Privacy Notice – Regulated Insurance and Compliance Processing (Extended Version)

This extended privacy notice is primarily intended for clients, counterparties and other data subjects involved in regulated insurance, claims handling and compliance-related processing.

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 client, 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 client 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. Where clients or counterparties provide personal data about their representatives or other individuals, we ask them to make this Notice available to those individuals and to ensure that they are entitled to provide the information. This does not remove WIS's own obligations to provide information or establish an appropriate legal basis for its processing. Where consent is required for a particular activity, it must be obtained from the relevant individual or a person legally authorized to act on their behalf.

1. Who is responsible for your personal data?

Wilhelmsen Insurance Services AS, organization number 978 320 215, with registered office at Strandveien 20, Lysaker, Norway, is part of Wilh. Wilhelmsen Holding ASA (the "Wilhelmsen Group").

WIS acts as a data controller where it determines the purposes and means of processing personal data, including processing for its own legal, regulatory and professional obligations. Depending on the particular activity, WIS may instead act as a processor on another controller's documented instructions, or as a joint controller where it jointly determines the purposes and means with another party. The applicable role is determined for the specific processing activity.

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 is responsible for fulfilling the data protection obligations applicable to its role in the relevant processing. 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 using the contact details provided below. 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?

We identify the applicable legal basis for each processing activity. Depending on the purpose and circumstances, we rely on:

- Legal obligations under Article 6(1)(c) GDPR, where processing is necessary to comply with an obligation applicable to WIS, including relevant AML, accounting and regulatory requirements.
- Legitimate interests under Article 6(1)(f) GDPR, where processing is necessary for activities such as administering business relationships, supporting insurance services, preventing fraud, protecting information and systems, or establishing, exercising or defending legal claims. We assess these interests against the rights and interests of the individuals concerned.
- Contractual necessity under Article 6(1)(b) GDPR, where processing is necessary for a contract with the individual concerned or for pre-contractual steps requested by that individual. A contract with an individual's employer or another legal entity does not, by itself, establish this legal basis for processing that individual's data.
- Consent under Article 6(1)(a) GDPR, for activities for which we separately request consent. Marketing or promotional communications require prior, explicit and separate written consent as described in subsection (6).

Where processing is required by law, withdrawal of consent does not remove that obligation. Processing based on legitimate interests remains subject to the applicable right to object. Special category data and data concerning criminal convictions or offences are subject to additional requirements, as described below.

We do not disclose personal data for third-party advertising or use it for behavioural advertising.

Classified as Internal - This content is proprietary information intended for employees and partners only.

(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/CFT/CPF) purposes.
As a part of the Wilhelmsen Group and for providing our professional services, we must have a robust system of AML/CFT/CPF 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 Client (KYC) process (to identify you, verify your identity and screen your details against sanctions lists, prior to and in the course of our services).
For KYC, AML/CFT/CPF and sanctions-related processing carried out to meet WIS's own obligations, WIS acts as a controller. Insurers, other intermediaries and Group entities may act as separate controllers for their own processing. Where WIS and another party jointly determine the purposes and means of a particular activity, we establish the respective joint-controller responsibilities and make the essence of that arrangement available to the individuals concerned. Sharing information or participating in the same insurance arrangement does not, by itself, establish joint controllership.

(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 at the end of this Notice.

(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 clients 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 client services.
- Commercial purposes: to identify the products and services that could best meet our clients' needs, to create new offers based on trends arising from our web communication channels, to develop our commercial policy taking into account our clients' preferences.
- Safety purposes: to prevent potential incidents and enhance our safety/emergency management.
- Compliance and risk management purposes (e.g., AML/CFT/CPF);
- Anti-fraud purposes.

(6) Business communications and restrictions on marketing.
WIS primarily provides services in a business-to-business context. We do not send marketing or promotional communications unless the client or intended recipient has separately given prior, explicit written consent covering those communications. An existing business relationship, designation as a business contact, or acceptance of our service terms or this Privacy Notice does not, by itself, constitute such consent.
Any consent must identify the nature and purpose of the communications and whether they concern WIS's services or those of another party. Where communications are addressed to an identifiable individual, the consent must cover that individual's receipt of them and satisfy applicable data protection requirements. Consent may be withdrawn at any time by contacting us. Refusal or withdrawal will not affect our insurance-related services.
Separately, we may send or relay service-related communications concerning a client's insurance arrangements, claims, premiums, payments or associated compliance requirements, including communications issued on the instructions of an insurer or bank involved in the relevant matter. These communications do not depend on consent to receive marketing or promotional material.

Classified as Internal - This content is proprietary information intended for employees and partners only.

The distinction depends on the actual purpose and content of the communication. Instructions from an insurer, bank or another party do not exempt marketing or promotional content from the separate written-consent requirement above. We do not engage in consumer advertising or behavioural profiling for marketing purposes.

