GDPR

Caspeco’s services

Data Protection Officer: dpo@caspeco.se

CONTENTS

1. GDPR – what is it? 2
1.1 Processing of personal data 3
1.2 Sensitive personal data 3
2. Caspeco's GDPR work 3
2.1 Background 3
2.2 GDPR – guide for restaurateurs 3
2.3 Data processing agreement 3
2.4 The relationship between you and Caspeco 4
2.5 Questions and answers 4
3. Time and Schedule 5
3.1 General 5
3.2 Measures taken 5
3.3 Questions and answers 6
4. Booking 7
4.1 General 8
4.2 Contact details 8
4.3 Measures to adapt to the GDPR 8
4.4 Questions and answers 9
4.5 Privacy policy 10
4.7 Booking system features, Cloud 12
5. Payroll administration 12
5.1 Caspeco's payroll system and the GDPR 13
5.2 Salary and other employee data 13
5.3 Measures taken 13
5.4 Questions and answers 13
6. Casper AI assistant 15
6.1 Questions and answers 16

1. GDPR – WHAT IS IT?

1.1 PROCESSING OF PERSONAL DATA

The General Data Protection Regulation (GDPR) replaced the Swedish Personal Data Act and entered into force on 25 May 2018. It can seem challenging, 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.

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.

1.2 SENSITIVE PERSONAL DATA

Sensitive personal data should not be recorded unless it can be justified why it must be recorded. The personal data considered sensitive under data protection legislation is listed below:

- Racial/ethnic origin
- Political opinions
- Religious/philosophical beliefs
- Trade union membership
- Health information
- Sex life
- Criminal offences / suspected offences
- Genetic data
- Biometric data for the purpose of uniquely identifying a natural person

2. CASPECO'S GDPR WORK

2.1 BACKGROUND

This document has been compiled based on the interpretations of the law we have been able to make together with lawyers, the Swedish Authority for Privacy Protection (IMY), the Swedish Tax Agency and other bodies. One challenge with the GDPR is that the regulation is complex and requires you to make your own assessments. Even though a fair amount of guidance and some case law has been published, the area of law is far from easily accessible. It is therefore a good idea to be careful in the considerations you make about what should and should not be stored. For more specific questions, we recommend that you contact the Swedish Authority for Privacy Protection (IMY).

2.2 GDPR – GUIDE FOR RESTAURATEURS

The guide that was sent to all restaurants can be found on our website.

2.3 DATA PROCESSING AGREEMENT

Under the GDPR, certain information must be included in an agreement between parties when one processes data on behalf of the other. This is usually called a data processing agreement (DPA).

Caspeco has included the terms required by the GDPR in its general terms and conditions. If you have questions about the data processing agreement, please contact us at dpo@caspeco.se.

2.3.1 NATURE AND PURPOSE OF THE AGREEMENT

The Processor provides certain agreed services to the Controller, which may include personnel administration tasks such as scheduling, payroll, or sales-promoting services such as bookings. The assignment means that the Processor processes personal data, including other information, on behalf of the Controller, and may also include additional services that the parties may agree on.

The purpose of the Data Processing Agreement is to ensure that the personal data handled under the assignment is processed in accordance with the provisions of applicable data protection legislation, which also includes the EU General Data Protection Regulation and any subsequent legislation that replaces or supplements it ("Data Protection Legislation"). In its capacity as processor, the Processor shall process personal data on behalf of the Controller ("the Processing") in accordance with the Data Processing Agreement and the service agreement, which constitute the Controller's instructions to the Processor.

2.4 THE RELATIONSHIP BETWEEN YOU AND CASPECO

When you use Caspeco's services in your 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 in accordance with your instructions.

The GDPR places 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, as mentioned above, there must be a written agreement (the Data Processing Agreement) between the controller and the processor. 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.

2.5 QUESTIONS AND ANSWERS

2.5.1 GDPR INFORMATION

QUESTION: Do you have any information about Caspeco's GDPR work?

