Data protection for restaurateurs

Data Protection Officer: dpo@caspeco.se

CONTENTS

PROCESSING OF PERSONAL DATA 3
THINK OF IT AS ONLY BORROWING THE DATA 3
YOU ALSO NEED TO MAKE SURE THERE IS A LEGAL BASIS 3
FOR PROCESSING THE PERSONAL DATA 3
THE RELATIONSHIP BETWEEN CASPECO AND RESTAURANTS 4
MORE TO KNOW AS A RESTAURANT OWNER 5
PERSONAL DATA IN EMAILS AND ONLINE 5
PERSONAL DATA BREACH 5
DATA PROTECTION BY DEFAULT 5
ADMINISTRATIVE FINES 5
DATA PROTECTION OFFICER 5
CHECKLIST, DATA PROTECTION FOR RESTAURATEURS 5

The General Data Protection Regulation (GDPR) has applied since 25 May 2018. It can seem daunting, especially given the high "fines" a company can face if it does not comply with the GDPR. But essentially, the GDPR is about being in control of how personal data is processed and keeping your systems in good order.

PROCESSING OF PERSONAL DATA

If you have a customer register, a payroll or staff register, or if your company otherwise collects and/or stores personal data, i.e. names, personal identity numbers, email addresses, images or other information that makes it possible to identify a natural person – then you are processing personal data.

THINK OF IT AS ONLY BORROWING THE DATA

The basic idea is that you are only borrowing personal data from a person in order to fulfil a purpose in your business. Imagine that you borrow tableware from another restaurant to serve an extra-large dinner. You would probably:

- Only use the tableware for the dinner you borrowed it for
- Only borrow exactly as much tableware as you need
- Take extra care of the tableware so that it does not go missing or get broken
- Return it as soon as the dinner is over

You should think the same way when you process personal data in your business, whether it concerns your employees or your customers. Make sure the personal data is only used for the purpose for which you collected it, protect it from unauthorised access, stay in control of how and why it is used, inform people about what you do with their personal data, and give it back when you no longer need it.

YOU ALSO NEED TO MAKE SURE THERE IS A LEGAL BASIS

FOR PROCESSING THE PERSONAL DATA

- Performance of a contract can be used as the basis for, for example, processing your employees' personal data to pay salaries, keep time records and set up logins to the systems you use in your business.
- Legal obligation applies when there is a regulation that requires you to process the personal data. This basis can be used, for example, to withhold tax and report to the tax and social security authorities.
- Legitimate interest means balancing how important it is for your business to process the personal data against the person's privacy. You must therefore be able to objectively justify why your interest outweighs the person's privacy.
- Consent can be used to store information about guests' allergies or to deduct trade union fees directly from an employee's salary. The GDPR sets high requirements for how consent is obtained for it to be valid, so if you can base the processing on one of the other legal bases, that is preferable.

If the data concerns health (for example sick leave), race, ethnic origin, trade union membership, political opinions, sexual orientation or sex life, biometric and genetic data or religious beliefs (so-called sensitive personal data), special requirements apply, such as explicit consent or a legal basis in law. Higher IT security is also required.

You must therefore take control of how and when personal data is processed. For example, recording a person's sexual orientation, ethnic origin, certain health information or anything else that is not directly necessary to fulfil the employment contract in a register of the restaurant's employees is normally not compatible with the GDPR. The payroll office has no interest in knowing that Rickard is allergic to peanuts, and the maître d' has no interest in knowing that Rickard clocked in two minutes later than Emma.

When it comes to your guests, simply use common sense. There is no legal basis for noting that Rickard was stingy with the tip. On the other hand, it may be a good idea to note how many in the party are vegetarians or would like non-alcoholic options. When your customers book a table with you, you may process the guest's personal data for the table booking on the legal basis of legitimate interest.

If you want to send marketing emails to customers who have booked a table and thereby given you their email address, that is fine as long as you informed them that this would happen when they booked the table and gave their email address. It is therefore important to give correct and sufficient information to those who provide you with personal data, and the duty to inform applies to both your guests and your employees.

The person the data concerns has been given extended rights under the GDPR. Among other things, anyone in your systems (both guests and employees) has the right to request a copy of all the data you hold about them, and the data must be sent to the person within one month. For this to be practically possible, your systems need to be in good order so that you know where to find the data. In addition to the right to request a copy, the person can also exercise their "right to be forgotten", which in practice means that you must erase all data about them in your systems. However, the right to be forgotten does not override a law such as accounting legislation that requires you to keep the data, or a situation where the guest has an outstanding invoice to pay; in those cases you may keep the data to meet those requirements.

