union membership, biometric data which identify a person in a unique way, health information (allergies), sexual life or sexual orientation of the individual, information added in the profile notes (video notes, print notes, service notes), notes present in the reservation card and possible pictures.

2. Data Retention for tax records

Personal data retention for tax records, according to the Italian law, may be up to 10 years (please verify retention period required by your country).After this period the company no longer has a reason to store such data and data must be automatically anonymized from the PMS: all information that can identify a person in an unique way will be replaced by asterisks (in this way, information be maintained for statistical purposes, for example in the sales report).

To anonymize data automatically the following parameter shall be configured in the PMS:

- [V] Anonymize data after expiration of documents storage period for tax purposes (10 years).

3.Data Retention for email marketing activities
(if the company uses the CRM module)

As already indicated, the hotel or restaurant manager, together with his privacy advisor, will have to set in the PMS a maximum limit (for example 2/3 years) for which he will have the possibility to store his in his database customers information for promotional emails. After such period, the PMS will automatically remove the consent for email marketing.

To configure automatic data cancellation, you will need to set the following parameter:

- [V] Consider marketing authorisation expired after years: X.

New CRM functionalities for data retention

Using the Ericsoft CRM, you will be **able to extend the data retention period of information** within the database. This new functionality allows the company to **renew customer consent to email marketing activities automatically** and it's unique in its kind.

This is why we invite customers, which have not purchased the module yet, to integrate it to their PMS, not only for correct data management according to GDPR, but also as a tool that can positively contribute to marketing and sales activities.

In detail, the PMS will send an automatic email before the expiry date to the customer with a request to renew his consent to receive promotional email. The email will include a link (with limited validity) that leads to a website containing the privacy statement. In case of acceptance by the customer, the date of the new consent will be automatically updated in the PMS via a token associated with the customer profile.

4.Access to data visualization

4.1. Credit card visualization

Credit card data will be made visible within the software only if access passwords respect PCI Level 1° regulations (listed below). If the password does not comply with these requirements, card data will still be stored inside the database, but will not be visible to operators.

Below are the minimum password requirements for PCI compliance:

- Length of at least 7 characters
- Alphanumeric
- With uppercase and lowercase letters
- Must be changed at least every 90 days
- Cannot be equal to the previous 4 passwords used
- Can be mistaken a maximum of 6 times before incurring in a 30-minute suspension

4.2. Visualization and access to data

For greater protection, a "log" section may be activated in the PMS. Once the section is configured, all movements carried out by different operators in the PMS will be registered.

From this section you will be able to view the following operations:

- PMS Log-in or log-out
- Data insertion, modification and cancellation
- Prints and data export
- Search filters applied
- Search of a specific guest profile and visualization of information

In addition, it will be possible to configure different levels of access for operators to the PMS. Each member of the staff will have access only to guests' data related to their duties. At the hotel, for example, housekeeping staff will be able to view notes on guests' allergies but will not have access to other information such as name, nationality, etc…

5.Additional information

With the Ericsoft update will we be compliant with the new European privacy policy GDPR?

The software has been adapted to the legislation "by design" e "by default", as it allows to put in practice the new privacy rules thanks to the introduction of automatic operations that facilitate proper data management, but **without a configuration by the software user of these automatic processes, the software will not respect the new regulation.** The PMS user will have to ensure that GDPR principles are applied within his company, therefore we recommend that he contacts a legal adviser or a privacy expert (as previously stated).

What does the Ericsoft software guarantee?

The Ericsoft software ensures that consent policies, data handling, storage, anonymization and cancellation of customers profiles are managed automatically and in compliance with the new regulation.

Below is a list of some **automatic procedures** that have been added to the PMS in adaptation to GDPR:

- Anonymization of profiles after 10 years (tax records)
- Elimination of all sensitive data if customer did not provide consent to receive promotional emails
- Elimination of all sensitive data after the period configured (expressed in years)
- Elimination of all sensitive data from customer profiles if the customer withdrew his consent to data processing for marketing purposes
- Registration of staff operations in the PMS (data access, display and printing)
- Display of credit card data subject to a control of the password parameters in accordance to PCI Rules

How is data protection guaranteed within the database?

- **Version 4°**: the database is protected by a username and password and without this information it's impossible to access data. As a result, the software is already compatible in its design with the regulation.