ANSWER: Of course! As a business owner, you can find basic information in the guide on our website. See this link: https://caspeco.com/gdpr/. There you will find information about what is important to consider. Otherwise, there is a lot of information in this document, or you can contact our support via our website https://caspeco.com.

2.5.2 DATA PROCESSING AGREEMENT

QUESTION: We would like to set up a data processing agreement with you. How do we do that?

ANSWER: If you have signed an agreement with us, you will find the data processing terms required by the GDPR in the general terms and conditions. If you still have questions, you are welcome to email us at dpo@caspeco.se.

2.5.3 REMOVING DATA FOR EMPLOYEES WHO HAVE LEFT

QUESTION: What about people who have left? Do we need to remove their data?

ANSWER: It will need to be cleaned up on an ongoing basis. All non-payroll-related information such as phone numbers and addresses should be removed as soon as possible. In short, the Swedish Authority for Privacy Protection (IMY) states that personal data should be removed when the employee has left, but that certain documents must be kept if other laws require it. For example, payslips and income statements must always be kept for a longer period under the Swedish Accounting Act (usually 7 years). You can read more about examples of when personal data should be kept and removed here: https://www.imy.se/.

2.5.4 ARE CARD DETAILS STORED ONLINE?

QUESTION: I entered my card details when booking a table online, and noticed afterwards that the page is classified as “not secure”. Are my card details safe?

ANSWER: Even though the booking system itself is provided by Caspeco, this is about the restaurant’s website being insecure. Card details are not entered on the restaurant’s website; instead, payment redirects to a page provided by a payment service provider, which must follow strict security requirements set by the card companies.

3. TIME AND SCHEDULE

3.1 GENERAL

Caspeco is the processor for the company that buys our services, which means that we make it possible for our customers to comply with the GDPR. One important GDPR consideration is how you want to set up the time clock.

Do you want the staff ledger on the time clock to be open and available to everyone who uses it, or only to individual users? The staff ledger must be available if you receive a visit from the Swedish Tax Agency’s inspectors. If you choose to remove the staff ledger button from the time clock, you should therefore always have someone on site who can produce the staff ledger in the system. The Swedish Tax Agency’s requirements on staff ledgers mean, however, that the personal data must be included in the ledger.

It is important not to use free text or labels in the schedule that could be regarded as sensitive data. Another tip from us is for each company to have its own internal GDPR text describing how the company works with this. The document can be uploaded to the portal as an information text about how your company has chosen to store and share data.

3.2 MEASURES TAKEN

Caspeco has taken measures regarding the GDPR – we would rather show too little than too much to a user, and you can choose to adjust the user to see more. This lets you decide for yourself whether there is a purpose for person X to see person Y’s personal data. Under the GDPR, it is important that people only see the information they need to perform a task.

- We have chosen to limit how far back in time the standard user can see the schedule; they can only see who worked up to 3 months back in the schedule view. However, there is a permission that can be added so that a user can see more than that.
- The time clock's offline files are encrypted and can only be decrypted at the customer's request for troubleshooting purposes.
- Because sickness information is especially sensitive, we have chosen to hide all absences for employees. They can of course see their own absences but not their colleagues'. They can see that a person is absent, but not the type of absence.

There is nothing to prevent you from clearing old schedules or removing information from the schedule when it is no longer relevant. However, remember that the schedule is the basis for forecasting and for employees' pay. This is because, as an employer, you are required to schedule according to the employee's employment rate.

3.3 QUESTIONS AND ANSWERS

3.3.1 NAMES ON THE TIME CLOCK

QUESTION: I have a question about our time clock. It should not show names, and if the Swedish Tax Agency comes, surely they need a separate list with personal identity numbers anyway? Is this something we can remove ourselves?

ANSWER: We can certainly remove the live staff ledger from your time clock. Would you also like the staff ledger button to be removed from the time clock? That button is used to produce the ledger if the Swedish Tax Agency visits. However, it is available to everyone who clocks in. As a customer, you can decide how you want it; contact us and we will set it up to suit your needs.

