

PRIVACY NOTICE

Privacy and the protection of your personal data is important to us, and we are committed to protecting the integrity, availability and confidentiality of your personal data. This Privacy Notice outlines your rights to privacy and our commitment to safeguarding personal data. It is meant to keep transparency about how your personal data is collected, used, disclosed, and shared, and in the meantime help you in control of your personal data, including accessing, correcting, and deleting your personal data.

This Privacy Notice applies to any processing by us of your personal information, including information provided by visitors on all our websites, as well as processing of your information as our current or potential customer, employees, cooperation partners, counterparties, etc. We strongly encourage you to familiarize yourself with this Privacy Notice.

Where any conflict between the requirements outlined in the KYC Forms and this Privacy Notice, this Notice shall take precedence and prevail.

Pursuant to [Regulation \(EU\) 2016/679](#) (hereinafter the “GDPR”) and [Act relating to the processing of personal data \(personopplysningsloven\)](#), Wilhelmsen Insurance Services AS (hereinafter the “WIS” or “we”) hereby inform data subjects (individual persons) that the personal data collected in performing professional services requested by the customer shall be processed in accordance with the provisions of the GDPR, other legal frameworks might be relevant to your personal data and/or privacy rights, and according to the following information. It is understood that it is the customer’s responsibility to inform the natural persons acting on their behalf about the personal data collecting and processing hereunder and seek their consent, where required.

1. Who is responsible for your personal data?

The Data Controller is WIS, organization number: 978 320 215, with registered office at Strandveien 20, Lysaker, Norway, being part of the Wilh. Wilhelmsen Holding ASA (hereinafter the “Wilhelmsen Group”). WIS shall act as an autonomous data processor in relation to the processing of third-party data subject’s personal data collected from the customer, or from the third-party data subjects or other third parties to fulfil our professional services, and, in particular, to enforce or defend any rights, whether in court or out-of-court, in pursuing the legitimate interest of the Controller.

Please note data privacy is a highly regulated complex domain with evolving legislation. We are consistently endeavoring to enhance our compliance with these laws, and we will update our processes, disclosures, and this Privacy Notice as these implementing rules are finalized.

WIS will be responsible for your personal data. We want to be transparent regarding the information we hold about you and we want to make sure it is accurately updated. If you would like to exercise any of your rights, or should you have any questions regarding the processing of your personal data, you can always contact us via the contact details given in section 9. If you would like to receive a copy of the personal information we hold about you, or a “data extract”, please contact our compliance team.

2. Why and on which legal basis do we use your personal data?

In this section we explain why we process your personal data and the legal basis for doing so. We only process your data based on your agreement and in accordance with the strict policies and procedures that we have contractually agreed to. Your consent or as permitted or required under applicable laws is always our priority before we collect and process your data. We don’t share your data with advertiser-supported services or mine it for any purposes, such as marketing research or advertising.

(1) Your personal data is processed to comply with our various legal and/or regulatory obligations.

Your personal data is processed where necessary to enable us to comply with the laws and/or regulations to which we are subject, including but not limited to insurance and insurance brokage regulations, anti-money laundering, accounting, and tax legislations, Norwegian Transparency Act, Norwegian Environmental Information Act, etc.

(2) We use your personal data to:

- monitor operations and transactions to manage, prevent and detect fraud;
- monitor and report risks (financial, credit, legal, compliance or reputational risks, operational risks etc.) that we and/or the Wilhelmsen Group could incur;
- record, in compliance with the laws and/or regulations to which we are subject, communications in any form, including voice, emails, chats, relating to, at the very least, transactions performed within the provision of services agreement relating, in particular receipt, transmission, execution and recording;
- fulfil our obligations to declare and register transactions with the competent authorities (judicial, criminal, etc);
- record transactions for accounting purposes;
- prevent, detect and report risks related to Corporate Social Responsibility and sustainable development;
- detect and prevent bribery and corruption;
- detect and manage suspicious agreements and transactions;
- exchange and report different operations, transactions or orders or reply to an official request from duly authorized local or foreign financial, tax, administrative, criminal or judicial authorities, arbitrators or mediators, law enforcement, state agencies or public bodies.

