



This Document Describes How Willis Towers Watson Handles the General Data Protection Regulation

Pursuant to the General Data Protection Regulation (GDPR), which came into effect on 25 May 2018, Willis Towers Watson is required to enter into a Data Processor Agreement with your company, which will regulate how we process the personal data that we receive from you.

Is Willis Towers Watson Data Controller or Data Processor?

If Willis Towers Watson – as part of our counselling services – receives personal data from you for the purpose of establishing insurance agreements or carrying out counselling in the event of claim, we are data processors, as we are processing the received data according to your instructions and interests.

When receiving personal data from you, we assume that you have the legal authority to pass on the personal data to us.

The Role of the Insurance Companies

The insurance companies are not data processors on behalf of you as a client. The insurance companies process the received personal data to deliver an independent service to you and will therefore be considered **data controllers** of the personal data, they receive from you.

Your company and the insurance company are two independent parties entering into an agreement on insurance. Therefore, you submit personal data to the insurance company – possibly through Willis Towers Watson – for the purpose of establishing and fulfilling the agreement. The data is being used for a new and “independent” purpose, namely the conclusion of an insurance agreement on terms set out by the insurance company.

Therefore, it is not necessary for your company to enter into a Data Processing Agreement with the specific insurance company.

Establishing the Data Processing Agreement

Willis Towers Watson acts as a data processor in relation to you and therefore we must enter into a Data Processing Agreement. This agreement will be enclosed for your signature.



If you have any questions concerning the Data Processing Agreement you are welcome to contact:

Assistant General Counsel, Anne Patricia Rehlsdorph (Data Protection Officer)

E-mail: AnnePatricia.Rehlsdorph@WillisTowersWatson.com

Phone: +45 88 13 97 37

Legal Consultant, Nikolaj Simonsen

E-mail: Nikolaj.Simonsen@WillisTowersWatson.com

Phone: +45 88 13 98 90

Please note that you are required to ensure that you have the legal authority to pass on personal data to us. We will not verify that this authority is in place.

The rights of Data Subjects and their Request for Access

The General Data Protection Regulation provides the data subject (the individual) with a number of specific rights.

We have enclosed an information letter for the data subjects, explaining how we process their personal data and the rights the subjects have in relation hereto, including how to send a request for access, rectification and erasure.

You are welcome to hand out the information letter to the employees, whose personal data we will be receiving from you. Willis Towers Watson will be responsible for sending the information letter to those of your employees with whom we have direct contact.

Secure Communication

It is important that communication is secure and in compliance with industry standards, when we exchange personal data between Willis Towers Watson and your company.

We currently have two different options for exchanging information with you via secure connections, e-Boks and encrypted e-mail:



1. Communication via e-Boks

e-Boks is a secure communication solution that can be used by companies as well as private individuals. This requires that your company has signed up to the e-Boks solution and configured a permission to receive mail from Willis Towers Watson.

2. Use of Encrypted E-Mail

a. TLS Encryption

Transport Layer Security (TLS) is a protocol providing security and data integrity between two communication applications. TLS is the most widely used security protocol today. Willis Towers Watson uses TLS 1.2.

Willis Towers Watson sends all e-mails via TLS as standard procedure. All e-mails will be sent securely via TLS if the recipient's e-mail system supports this. If the recipient's e-mail system does not support TLS, e-mails will be sent without TLS encryption via general e-mail.

The same is applicable if you send TLS encrypted e-mails to Willis Towers Watson. We will receive them securely, as Willis Towers Watson's e-mail system supports TLS encryption by default.

It is possible to establish a permanent TLS tunnel between Willis Towers Watson and your company, ensuring that the TLS encryption is always being used. A permanent solution requires technical information and configuration at your end and ours. Our IT Support can assist you if you are interested in this solution.

b. Certificate-Based Encryption

Alternatively, Willis Towers Watson offers certificate-based encryption between two mail boxes. Certificate-based encryption requires that the company is using NemID and has company certificates assigned to its employees. The certificate must be exchanged between the sender and the receiver companies/employees, and a configuration in Outlook is required.

Certificate-based encryption ensures that the e-mail sent is encrypted. Certificates can be found and downloaded here:

https://www.medarbejdersignatur.dk/produkter/nemid_medarbejdersignatur/information_om_nemid/sikker_e-mail/soeg_certifikat/

Secure Communication Between Willis Towers Watson and the Insurance and Pension Provider

We use secure communication solutions when exchanging personal data with the insurance and pension companies. We either use a private portal solution or encrypted e-mails to communicate with the insurance and pension companies.



Data Protection Policy

You can read more about our data protection policy on our website www.willis.dk and you are always welcome to contact us if you have any questions concerning our processing of personal data.

Best regards,

Anne Patricia Rehlsdorph

Assistant General Counsel, Partner