3.3.2 KEEPING THE SCHEDULE

QUESTION: How long may the schedule be kept?

ANSWER: Unfortunately, there is no clear answer here. However, our recommendation is to configure the schedule so that it can only be viewed 3 months back in time, and not to assign the GDPR role to more than one user per company. The schedule is the basis under working hours legislation and may be needed several years later to resolve any compensation claims.

3.3.3 SENSITIVE DATA IN THE SCHEDULE

QUESTION: How should sensitive data in the schedule be handled?

ANSWER: The schedule has free text and labels that you need to be careful with, as they may contain sensitive data. The company should review what information is entered in free-text fields and make sure that only those who need it have access to scheduling and daily reconciliation.

3.3.4 AUTOMATIC CLEAN-UP

QUESTION: Why is the schedule not cleaned up automatically?

ANSWER: The obligation to delete data depends on many different factors, for example restaurants may have chosen different routines for deletion. It is therefore entirely up to the company to clean up the schedule if it wishes, but nothing is done automatically as that would increase the risk of errors. Please get in touch and we will show you which support functions are available for deletion.

3.3.5 PRINTING THE SCHEDULE BACK IN TIME

QUESTION: Will it be possible to see via a schedule printout how someone worked a year ago?

ANSWER: No, this is blocked just as in the schedule, and only the GDPR role will be able to use this.

3.3.6 DAILY RECONCILIATION BACK IN TIME

QUESTION: Will it be possible to see the daily reconciliation back in time?

ANSWER: Just as with the schedule, we hide the ability to see more than 3 months back in time. Only the GDPR role can see more than that.

3.3.7 INFORMATION TO EMPLOYEES

QUESTION: How do I inform my employees about the GDPR?

ANSWER: Caspeco's suggestion is that the company creates a document and uploads it to the portal for all employees, so that they can easily read how their personal data is used in the company.

3.3.8 PERSONAL IDENTITY NUMBERS IN THE OVERVIEW

QUESTION: Why are personal identity numbers visible in the system?

ANSWER: Certain permissions give access to personal identity numbers, which are needed to pay salaries. However, people with low-level permissions cannot see personal identity numbers.

3.3.9 PERSONAL DATA IN THE STAFF LEDGER

QUESTION: Why does the staff ledger show personal data? Everyone can access it.

ANSWER: As a customer, you can choose to turn this off on time clocks and for users if you wish. However, it must be easily accessible when the Swedish Tax Agency visits, so make sure there is always a user on site who can produce it in the system.

4. BOOKING

4.1 GENERAL

Caspeco provides a booking service that conveys information between the person booking (a guest via online booking) and service companies (for example restaurants), or between service companies, for example conference venues, and their customers.

In this sense, Caspeco is the processor, and the company that provides the final service (the service company) is the controller. As processor, Caspeco may not handle personal data in any way other than as instructed by the controller. Below are the measures that have been or are being taken in the booking system to adapt it to the GDPR. There are images and explanations of where in the system you can find features that may support your business. At the end of the document is the privacy policy that a guest booking online can read. As an addition to this text, you can add information specific to your business. The addition is placed at the end of the text.

4.2 CONTACT DETAILS

There is no exact time limit to rely on for how long contact details may be kept if the contact/guest has not agreed to it. The Regulation only states that data may not be kept longer than necessary for the purpose of the register. Not even Caspeco's lawyer, who is an expert in this area, can give an exact time limit. However, our pragmatic view is that the data needs to be kept at least as long as it is reasonable that a guest may come back with feedback on their visit. You must decide what this time limit is for you.

We have a semi-automatic function that makes it easy to "bulk anonymise" old/unused contacts, i.e. you press the button to carry out the anonymisation. In the contact register there is a button that only users with the highest permissions can access. The button is called "Anonymise contacts". If you click the button to anonymise contacts, the system will automatically anonymise contacts that are "old", have no future bookings and do not have the "Save details" checkbox ticked.