(3) We also process your personal data for anti-money laundering and countering of the financing of terrorism (AML/CTF) purposes.

As a part of the Wilhelmsen Group and for providing our professional services, we must have a robust system of AML/CTF in each our department, as well as an internal process for applying local, Norwegian, European, and international sanctions which may require the processing of your personal data primarily through our Know Your Customer (KYC) process (to identify you, verify your identity and screen your details against sanctions lists, prior to and in the course of our services).

In the context of this processing, we as your insurance broker and claims handler, are joint controllers with your insurers, other insurance brokers involved, and the Wilhelmsen Group.

(4) Your personal data is processed to fulfil our legitimate interest or that of a third party.

Where we base a processing activity on legitimate interest, we balance that interest against your interests and fundamental rights and freedoms to ensure that there is a fair balance between them. If you would like more information about the legitimate interest pursued by a processing activity, please contact us using the contact details provided in Section 9 below.

(5) In the course of our services as your insurance broker and claims handler, we process your personal data to:

- communicate with you in the context of services provided to our customers and counterparties.
- manage the risks to which we are exposed:
 - we keep evidence of, and sometimes record operations, transactions and communications when you interact with our employees (e.g. during first-time ID verification, via emails, or during video conferences);
 - we monitor transactions to manage, prevent and detect fraud including, where required by law, the establishment of a fraud list (which will include a list of fraudsters);
 - we manage legal claims and defend our position in the event of litigation.
- enhance cyber security and data leakage prevention measures, manage our websites and third-party platforms and services we used, and ensure business continuity.
- monitor compliance with our internal policies and procedures including but not limited to our code of conduct. This may include monitoring of email and chat communications when you interact with us.
- enhance the automation and efficiency of our operational processes and customer services.
- commercial purposes: to identify the products and services that could best meet our customers' needs, to create new offers based on trends arising from our web communication channels, to develop our commercial policy taking into account our customers' preferences.
- safety purposes: to prevent potential incidents and enhance our safety/emergency management.
- compliance and risk management purposes (e.g., AML/CTF);
- anti-fraud purposes.

(6) We use your personal data to send you commercial offers and business-related information and notifications by electronic means, post, and phone.

As an active member of our shipping community, we want to be able to offer our customers access to the full range of products and services that best meet their needs.

If you are identified as a contact or representative of a customer; or counterparty, and unless you object, we may send you offers by any means for our products and services and those of your insurer.

We will use reasonable endeavors to ensure that these offers relate to products or services that are relevant to our customers or prospective customers' activities.

We will only send you business material via electronic communications (such as e-mails) in accordance with Norwegian law.

(7) We may keep records of electronic communication.

We are required to detect and report any suspicious behavior may related to AML/CTF under Norwegian legislations.

All records storage will be done in accordance with applicable laws.

(8) Your personal data is processed if you have given your consent.

Personal data may be processed either by paper or by any other electronic instruments (including portable devices) or forms, according to logic strictly connected with the above purposes.

For some personal data processing activities, we will give you specific information and ask for your consent. You can withhold your consent or, if given, withdraw your consent at any time.

In particular, we ask for your consent to:

- KYC.

You may be asked for further consent to process or share your personal data where necessary.

(9) Sensitive Personal Information

Subject to your consent, and depending on our service agreement with you, we may collect, process, or disclose certain information that qualifies as "sensitive data" under certain applicable data privacy laws. Sensitive data is a subset of personal data.

You have the right to **limit the use or disclosure** of your sensitive data to certain types of activities, in accordance with certain applicable data privacy laws. Please note that we do not use or disclose your sensitive data for purposes other than what we described in this Privacy Notice, without your consent, or as permitted or required under applicable laws. So, we do not offer an ability to limit the use of sensitive data.

3. Who do we collect personal data from?

We may collect personal data directly from you as staff of our customers, counterparties, and their service providers in the context of our activities and services.

We sometimes collect data/information from below public sources:

- publications/databases made available by official authorities or third parties.
- websites of legal entities or business customers containing information that you have disclosed.
- public information such as that published in the press, social media, or in the database which is open to the general public.

