

# Data Protection Policy

Willis Towers Watson I/S



May 2018

# Content

1.	<b>Introduction.....</b>	<b>3</b>
2.	<b>Accountability.....</b>	<b>3</b>
3.	<b>Whom Does the Data Protection Policy Concern? .....</b>	<b>4</b>
4.	<b>Who Is Responsible for this Policy? .....</b>	<b>4</b>
5.	<b>Personal Data.....</b>	<b>4</b>
6.	<b>Basic Principles for the Processing of Personal Data .....</b>	<b>5</b>
7.	<b>Legal basis for Data Processing.....</b>	<b>5</b>
8.	<b>Transparency.....</b>	<b>7</b>
9.	<b>Rights of the Persons on Whom We Process Data .....</b>	<b>7</b>
10.	<b>Integrity and Confidentiality .....</b>	<b>8</b>
11.	<b>Personal Data Safety.....</b>	<b>9</b>
12.	<b>Reporting Breach on Personal Data Security .....</b>	<b>9</b>
13.	<b>Transfer to Countries Outside the EEA .....</b>	<b>9</b>
14.	<b>Data Controller and Data Processor .....</b>	<b>10</b>
15.	<b>Data Processors .....</b>	<b>11</b>
16.	<b>When We Are the Data Processor .....</b>	<b>11</b>
17.	<b>Training and Information .....</b>	<b>11</b>
18.	<b>Policy Changes.....</b>	<b>11</b>

## 1. Introduction

- 1.1 This data protection policy defines the overall principles for how we collect and process personal data at Willis Towers Watson I/S (hereinafter 'we', 'us', and 'our').
- 1.2 We take the protection of personal data on our customers, our customers' employees, our own employees, as well as other persons, with whom we have relations, seriously. Those who submit their personal data to us, should be confident that we take care of their data, and that we adhere to all current legislation on the processing of personal data.
- 1.3 If we do not fulfil this obligation, it will hurt not only those about whom we process data, but also our and the insurance broker industry's credibility, brand value, and thereby esteem and business opportunities.
- 1.4 To add to this, repeated breach of personal data rules is punishable with fines of up to 4 percent of our global turnover, or 20 million EUR.
- 1.5 It is therefore vital to Willis Towers Watson I/S that we, our management, and all our employees, suppliers, and collaboration partners, who process data on our behalf, familiarise themselves with and adhere to the guidelines in this policy.
- 1.6 Infringement and non-adherence to this data protection policy will be viewed as a significant breach of the company's and employees' obligations, and may result in disciplinary sanctions, including termination of employment.

## 2. Accountability

- 2.1 To Willis Towers Watson I/S, it is a basic requirement to always ensure that our processing of personal data takes place pursuant to the rules on personal data processing to which we are subject, including, but not limited to, the Data Protection Regulation (EU Regulation 2016/679) and the Data Protection Law (expected adopted 17 May 2018), hereinafter 'The Data Protection Legislation'.
- 2.2 We have set up our business and our business activities in such a way that we can adhere to the Data Protection Legislation, and at all times can demonstrate that our processing of personal data lives up to the Data Protection Legislation.
- 2.3 We prioritise personal data protection as one of our most significant values, and we incorporate data protection principles when planning, and as a standard for our business activities. This means that we limit our collection and processing of personal data to what is necessary, and that we have implemented suitable technical and organisational measures, which ensure that we only process the required personal data to each specific purpose, and that the data subjects' rights are protected ("Privacy by design and default").

### 3. Whom Does the Data Protection Policy Concern?

- 3.1 This policy concerns all our interested parties.
- 3.2 The data protection policy is an addition to other instructions and policies, which we have issued, including our IT safety policy and archiving policy, which establish the framework for our general IT and personal data security.

### 4. Who Is Responsible for this Policy?

- 4.1 This data protection policy has been drawn up and approved by the management and board at Willis Towers Watson I/S.
- 4.2 In order to strengthen our data protection organisation, we have pointed to the legal department as our department responsible for personal data, with the following areas of responsibility:
- Guide and assist our employees by answering queries regarding processing of personal data
  - Monitor our and our employees' adherence to this data protection policy as well as the data protection legislation in general
  - Contact point for all external queries regarding the processing of personal data - including from those persons whose data is being processed, as well as the Danish Data Protection Agency and other public authorities, who make sure that companies adhere to legislation
- 4.3 Updated contact information can be found on [www.website.willis.dk](http://www.website.willis.dk)

### 5. Personal Data

- 5.1 The guidelines in this data protection policy pertain to all personal data, which we collect and process. Personal data is any type of data about an identified or identifiable physical person.
- 5.2 The data protection policy pertains to all personal data
- 5.2.1 Regardless of whether the data is submitted by the person in question, or has been collected from other sources, including publicly available data,
  - 5.2.2 regardless in which form or media the personal data is stored, including as text, picture, sound, electronically or other way,
  - 5.2.3 regardless of whether the personal data relates to present or past customers, the customers' employees, our own employees, homepage users, persons connected to our suppliers or other business connections, as well as other people with whom we have relations or on whom we process data,
  - 5.2.4 regardless of whether we process the data as data controller or data processor.