What the system counts as "old" and anonymises is controlled by a choice of number of months each time anonymisation is carried out.

If a guest makes a booking via Caspeco's online booking, for example from the restaurant's website, the guest can choose whether their contact details may be kept. When you (waiting staff, maître d', etc.) make a booking for a guest, you can tick this checkbox after asking the guest directly whether it is OK to keep the details after the booking. If instead you have built the guest-facing interface yourselves and the booking is made via Caspeco's booking API, we cannot check whether this choice is shown to the guest.

4.3 MEASURES TO ADAPT TO THE GDPR

- Anonymise contacts/guests (delete contact details)

  Function for bulk anonymisation of old contacts. Administer/Contacts. There is also an option to delete what has been written in free-text fields in bookings if there is information that does not need to/should not be kept. A contact can also be anonymised from their contact card. Administer/Contacts.

- Collect consent via online booking, e.g. for newsletters Under development

  Option to show a checkbox for this to the guest. It is then possible to export a list of only the contacts who ticked the checkbox.

- Handling of personal data in online booking

Default text from Caspeco. In the online booking, the controller can display information that a guest making a booking can see, describing how you specifically handle personal data (your contact details, how long you keep contact details after a booking, how to request a copy of their data, etc.). Default text from Caspeco is provided.

- Help texts for free-text fields in bookings

  Tooltips that give quick information about what counts as sensitive personal data and therefore requires consent to be stored.

- Copy of personal data (subject access)

  Option to create a complete copy of a contact's personal data from the contact card if the contact requests it. Personal data from the contact card and all booking data are included in this copy, including everything entered in the bookings' free-text fields.

4.4 QUESTIONS AND ANSWERS

4.4.1 KEEPING INFORMATION IN THE BOOKING SYSTEM

QUESTION: How long are customer details kept?

ANSWER: The Regulation only states that data may not be kept longer than necessary for the purpose of the register. Not even Caspeco's lawyer, who is an expert in this area, can give an exact time limit. However, our pragmatic view is that the data needs to be kept at least as long as it is reasonable that a guest may come back with feedback on their visit. However, Caspeco may not decide what this time limit is for you. For contact details to be kept, there must be a legal basis, and the purpose of the register must make it reasonable to keep them.

4.4.2 REMOVING INFORMATION FROM THE BOOKING SYSTEM

QUESTION: How do we remove contact details stored in our customer register?

ANSWER: Caspeco's booking service has a semi-automatic function (Business Control and Cloud) that makes it easy to "bulk anonymise" old/unused contacts, i.e. you press the button to carry out the anonymisation and decide how long contacts must have been inactive/unused to be anonymised.

In the contact register there is a button that only users with the highest permissions can access. The button is called "Anonymise contacts". If you click the button to anonymise contacts, the system will anonymise contacts that are "old", have no future bookings and do not have the "Save details" checkbox ticked. What the system counts as "old" contacts, and anonymises when you choose to do so, is controlled by a choice of number of months each time anonymisation is carried out. There is also an option to delete, at the same time, what has been written in selected free-text fields in bookings.

4.4.3 RIGHT TO ERASURE

QUESTION: Do customers who have used the booking system have the right to have their data erased?

ANSWER: Customers have the right to have their data erased. Unless there is a future booking that requires the data to be kept, this can be done for an individual contact from the contact card.

4.4.4 SUBJECT ACCESS REQUESTS

QUESTION: Can our customers request the information we have stored about them?

ANSWER: Yes. Under the General Data Protection Regulation, an individual has the right to request, free of charge, a copy of the information collected and to have any inaccuracies in that information corrected where necessary. If the customer wishes to request access to their information, they should contact the service company where the visit was booked. A subject access request must be answered within one month.

4.5 PRIVACY POLICY

4.5.1 TEXTS

A guest booking online can see the texts below by clicking the question mark on the contact details page.