We also collect personal data from:

- The Wilhelmsen Group and its affiliated entities.
- our business partners or our customers' business partners.
- fraud prevention agencies.

4. What personal data do we collect?

You will always be notified what personal data will be collected and its purpose of collecting during our service process. Please note we very seldom collect all below information; it is only examples for your reference.

The personal data will often include information relating to:

Type of information	Examples
Contact information, private or professional	Postal and e-mail address, phone number.
Identification information	Full name, valid original ID (e.g. valid passport, travel document, birth certificate, driver's license or other documents with a photo issued by public authorities), nationality, place and date of birth, gender, photograph.
Government and other official identification numbers	Social security number, passport number, tax identification number.
Employment information	Employer's details, affiliations.
Administration and settlement of the policy or a claim	Current or previous physical, mental or medical condition, health status, pregnancy, injury or disability information, medical diagnosis, medical procedures performed and treatment given, personal habits (for example, smoking or consumption of alcohol), prescription information, and medical history.
Other sensitive information (only applies on a case-by-case consideration)	Political opinions, religious or philosophical beliefs, information regarding legal procedures, frauds, crimes, criminal convictions, offences, fines or similar relevant for security measures, subject to compliance with the strict conditions set out in data protection regulations.
Photographs	Images (including photographs, pictures and other types of softcopies) created and presented in connection with your insurance or other business activities, including for identity verification, claims assessment, administration and settlement, claim disputes, or for other relevant purposes as permitted by law.
Interactions with us and customer contacts	E-mails, chats, calls, meetings, phone conversation, contact history, letters, information and online identifier, to the extent that they are personal data gathered during your interactions with us.
Financial information or other information relevant for risk assessment	Bank account number, or other financial account number and account details.
Information to detect, investigate or prevent crime, including fraud and money laundering	Information about previous dealings with policyholders and claimants with the intention of the detection, investigation, and prevention of insurance fraud (unclear insurance claims), money laundering and other criminal activities.
Information from Wilhelmsen's Whistleblowing Channels	Information received in whistleblowing reports and collected for investigating reports.

Please note that you are not required to provide any of the personal data that we request.

However, in those cases in which the processing is based on the performance of a contract, we require your information to be able to fulfil our obligations. If you do not provide your personal data and/or refusal to allow processing shall entail the risk that we and/or your insurer will not be able to establish or continue to provide you with our and/or their services.

5. Who do we share your personal data with and why?

As a main principle, we **DO NOT** sell, rent, distribute, share or otherwise make your personal information available to any third party for marketing purposes. Therefore, we do not offer customers a way to opt out of the sale of related personal information or limit the use of this personal data. Please note above “sell, rent, distribute, share” or similar action does not include when we disclose your personal data at your direction, or when otherwise permitted under law. In connection with the purposes described above, we sometimes need to share your personal information with third parties.

Such third parties may both be independent third party controllers (i.e. third parties that have their own purpose for handling your personal information, for example other insurers/reinsurers) or, data processors operating on behalf of us and for the abovementioned purposes only (for example service providers that allow us to administer your policy and provide our service to you or suppliers maintaining and supporting our IT systems).

We always take appropriate technical, physical, legal (data processing agreements) and organizational measures, which are consistent with applicable privacy and data security laws to protect your personal information. Any service providers are selected carefully and are required to use appropriate measures to protect the confidentiality and security of your personal information.

For example, we may, before storing personally identifiable information, anonymize or pseudonymize the information so that individuals cannot be identified solely based on the stored information.

Personal data may be made accessible, disclosed or communicated to the following persons, who shall be appointed by the Controller, depending on the cases, as processors or controllers:

(1) With your insurer/reinsurer and its contractors

According to your service agreement with us and your insurance contract with the insurer, we may, where necessary, and per your insurer’s request, share your personal data with your insurer and its contractors.

(2) With the Wilhelmsen Group’s entities

As a member of the Wilhelmsen Group, we work closely with the Group’s other companies worldwide. Your personal data may therefore be shared between Group entities, where necessary and under a duty of confidentiality, to:

- comply with our various legal and regulatory obligations described above.
- fulfil our contractual obligations or legitimate interests described above.
- conduct statistical studies and develop predictive and descriptive processes, including data automation, for business, security, compliance, risk management and anti-fraud purposes.