If you receive a communication appearing to come from WIS that you believe is marketing or promotional material for which you have not given separate written consent, or if you are unsure about its nature, please contact us using the contact details in this Notice or another independently verified WIS contact.
Unexpected communications may involve impersonation, phishing or fraud. Until authenticity has been independently verified, do not provide business, confidential or personal information, disclose passwords or verification codes, make payments, or act on requests to change payment details. Do not use links or contact details contained in a suspicious message to verify it.

(7) We may keep records of electronic communication.
We are required to detect and report any suspicious behavior related to AML/CFT/CPF under applicable legislation.
All record storage will comply with relevant legal requirements.
Any monitoring or recording of communications is proportionate, risk-based, and primarily driven by regulatory requirements. It is not conducted for general surveillance purposes.

(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.
Where consent is not the applicable legal basis, withdrawal of consent will not affect processing carried out to comply with legal or regulatory obligations.
In particular, we may request your acknowledgement (e.g. confirmation of information provided) and, where applicable, your consent in connection with certain KYC-related information requests.
You may be asked for further consent to process or share your personal data where necessary.

(9) Special category data and criminal-offence information.
Where strictly necessary for a particular insurance, claims or compliance activity, we may process special categories of personal data, such as health information. Such processing requires both an appropriate legal basis under Article 6 GDPR and an applicable condition under Article 9 GDPR, such as explicit consent or necessity for the establishment, exercise or defense of legal claims, where relevant.
Information concerning criminal convictions and offences is subject to the separate requirements of Article 10 GDPR and applicable national law. A general business interest or inclusion in this Notice does not, by itself, authorize such processing.
We limit access, use and disclosure to what is necessary for the relevant purpose and apply additional safeguards appropriate to the information. Your rights remain available under applicable law, including rights to request access, correction, restriction or deletion where the relevant conditions are met. Where processing relies on consent, you may withdraw that consent at any time. We will explain any applicable legal restrictions when responding to a request.

(10) AI-assisted processing
We may use approved AI tools, including AI-enabled functions within our business systems, to assist with information retrieval, document comparison, summarization, drafting and analysis in insurance brokerage, claims support, KYC, compliance and internal administration.
Depending on the task, these tools may process relevant business contact details, correspondence, insurance or claims information, identification information and other data described in Section 4. Only information appropriate and necessary for the approved task may be used. Sensitive personal data is subject to additional assessment and safeguards before use.
AI is a means of supporting the purposes described in this Notice; its use does not itself create a new purpose or legal basis for processing. AI-generated summaries, assessments and inferences are subject to appropriate verification before they are relied upon in professional advice or material business decisions. WIS remains responsible for its services and the processing for which it acts as controller.
Where stored context or memory is used, it remains subject to applicable purpose, access and retention restrictions. Information relating to one client or matter is not automatically available for use in another.
Where an AI agent communicates directly with you on behalf of WIS, we will identify its AI role and provide a route to the responsible WIS function or person.
Where necessary to explain a particular processing activity, we will provide additional information before that processing begins.
We do not make decisions concerning individuals that are based solely on automated processing and produce legal or similarly significant effects. AI may assist an assessment, but relevant material decisions remain subject to meaningful review by an authorized person who can question, change or reject the AI-supported result. If we propose to introduce solely automated decisions of this kind, we will first assess the applicable requirements and provide the necessary information and safeguards before that processing begins.
The privacy and data protection rights of individuals, including client representatives, third parties and business partners, take precedence over convenience, efficiency or other benefits sought from AI use. The use of AI does not diminish those rights, alter their applicable protections or restrict their exercise. Where an AI use cannot meet those requirements, we will restrict, change or discontinue that use.

3. Who do we collect personal data from?

We may collect personal data directly from you as staff of our clients, 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 clients containing information that you have disclosed.

Classified as Internal - This content is proprietary information intended for employees and partners only.

- 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, including joint ventures where applicable.
- Our business partners or our clients' business partners.
- Other financial/insurance institutions.
- 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 email 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 or other addictive substances), 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 client contacts	Emails, 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 Whistleblowing Channels	Information received in whistleblowing reports and collected for investigating reports.

Whether you must provide personal data depends on the particular request. We will explain whether information is required by law, necessary for the relevant service or insurance arrangement, or optional, and the consequences of not providing it.

KYC information may be required both for WIS's own compliance obligations and for an insurer's customer due diligence requirements under applicable law and the insurance contract. Where incorporated into the relevant contract, Clause 2-18 of the Nordic Marine Insurance Plan, Version 2027, makes cover subject to satisfactory customer identification and assessment. It requires relevant information before inception and prompt provision of further information and updates during the insurance period.
Under that Clause, where information is unsatisfactory or missing, the insurer must notify the customer and/or assured and request additional information. If that information is not provided within fourteen days, the insurer may terminate the contract by giving fourteen days' notice, or shorter notice where required by law. The applicable policy wording and version govern the particular insurance.