## 6. Basic Principles for the Processing of Personal Data

- 6.1 Willis Towers Watson I/S and all the company's partners and employees must at all times live up to the following basic principles on the processing of personal data:
- 6.1.1 We only collect and process personal data when this is legal and fair, and always with the greatest amount of transparency for the person about whom we are processing data. We are open about the processing of personal data, which we carry out.
  - 6.1.2 We only collect and process personal data for specific and legitimate reasons. If we do not have a relevant purpose with a given piece of personal data, we do not collect it, or we delete it.
  - 6.1.3 Data, which we have collected, we do not subsequently process for purposes that are incompatible with the purpose of collection.
  - 6.1.4 We only collect and process data, which is required and relevant for the purposes for which we collect data. We strive to minimise the collection of data to the extent that is sufficient for the purpose.
  - 6.1.5 We strive to ensure that the personal data, which we collect, is correct, and to keep it up-to-date. If we identify that personal data is incorrect, we rectify it or delete it.
  - 6.1.6 We do not store personal data for longer time than needed. Once the purpose has been exhausted, and we no longer have a factual reason to continue to store the personal data, we delete it in a secure manner.
  - 6.1.7 We handle personal data in a secure manner, also internally, as well as against accidental loss, destruction, or damage.

## 7. Legal basis for Data Processing

- 7.1 The Data Protection Legislation requires that personal data solely is collected and processed if a reference can be made to a relevant provision in the Data Protection Legislation. If no reference can be made, collecting and processing are illegal.
- 7.2 With regard to the personal data, which we primarily collect and process in our company, the legal basis will most often be:
- 7.2.1 that the person in question through his/her voluntary, specific, informed, and unambiguous expression of will has given his/her consent to the processing
  - 7.2.2 that processing is necessary in order to enter into or fulfil a contract to which the person in question is a part
  - 7.2.3 that processing is necessary to adhere to a legal obligation, which we are subject to
  - 7.2.4 that processing is necessary to protect the vital interests of the person in question or of another physical person
  - 7.2.5 that processing is necessary to pursue a legitimate interest, unless the interests of the person in question take precedence



- 7.3 For some data categories, it is more complicated to find a relevant legal basis. These particular categories are personal data on race or ethnic origin, political, religious, or philosophical conviction, or labour union affiliation, as well as processing of genetic data, biometric data with purpose of unambiguously identifying a physical person, health data or data on a physical person's sexual relation or sexual orientation
- 7.4 Generally, we do not collect these categories of data.
- 7.5 However, in certain cases we may have a factual and relevant purpose with collecting data about a person's health or labour union affiliation. In those cases, we may only collect and process the data, if:
- 7.5.1 The person in question through his/her voluntary, specific, informed, and unambiguous expression of will has given his/her consent to the processing
  - 7.5.2 processing is necessary for us to fulfil our labour law, health law, and social law obligations, inasmuch that it has a legal basis in law or collective agreement
  - 7.5.3 processing is necessary to protect the vital interests of the person in question, or of another physical person, where the person physically or legally is not capable of giving consent
  - 7.5.4 processing is necessary to determine, raise, or defend legal claims
- 7.6 We only collect and process a person's CPR number, when:
- 7.6.1 it follows from law that we must or may process CPR numbers, e.g. to be able to submit mandatory reports to public authorities.
  - 7.6.2 the conditions for processing specific categories of personal data are fulfilled, cf. item 7.5
  - 7.6.3 the person in question has consented
- 7.7 It is paramount that no data is collected and processed if no reference can be made to a legal basis, as described above. In all cases of doubt, you must confer with the Legal Department prior to commencing the collection and/or processing.
- 7.8 With regard to ensuring that a submitted consent adheres to the legislation requirements, we have drafted a number of standard consent forms. In those cases, where a form has been drafted, it is mandatory to use the form. We are thorough in making sure that consent forms are filled in correctly.