- General

Caspeco provides a booking service that conveys information between the person booking (guest) and service companies (for example restaurants). In this sense, Caspeco is the processor, and the company that provides the final service (the service company) is the controller. As processor, Caspeco may not handle personal data in any way other than as instructed by the controller.

By using the booking service, you agree to the practices described in the privacy policy. If you do not accept the practices described in the privacy policy (for example what information you need to provide to make a booking), you should not use the booking service. In that case, contact the company that provides the requested service directly. Caspeco is in no way responsible for the quality of the service booked (e.g. a restaurant visit) and cannot be held liable for it.

- Identity and contact details of the controller.

Each service company may add its own information at the end of this policy, for example to clarify the identity and contact details of the controller, state how long contact information is kept before it is anonymised, and explain how you can get access to your information or have your contact information deleted.

If no information has been added, contact the service company for these details.

- What information is collected about you?

To make a booking through the booking service, you must provide certain information about yourself (Customer Data). For a regular table booking, this information currently is: first and last name, mobile phone number and email address.

Where card payment is required to complete a booking, the usual information for online card payments is collected. Card details are stored in a PCI-certified environment and cannot be seen in plain text by Caspeco or its staff.

- Cookies and collection of traffic data

Caspeco collects device information and measurements to compile statistics on the use of our services, in order to see flows and general patterns and to maintain and improve the booking service. This information includes, for example, which browsers and operating systems are used, screen size, etc. IP addresses are not stored. The information from you cannot be linked to your identity. Among other things, the information is used to analyse use of the service through third-party functions, for example Google Analytics. Google Analytics has been configured not to store your IP address.

- What is the information used for?

The contact information collected is used by the service company primarily to communicate (send) booking confirmations, reminders and similar information related to a booking. The purpose of the communication may be, for example, to confirm that a booking has been created, to allow you to edit the booking yourself, to allow the restaurant to send menu choices, to send payment requests if agreed, to remind you of the booking, and for follow-up, for example to improve the business based on your experience.

The service company is responsible for the personal data (the controller) and for how it is used.

- Legal basis for processing personal data

When you make a booking with the service company, you enter into an agreement with the service company to arrive on the booked day and time with the number of people you booked for. By entering your contact details and completing the booking, you accept this agreement.

Legal basis: performance of a contract

There is also a legitimate interest in sending booking confirmations, reminders and similar communications through various channels before the booking takes place, for example to confirm that you have a booking, allow you to edit the booking yourself, send menu choices, pay payment requests if agreed, remind you of the booking or similar, so that you get the best possible experience. A legitimate interest in processing personal data for bookings may also be that service companies can communicate follow-ups to find out what you thought of the experience (customer survey) in order to improve the business.

The recipient of the information you provide is the service company.

Legal basis: legitimate interest

- How long is the information kept?

Caspeco's booking service has a function that allows the service company to anonymise old "Contacts/Guests" and their contact information, unless there is a new future booking. This is because, under the GDPR, contact information may not be kept longer than necessary for the purpose. How long the contact information is kept before it is anonymised is managed by each service company. Each service company is responsible for stating this in any addition to this policy.

If you wish, you can request that your data be anonymised after your booking has taken place, provided there is no future booking.

If you have agreed to your data being kept for future bookings, it is kept until you choose otherwise.

- Access to your information

Under personal data legislation, you have the right to request, free of charge, a copy of the information collected about you and to have any inaccuracies in that information corrected. If you wish to request access to your information, contact the service company where the visit was booked. The service company's contact details are on the booking confirmation. To release the data, the service company needs you to verify your identity in an acceptable way. A subject access request must be answered within one month.

- Right to erasure

If you have agreed to contact information being kept for future bookings, it is kept until you choose otherwise.

You have the right to have your contact information deleted unless there is a future booking that requires the contact information to be kept.

To have your contact information deleted by a service company, contact the service company directly.

- Right to object

You have the right to object to the service company's processing of your contact information. Please specify which processing you object to.

You always have the right to object to direct marketing.