(3) With other recipients outside the Wilhelmsen Group

In order to fulfill the obligations described in this Privacy Notice, we may, where necessary, share your personal data with other data processors which perform services on our behalf (e.g. IT and cloud service providers, insurance brokers).

We may also, where we consider it necessary, share your personal data with other data controllers, as follows:

- banking and commercial partners, independent agents, intermediaries or brokers, financial/insurance institutions, counterparties with which we have a relationship if such transmission is required to allow us to provide you with the services and products or execute our contractual or legal obligations or process transactions (e.g., banks, correspondent banks, paying agents, exchange platforms, payment system operators, intermediaries).
- regulators and/or independent agencies, local or foreign financial, tax, administrative, criminal or judicial authorities, arbitrators or mediators, public authorities or institutions, to which we, or any member of the Wilhelmsen Group, are required to disclose pursuant to:
 - their request.
 - our defense, action or proceeding.
 - complying with a regulation or a recommendation issued from a competent authority addressed to us or any member of the Wilhelmsen Group.
- service providers or third-party payment providers, for the purposes of providing a payment initiation or account information service.
- certain regulated professions such as lawyers, notaries, or auditors particularly when needed under specific circumstances (litigation, audit, etc.) as well as to our insurers or to an actual or proposed purchaser of the companies or businesses of the Group.

You can obtain more details about sharing with recipients outside the Wilhelmsen Group by sending written request to our compliance team on wis.osl.compliance@wilhelmsen.com.

For your personal data gathered from our KYC Forms, they will not be disseminated by WIS. The KYC Forms will be stored and/or shared “as is”.

6. Where do we process and transfer your personal data?

Personal data collected by WIS may be stored and processed in your region, in Norway, the European Union (and Liechtenstein and Iceland), the United Kingdom, the United States, and in any other jurisdiction where WIS, the Wilhelmsen Group and its affiliates, subsidiaries or service providers operate facilities. It is primarily processed and stored within the territory of the European Union and the European Economic Area. Due to the global nature of our services and to technological solutions, for the purposes set out above, in certain cases we may transfer personal data to parties located in other countries.

The level of protection of your personal information in such countries might be lower than the regulation within the territory of the European Union and the European Economic Area provides for. Therefore, such transfers will only be performed subject to appropriate safeguards required by applicable data protection laws, meaning only to countries deemed to have an “adequate level of protection” (as set out on the [European Commission’s website](#)) or with the use of the

European Commission [standard contractual clauses](#) (SCC), the United Kingdom Government (as applicable), or binding corporate rules (BCR), to ensure your personal data will be safeguarded properly.

In the absence of an adequacy decision or an appropriate safeguard we may rely on a derogation applicable to the specific situation (e.g., if the transfer is necessary for the exercise or defense of legal claims).

We and the Wilhelmsen Group will also take appropriate technical and organizational measures against unauthorized or unlawful processing of your personal data and against accidental loss or destruction of, or damage to, your personal information in accordance with our internal security procedures.

We regularly check our security policies and procedures to ensure our systems and our service provider's systems secure and protected. Only the personnel of us, the service provider's personnel who need to process your personal information for the purposes mentioned have access to your personal information.

7. How long do we keep your personal data?

We will retain your personal data for the longer of:

- the period required by applicable law.
- such other period necessary for us to meet our operational obligations, such as: proper account maintenance, facilitating customer relationship management, and/or responding to claims handling, legal claims or regulatory requests.

Most personal data collected is kept for the duration of the contractual relationship with our customers plus a specified number of years after the end of the contractual relationship or as otherwise required by applicable law.

In general and unless there are special reasons for a longer retention period, your personal data will be stored for up to five (5) years after the contractual relationship with us has terminated or the single transaction conducted pursuant to requirements in [the Norwegian Act relating to Measures to Combat Money Laundering and Terrorist Financing \(hvitvaskingsloven\)](#), as amended.