## 8. Transparency

- 8.1 We strive to be as transparent as possible about our collection and processing of personal data. The persons about which we process data must know which data we process for which purposes. Information must be given, regardless of whether we receive the data from the person himself/herself or from other sources.
- 8.2 The Data Protection Legislation requires us to inform on:
  - 8.2.1 Who we are, and how we can be contacted
  - 8.2.2 The purposes of the processing for which we wish to collect personal data, as well as the legal basis on which we may carry out the processing (see item 7)
  - 8.2.3 Which categories of data we process
  - 8.2.4 Any recipients or categories of recipients of personal data
  - 8.2.5 Whether we intend to transfer personal data to a recipient outside the EEA - and if so on what basis.
- 8.3 In most cases there also needs to be given information on:
  - 8.3.1 How long we intend to process the personal data for
  - 8.3.2 What our legitimate interests are with the processing
  - 8.3.3 Which rights the person in question has (see item 9)
  - 8.3.4 Where we have the data from (when not collected from the individual), including whether the data is from publicly accessible sources
  - 8.3.5 Presence of automatic decisions (without human intervention)
- 8.4 This information must be given at the same time that the data is collected from the individual, and within a reasonable time frame when the data is collected from another source.
- 8.5 There are exceptions to the obligation to inform, but we only make use of these exceptions if so approved by the Personal Data Controller.
- 8.6 In order to ensure that we in a correct and comprehensive manner give the information required by law, we have drafted a number of standard information forms. In those cases, where a form has been drafted, it is mandatory to use the form.

## 9. Rights of the Persons on Whom We Process Data

- 9.1 Persons on whom we process data have a number of rights pursuant to the data protection legislation. These are, among other:
  - 9.1.1 The right to receive information regarding our collection and processing of personal data (see item 8)
  - 9.1.2 The right to gain insight into the personal data, which we process about the individual

- 9.1.3 The right to have incorrect personal data rectified by us
  - 9.1.4 The right to in certain situations have all or parts of their personal data deleted by us
  - 9.1.5 The right to under certain circumstances limit the processing to storage
  - 9.1.6 The right to have certain personal data, which the individual has given us himself/herself, handed over in a structured, commonly used, and machine-readable format, and to have this data transferred to another data controller.
  - 9.1.7 The right to object to our processing of personal data, including an unconditional right to object to the processing of personal data for the use of direct marketing.
  - 9.1.8 The right to revoke a given consent
  - 9.1.9 The right to submit a complaint to the Danish Data Protection Agency.
- 9.2 We will assist, facilitate, and support individuals in exercising their rights, and respond to queries without undue delay, at the latest one month upon receipt of the query. If we receive a query from a person about whom we are processing data, the person should be referred to [www.website.willis.dk](http://www.website.willis.dk), where a request for insight can be logged.

## 10. Integrity and Confidentiality

- 10.1 Everyone at Willis Towers Watson I/S is subject to confidentiality. The confidentiality also applies internally, and we do not share personal data with colleagues, also not informally, unless it is substantive, relevant, and necessary in order for us to carry out our tasks.
- 10.2 Allocated user names and passwords are personal and may not be shared with others. Employees may not help others access data, which they otherwise would not have access to.
- 10.3 No one may access or in other ways familiarise themselves with personal data, which the person does not need to carry out his/her tasks.
- 10.4 No one may process personal data in breach of a given instruction or in breach of this policy. Anyone who suspects that an instruction is in breach of the data protection legislation or this policy must inform the Person Data Controller or Compliance immediately.
- 10.5 Everyone is bound to protect personal data against falling into the hands of unauthorised persons, as well as against other unauthorised or illegal processing, and against accidental loss, destruction, and damage.
- 10.6 Documents and files with personal data are stored in our protected case management systems. Personal data is not saved locally on PC's, USB-sticks, or other mobile media, in inboxes, or on open common drives. Printed material is shredded in a secure manner.



## 11. Personal Data Safety

- 11.1 Personal data must be protected against falling in the hands of unauthorised persons, and against accidental loss, destruction, or damage.
- 11.2 We have implemented technical and organisational measures, which based on a risk assessment are suitable with regard to our processing activities and the types of personal data, which we store. We continuously test and evaluate these safety measures as required.
- 11.3 It is the responsibility of the employees to follow any instructions, which we give with regard to processing and protection of personal data, and to adhere to the policies and guidelines, we have drafted, including IT safety policy and archiving policy.
- 11.4 Upon identification or suspicion that personal data is not being subjected to the necessary safety measures, or that the indicated minimum requirements are not being upheld, our Personal Data Controller or Compliance must be contacted immediately.

## 12. Reporting Breach on Personal Data Security

- 12.1 We are obligated to report any breach on personal data security to the Danish Data Protection Agency at the latest 72 hours after the breach has come to our knowledge. Security breaches, where personal data has come in the hands of unauthorised persons, may have extensive consequences for the people involved. Therefore, we are also obligated to inform the persons concerned, when the breach carries a high risk for the security and rights of the persons involved.
- 12.2 A breach on personal data security is any incident that leads to accidental or illegal destruction, loss, change, unauthorised transfer of, or access to personal data, regardless of whether this concerns transmitted, stored, or in other way processed personal data.
- 12.3 Upon identification or suspicion that a breach on personal data security has taken place, employees are obligated to do what they can to stop or limit the breach and its consequences, and to immediately inform the Personal Data Controller about the breach. Upon identification or suspicion of breach, employees are obligated to in any way possible assist in stopping, reducing, or in other ways handle the breach and limit possible damage. Additionally, employees are obligated to be available to the Personal Data Controller and the contingency group, so that we may fulfil our obligations pursuant to the data protection legislation.