- Right to data portability

You have the right to receive the information you have provided to the service company in order to use it elsewhere (port it). However, this only applies to information provided on the basis of consent or required to perform a contract. Data processed on the basis of legitimate interest is not covered.

- Right to withdraw consent

You have the right to withdraw your consent, in which case you should contact the service company concerned directly.

- Reporting an infringement (complaints)

If you believe your contact details have been processed incorrectly, you should contact the service company as soon as possible so that this can be assessed and, if necessary, corrected. You can also lodge a complaint with the Swedish Authority for Privacy Protection (IMY).

4.6 BOOKING SYSTEM FEATURES, BUSINESS CONTROL

- Anonymise old contacts in Business Control

  Permission-controlled function for bulk anonymisation of old/unused contacts and free-text fields in bookings.

- Anonymise an individual contact from the contact card

  Search for and select the contact. Choose Edit details and then Anonymise.

- Help texts for free-text fields in Table booking

  Hover over the information icon for guidance on free-text information.

- Help texts for free-text fields in Table booking

  Hover over the information icon for guidance on free-text information.

4.7 BOOKING SYSTEM FEATURES, CLOUD

- Anonymise contacts in Cloud

  Permission-controlled function for bulk anonymisation of old/unused contacts and free-text fields in bookings.

- Anonymise an individual contact from the contact card
- Help text for free-text fields

5. PAYROLL ADMINISTRATION

5.1 CASPECO'S PAYROLL SYSTEM AND THE GDPR

5.1.1 GENERAL

Caspeco is the processor for the company that buys our services. This means that we make it possible for our customers to comply with the GDPR. We encourage our customers to:

- Be careful about the purposes for storing personal data.
- Review the permissions in the system. A user should not have access to more personal data than their role requires.
- Think about what is written about employees in the system's free-text fields.
- Give the GDPR permission in the system to one of your users, for example the person responsible for data protection in the company.

Questions you should, among other things, be able to answer if the Swedish Authority for Privacy Protection carries out an inspection:

- What data do you handle?
- What information do you disclose?
- How do you handle data subjects' rights?
- How do you ensure that the processing is lawful?
- Who is responsible for data protection matters?

5.2 SALARY AND OTHER EMPLOYEE DATA

Employment involves handling and storing a large amount of personal data, which may include sensitive personal data. Some data is needed to fulfil the employer's legal obligations, and some is needed to fulfil the contract between employer and employee. Other data is needed so that the employer can report information to authorities, such as reporting taxes and employer contributions. How long the data may be kept depends on what data it is and what it is used for.

5.3 MEASURES TAKEN

- We no longer send payslips by email, since the file contains personal data. Instead, we send an email with a link to the payslip, where the user logs in and can read their payslip safely and securely.
- We have added help texts in the system to underline the importance of being careful with personal data. These remind users not to write down sensitive personal data about employees.
- We have removed personal identity numbers for users who do not need to see them, and we automatically hide people who are no longer relevant for users without the GDPR role, for example people who have left.

5.4 QUESTIONS AND ANSWERS

5.4.1 REMOVING EMPLOYEES' PERSONAL DATA

QUESTION: How do I remove data about employees?

ANSWER: For most personal data about an employee with an active employment, there is support in law or regulation for keeping it.

5.4.2 AUTOMATIC REMOVAL OF EMPLOYEES' PERSONAL DATA

QUESTION: Is it possible to set up automatic removal of employees' personal data?

ANSWER: There will be no automatic removal of this data, as it may be needed in different contexts for different lengths of time. The company is responsible for removing the data that can be removed.

5.4.3 CHANGING EMPLOYMENT CONTRACTS

QUESTION: Will Caspeco add any standard text on the GDPR rules to employment contracts?

ANSWER: No, we will not. In the e-signing service, it is possible to edit the employment contracts and add appendices to them.

5.4.4 THE RIGHT TO BE FORGOTTEN

QUESTION: What applies if a former employee wants to be forgotten?