Unnecessary or irrelevant personal data will be deleted, made anonymous or synthetic. The anonymized data or synthetic data may be used for statistical or other business legitimate purposes. As this data can no longer be associated with you and, as such, will not constitute personal data anymore. We reserve the right to retain and use such anonymous data or synthetic data.

We will keep your data for communication usage as long as you are our customer or as long as we have any kind of obligation towards you or any third party under our service agreement.

For the purposes of prevent, detect and investigate crime, establish and defend legal rights, we will keep part of the claims file may relate to the investigations and evidence as long as you are our customer or as long as we have any kind of obligation towards you or any third party under our service agreement. This period may vary depending on the type of services in question but is at least ten (10) years following the expiration of the insurance based on statutes of limitations.

We will keep the data for the purpose of processing payment and premium as long as necessary in order to comply with applicable bookkeeping legislation for a period of seven (7) years.

The procedures for deleting personal data comply with the Norwegian Accounting Act ([Regnskapsloven](#)), as amended, and other legislations as applicable.

If you would like further information on the period for which your personal data will be stored or the criteria used to determine that period please contact us at the information given under section 9 below.

8. How can you exercise your rights in the context of our personal data processing?

You have rights under, and in accordance with, applicable data protection law which allows you to exercise real control over your personal data.

You have the right to be informed of how we process your personal information. We do this through this Privacy Notice and by answering your questions.

You can request **access** to your personal data.

We will provide you with a copy of your personal data promptly upon request, together with information relating to its processing.

Your right of access to your personal data may, in some cases, be limited by applicable law and/or regulation. In this case, you must exercise your right of access with your data protection authority, which may request the data from us.

You can ask for the **correction** of your personal data.

Where you consider that your personal data is inaccurate or incomplete, you can request that we modify or complete such personal data. In some cases, you may be required to provide supporting documentation.

You can request the **deletion** of your personal data.

If you wish, you may request the deletion of your personal data, to the extent permitted by law.

You can **object** to the processing of your personal data or **request restricting** processing based on legitimate interests.

If you do not agree with a processing activity based on a legitimate interest, you can object to it, on grounds relating to your particular situation, by informing us precisely of the processing activity involved and the reasons for your objection. We will cease processing your personal data unless we can demonstrate compelling legitimate grounds for processing, which override the interest, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims.

An objection of processing or request restricting of processing may result in termination or halt of services.

You can **suspend** the use of your personal data.

If you query the accuracy of the personal data we use, we will review and/or verify the accuracy of such personal data. If you object to the processing of your personal data, we will review the basis of the processing. You may request that we suspend the processing of your personal data while we review your query or objection.

You can **withdraw** your consent.

If you have given your consent to the processing of your personal data, you can withdraw this consent at any time. Should you wish to withdraw your consent, please refer to Section 9 below.

You can request the **portability** of part of your personal data.

You may request a copy of the personal data that you have provided to us in a structured, commonly used and machine-readable format. Where technically feasible, you may request that we transmit this copy to a third party.

Please note that we will always verify your identity before enabling access to any personal data.

You have the **right to complain** to the relevant data protection authority.

If you think that we have processed your personal information in a manner that is not in accordance with data protection law, you may lodge a complaint with the Norwegian Data Protection Authority (Datatilsynet).

Please follow the links below:

In Norwegian www.datatilsynet.no

In English www.datatilsynet.no/en/

9. How to contact us?

We encourage you to contact us in the first instance to handle any of your complaints or concerns. If you wish to exercise the rights summarized in Section 8, or if you have any questions relating to our use of your personal data under this Privacy Notice, please find below information for your reference.

The Wilhelmsen Group
Data Protection Officer data.privacy@wilhelmsen.com

The Wilhelmsen Group
Privacy statement wilhelmsen.com/disclaimer/

WIS
Compliance team wis.osl.compliance@wilhelmsen.com

In some cases, you may be required to provide evidence of your identity.

10. How to follow the evolution of this Privacy Notice?

We are continuously working to better comply with applicable laws and legislations, and we will regularly review and update our internal processes, disclosures, and this Privacy Notice as these implementing rules are finalized.

We invite you to review the latest digital version of this document online, and we will inform you of any significant amendments through our standard communication channels.