## 13. Transfer to Countries Outside the EEA

- 13.1 Transfer of personal data to countries outside the EEA, i.e. outside the EU member states, including Norway, Iceland, and Liechtenstein, requires a special basis for transfer. Transfer includes transfer to a data controller, transfer to a data processor, and the fact that somebody in a country outside the EEA can access the data.
- 13.2 We expect that we only exceptionally will need to transfer personal data to a country outside the EEA.

- 13.3 If exceptionally the need arises to transfer data to a country outside the EEA, we ensure that the required basis for transfer is in place, a basis that ensures that the transferred personal data also will be processed securely in the recipient country.
- 13.4 A basis of transfer can consist of a) an EU Commission assessment that the country in question has established a sufficiently high protection level, b) that the recipient is certified pursuant to EU US Privacy Shield (recipients in USA), or c) that an agreement has been entered into with the recipient regarding data protection, which has been approved by the EU Commission (EU Model Contract) or by another competent authority. Besides these cases, no information may be transferred to a country outside the EEA without the Data Controller's approval.

## 14. Data Controller and Data Processor

- 14.1 Our obligations pursuant to the data protection legislation vary, depending on whether we are acting in the role as data controller or data processor.
- 14.2 A data controller is the physical or legal person, etc., who decides for which purposes personal data may be processed, and how the personal data may be processed, including by whom the personal data may be processed.
- 14.3 A data processor is a physical or legal person, etc., who processes personal data on behalf of the data controller. As opposed to the data controller, the data processor neither decides how or for which purposes personal data may be processed.
- 14.4 When we as part of our services to our corporate customers process data on the customer's employees, including preparation of insurance analyses, preparation of tender material, consultations with the customer, and ongoing administration of the customer's insurance matters, it is our opinion that we most often will be regarded as the customer's data processor. In this situation, we solely act on instructions from our customers on whether to facilitate and manage the customer's insurance and pension engagements.
- 14.5 However, when we carry out independent and personal consultations with individual employees in the customer's company or with other personal customers, e.g. regarding coverage needs, beneficiaries, and supplemental contributions, and in case of claims handling, our role will most often be that of data controller, since we are acting as an independent consultant, and thereby neither upon instruction from the customer, nor from the individual insurance company. In this situation, it is our responsibility to ensure that there is sufficient legal basis in the data protection legislation for the processing of personal data, and it is our responsibility to ensure that the employee has received the information that he or she is due pursuant to the Regulation.

## 15. Data Processors

- 15.1 We only use data processors, who can issue the required guarantee that they will implement suitable technical and organisational measures to ensure that the personal data processing complies with the requirements in the data protection legislation and this policy.
- 15.2 Prior to entering into an agreement with a data processor, we will ask the data processor to explain the security measures that have been established, both at the data processor's and at the sub-data processors' end, and we will ensure that this is in compliance with the data protection legislation, and that the security measures are suitable with regard to the type of personal data and the nature of the processing activities.
- 15.3 A data processor's processing of personal data, for which we are responsible, must always be regulated by a written data processor agreement, which ensures that the data processor solely acts upon our instructions, will not make use of data for other purposes, and in general lives up to the requirements stipulated in the data protection legislation.

## 16. When We Are the Data Processor

- 16.1 When we are the data processor for our corporate customers or others, we ensure that we do not process personal data contrary to the customer's instructions, and we protect the customer's personal data as fervently, as we protect our own.
- 16.2 To ensure that our data processing takes place according to agreements, which live up to the requirements in the data protection legislation, we have drawn up a standard data processor agreement, which regulates our processing of the customer's personal data with regard to the delivery of our insurance broker services to the customer. This agreement must be used when entering into agreements with customers. Deviations or changes to the agreement, or other agreement forms, may only be accepted upon approval by the Legal Department.

## 17. Training and Information

- 17.1 We ensure that new employees receive information on and training in adhering to the data protection legislation and this policy. We regularly conduct training sessions and send information to all employees with the aim of refreshing their knowledge on personal data protection, inform about new rules and requirements, and share our common experiences on the processing of personal data, so that we continue to ensure that Willis Towers Watson I/S lives up to the requirements stipulated in the data protection legislation.

## 18. Policy Changes

- 18.1 We ensure that all changes to this policy are disseminated throughout the organisation, so that all employees at any given time are informed about the latest version of the policy.

## About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 40,000 employees serving more than 140 countries. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas – the dynamic formula that drives business performance. Together, we unlock potential. Learn more at [willistowerswatson.com](https://willistowerswatson.com).