THE RELATIONSHIP BETWEEN CASPECO AND RESTAURANTS

When you use Caspeco's services in your restaurant business, you (the legal entity) are the controller and Caspeco is the processor. Even though Caspeco provides the time and payroll systems, booking systems, etc., the restaurant business is considered the controller, because ultimately it is the restaurant business that determines the purposes and means of the processing of personal data. You could have Rickard as an employee and Emma as a customer regardless of whether you use Caspeco or a competing system. The processor is the party that processes personal data on behalf of the controller, i.e. Caspeco only processes personal data for you on your instructions.

The GDPR places new requirements on processors, and Caspeco works actively to ensure that platforms and other processes that handle personal data comply with the Regulation. Among other things, there must be a written agreement between the controller and the processor, and both are responsible for ensuring that it exists. Caspeco therefore provides a data processing agreement which, among other things, sets out your role and Caspeco's role. Caspeco continuously monitors all subcontractors, i.e. sub-processors, and enters into sub-processing agreements with them. A sub-processor is bound by the same obligations as the processor has towards the controller. If a sub-processor fails to fulfil its obligations, the processor remains fully liable to the controller.

MORE TO KNOW AS A RESTAURANT OWNER

In addition to stricter requirements on the processor, the GDPR contains other rules that may be useful for you as a restaurant owner to know about.

PERSONAL DATA IN EMAILS AND ONLINE

The same rules apply to what is written about people in, for example, emails, on websites and in simple lists on a computer as to the processing of personal data in booking systems and customer registers. You therefore need a legal basis for the processing, must inform the people concerned and must keep records of your processing activities. This also applies, for example, when you publish pictures of employees.

PERSONAL DATA BREACH

If the restaurant suffers accidental or unlawful destruction, loss or alteration of, or unauthorised disclosure of or access to, personal data processed in the business, this must be reported to the supervisory authority (the data protection authority in your country) within 72 hours.

DATA PROTECTION BY DEFAULT

Processors and controllers must take appropriate measures to meet the requirements of the GDPR. Appropriate measures means weighing technical and organisational measures against the nature of the personal data, the scope of the processing and the risk to the individual from the processing.

ADMINISTRATIVE FINES

The supervisory authority has the right to impose an administrative fine on anyone who infringes the General Data Protection Regulation. The amount takes into account how serious the infringement is.

DATA PROTECTION OFFICER

The GDPR requires three types of organisations to appoint a so-called data protection officer, i.e. a role with special responsibility for data protection in the organisation. This is required for organisations that are public bodies or authorities, whose core activities require regular and systematic monitoring on a large scale, or whose core activities involve processing sensitive personal data (such as health, trade union membership or religion) or criminal convictions on a large scale.

CHECKLIST, DATA PROTECTION FOR RESTAURATEURS

1. Make sure you have a legal basis for processing personal data. Do not write offensive comments in the customer register, or comments that are not necessary for the purpose of the customer register.
2. Never collect more personal data than is necessary for the purpose. Distinguish between personal data that is collected because it is needed and personal data that is nice to have (need vs. nice). Only process the data you need!
3. Never keep personal data longer than is necessary for the purpose. What is necessary depends entirely on the purpose for which it is processed. Caspeco will help you set up routines for when certain personal data should be removed from the systems, but the responsibility still lies with the controller, i.e. you.
4. Keep a record of the processing carried out under your responsibility. Such a record must contain the following information:
    a. The name and contact details of the restaurant business (the controller).

   b. The purpose of the processing.
   c. A description of the categories of data subjects (employees, customers, contact persons, etc.) and of the categories of personal data (name, address details, telephone number, etc.).
   d. The categories of recipients (payroll office, partners, etc.) to whom the personal data has been or will be disclosed. This may, for example, be Caspeco.
   e. Where possible, the envisaged time limit for how long the data will be kept.
   f. Where applicable, transfers of personal data to a third country or an international organisation.
   g. Where possible, a general description of the technical and organisational security measures. This could, for example, be that the payroll office does not have access to certain data that HR has, and vice versa.
5. Implement and follow the organisational measures referred to in 4(g) above. Access controls are a simple way to protect personal data from unauthorised access. As a general rule, access to personal data should only be given to those who need it to do their job.
6. If the business intends to upload pictures or comments from satisfied employees or guests, do not forget to ask first!
7. Inform your employees and guests about how you process their personal data! For example, publish your privacy notice on your website and include it in the staff handbook.
8. Do you use AI features in Caspeco, such as Casper? Inform your employees about it and do not use the features to assess individual employees.