

Data controller

November 2025

Memo on data controller

Max Matthiessen Insurance Brokers has, following a comprehensive assessment in dialogue with both our Swedish owners and corporate legal experts, determined that we will henceforth consider ourselves the data controller in relation to the handling of personal data for our clients and their employees. This decision is based on our overarching role and responsibility in the processing of such data, which is no longer considered appropriate under a data processing agreement.

Previously, under Deloitte, a data processing agreement was used to support their specific policy. However, we have concluded that this is not necessary under our current practice, where we operate independently responsible for the processing of personal data.

We are not a data processor because we do not process data solely on the client's instructions. As a pension broker, we make independent decisions about why and how data must be processed in order to deliver our services. We use the information for our own purposes, such as ensuring correct pension and health solutions, maintaining updated data and documentation, and fulfilling our obligations as an advisor.

Processing of Personal Data

As a pension broker, Max Matthiessen acts as the primary data controller for the processing of personal data, as we determine the purposes and means of the processing. Our responsibility includes collecting and storing sensitive personal information about clients' employees in our systems, as well as ensuring the transfer of accurate and updated information to pension providers. This is a central part of our service and our obligation as a broker, and includes information such as employee CPR numbers, salary details, and more. The purpose of this processing is to ensure that our clients and their employees receive the best possible pension and health solutions. The legal basis for our processing is primarily the contract with the client (GDPR Article 6(1)(b)) as well as our legitimate interest in providing advisory services and solutions that meet the client's needs (GDPR Article 6(1)(f)).

In accordance with our Privacy Notice, which can be found on Max Matthiessen's website, we comply with our obligations under the GDPR by ensuring that all personal data is processed securely and in accordance with applicable data protection rules. Our processes include:

- **Receiving information from the client:** The client enters employee information (e.g., CPR numbers, salary details, coverage, etc.) into our shared portal (DePoS).
- **Storage and updating:** We store and update the information in our systems to ensure correct administration and maintenance.
- **Disclosure:** The information is forwarded to pension and health providers so that data is updated and consistent across all parties.
- **Ongoing administration:** In cases of new hires, resignations, or changes in coverage, the information is updated, and we ensure that all necessary parties are informed.



We make independent decisions regarding which data must be processed, how it will be processed, and which tools will be used. The purpose of this processing is to deliver our core service as a broker, meaning that data is used to ensure correct pension arrangements, optimise solutions, and fulfil our advisory obligations to both clients and their employees.

Our responsibility goes beyond the client's purpose because:

1. **We process data for our own purposes:** We maintain information in order to provide ongoing advisory services, even if the client terminates the collaboration. This includes responsibilities related to documentation and compliance.
2. **We have control over the information:** Although the data initially comes from the client, we are responsible for storage, security, and disclosure.
3. **Data is retained according to internal rules:** We do not delete data solely at the client's request, as we must comply with legal requirements, audit requirements, and internal procedures.

Compliance with the Privacy Notice

Our Privacy Notice, available on our website, describes how we handle and protect personal data. We comply with the principles of the GDPR and ensure that data is processed in accordance with applicable legislation.

We have determined that we act as the data controller, and this decision has been made based on legal advice and an internal assessment. We will continue to optimise our processes and ensure transparency for both clients and supervisory authorities.

Protection of personal data

1. The Parties agree that, in relation to the personal data processed in connection with the Parties' performance of this Agreement regarding the Company's employees (Data Subjects), both Parties are considered separate and independent Controllers in accordance with the General Data Protection Regulation (GDPR). Neither Party shall be considered the other Party's Processor or Joint Controller.
2. Each Party is solely and fully responsible for ensuring that its processing of personal data in connection with this Agreement, including the legal basis for processing and any transfer of data, is compliant with GDPR, statutory laws and regulations, that may be enacted or amended from time to time.
3. If a Party (the "Breaching Party") fails to comply with its data protection obligations, causing the other Party (the "Indemnified Party") to incur costs, fines, or liability to Data Subjects (Article 82 GDPR), the Breaching Party shall indemnify the Indemnified Party for all such costs, fines, and liabilities.