ANSWER: The right to be forgotten applies under certain specified conditions: if the data is no longer needed for the purposes for which it was collected or otherwise processed, if a data subject has withdrawn their consent to the processing or objects to the processing of personal data concerning them, or if the processing of their personal data otherwise does not comply with the General Data Protection Regulation. The right to be forgotten does not apply to data processed to perform the employment contract or processed on the basis of legal requirements.

5.4.5 SUBJECT ACCESS REQUEST

QUESTION: An employee wants all the information about them in the system. How do we do this?

ANSWER: The data subject can request a copy of their personal data. Examples of such data are name, personal identity number, address, holiday entitlement, notes, etc. Payroll transactions and other data processing needed in the payroll process are not included. The company can create the copy using the list and report functionality in each platform.

5.4.6 NEXT-OF-KIN CONTACT DETAILS

QUESTION: May contact details for next of kin be kept?

ANSWER: Yes, they may be kept during the employment based on a balancing of interests. If the employment ends, there is no longer a legal basis for keeping the data.

5.4.7 KEEPING JOB APPLICATIONS

QUESTION: May job applications be kept?

ANSWER: Applications that lead to employment are kept for the entire period of employment. Others should be deleted but may be kept for a shorter period to determine whether the recruitment gives rise to a dispute, for example discrimination. If a dispute arises, the documents may be kept for as long as the dispute is ongoing. If consent is given, the data may be kept for future needs, in which case the data must also be kept accurate and up to date.

5.4.8 HANDLING PAYSLIPS

QUESTION: Will we be able to send payslips by email?

ANSWER: An email is sent to the employee saying that there is a payslip to read. However, it does not contain any sensitive data. The payslip can be classified as sensitive personal information, and such information should never be handled via email.

5.4.9 HANDLING FREE TEXT IN THE PAYROLL SYSTEM

QUESTION: How should we approach notes about employees?

ANSWER: In general, no sensitive or particularly protected personal data should be recorded. All users should be extra careful when writing notes. Data in free-text fields should be factual, accurate and serve an important purpose. Note that employees have the right to request a copy of their personal data, and data in free-text fields will then also be included.

5.4.10 RESPONSIBILITY / DATA PROTECTION OFFICER

QUESTION: Who is responsible for data handling in my company?

ANSWER: Some companies have a legal obligation to appoint a data protection officer. In our systems, this person can be given the GDPR permission. The purpose is to make the company's GDPR work easier. Even if you are not formally required to appoint a data protection officer, the Swedish Authority for Privacy Protection recommends that you do so.

5.4.11 INFORMATION THAT CAN BE DELETED

QUESTION: What information can I delete directly for an employee without breaking current legislation?

ANSWER: After the employment has ended, contact and next-of-kin details can be deleted immediately. Most other data is data that may need to be stored, for example under the Swedish Accounting Act.

6. CASPER AI ASSISTANT

Casper is an AI assistant in Caspeco that helps you analyse and plan your business based on your data in Caspeco. As with Caspeco's other services, you are the controller and Caspeco is the processor, and the processing is covered by the data processing agreement. The terms for the AI features are available at caspeco.com/gdpr.

6.1 QUESTIONS AND ANSWERS

QUESTION: What information is used when I ask a question?

ANSWER: Your question and the data in Caspeco needed to answer it – and only data you have permission to see. Do not enter sensitive information about employees or guests in your questions.

QUESTION: Where is the data processed, and is it used to train AI models?

ANSWER: Casper runs in Microsoft Azure. Microsoft is a sub-processor and is included in the list of sub-processors, which shows where the processing takes place. Your data is not used to train AI models.

QUESTION: Is what I write in Casper saved?

ANSWER: Conversations are saved so that you can see your history and so that Caspeco can troubleshoot in support cases and improve our products.

QUESTION: May we use Casper to assess individual employees?

ANSWER: No. Casper is designed for analysing and planning the business, not for assessing individual employees. We recommend that you inform your employees that you use AI features in Caspeco.