Failure to provide necessary information may therefore prevent or delay placement, renewal, claims handling or other services, or lead to termination in accordance with applicable law and contractual terms. These requirements do not remove the obligation to protect personal data or establish an

Classified as Internal - This content is proprietary information intended for employees and partners only.

appropriate legal basis for its processing. Refusing optional processing, including promotional communications, does not by itself affect our insurance-related 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. We share personal data only to the extent necessary to perform the services agreed with our clients, including insurance placement, renewal and administration, premium and payment arrangements, claims handling and settlement, and related advisory services; to carry out necessary KYC, sanctions and other compliance checks; or to fulfil applicable legal and regulatory obligations or establish, exercise or defend legal claims. Any sharing is limited to the information and recipients necessary for the relevant purpose and remains subject to an appropriate legal basis, confidentiality obligations and applicable data protection safeguards. A service agreement does not, by itself, authorize unrelated use or disclosure of personal data.

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 therefor 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, finance, 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 Wilhelmsen Group.

Where approved AI functionality is provided through Group systems or external service providers, personal data may be processed by those providers and their authorized subprocessors as necessary to deliver the service. The provider's role, permitted use of the data, access, retention and processing locations are assessed for the relevant service.
Where a provider acts as our processor, its processing is subject to documented instructions and applicable data protection arrangements. As a general rule, personal data submitted through our AI use must not be used for purposes unrelated to the approved service, including training or improving general-purpose models for a provider's own purposes. Any exception requires the prior, explicit written consent of each individual whose personal data would be used, together with a separate assessment and approval by WIS Compliance before the use begins.

Any such consent must be freely given, specific and informed, identify the intended purpose and relevant provider, and be capable of withdrawal in accordance with applicable law. A client's or business partner's agreement does not by itself constitute consent on behalf of the individuals concerned. Written consent does not override applicable law, confidentiality obligations, Group restrictions or security requirements. International transfers remain subject to Section 6.

Classified as Internal - This content is proprietary information intended for employees and partners only.

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.

Personal data collected through our KYC Forms is used and shared only for the purposes and with the recipients described in this Notice, subject to applicable restrictions. Completed KYC Forms are stored and, where sharing is authorized, transmitted "as is", preserving the content supplied and any signatures. AI-generated content is not inserted into or substituted for the original completed form.

Where information is extracted, summarized or analyzed, including with approved AI assistance, the resulting records are maintained separately and remain traceable to their sources. Generated interpretations are not treated as statements made or confirmed by the individual unless separately verified. Any subsequent correction or updated form is recorded as a distinct, traceable version.

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

Personal data collected by WIS is primarily processed and stored within the European Union and the European Economic Area (EU/EEA), including Norway, Iceland and Liechtenstein. Due to the global nature of our services and the technological solutions we employ, personal data may also be processed in countries outside the EU/EEA, including Switzerland, the United Kingdom and the United States, where necessary for the purposes described in this Notice. The relevant locations depend on the insurers, counterparties, Group entities and service providers involved in the particular processing. Such processing and transfers are subject to applicable data protection laws.

The level of protection of personal data outside the EU/EEA may differ from that provided within the EU/EEA. Where we transfer personal data outside the EU/EEA, we rely on an applicable European Commission adequacy decision or appropriate safeguards, such as the European Commission's Standard Contractual Clauses (SCCs) or approved Binding Corporate Rules (BCRs) covering the relevant transfer. Where required, we assess the protection available in the destination country and apply supplementary measures. Where UK data protection law applies to a transfer, we use an applicable UK-recognized transfer mechanism where required.

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).

The transfer requirements described above also apply where personal data is processed through AI tools, including access by relevant service providers or their subprocessors outside the EU/EEA. Use of an approved AI tool or Group platform does not, by itself, establish that an international transfer is permitted.

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 review our security policies and procedures to protect personal data processed through our systems and those of our service providers. Access to personal data is limited to authorized WIS and service-provider personnel who need it for the purposes described in this Notice.

7. How long do we keep your personal data?

We retain personal data only for as long as necessary for the relevant purposes and applicable legal requirements.

These retention principles also apply to personal data contained in AI inputs, outputs, stored context or memory, and relevant activity logs. Working copies and stored context are retained only for as long as necessary for their approved purpose. Discontinuing an AI tool does not automatically require deletion of records that must be retained for legal obligations, material decision evidence, claims or investigations.

Necessary retained records are subject to restricted access and appropriate retention review. Information no longer required is deleted or otherwise disposed of securely, including through relevant service-provider arrangements. Where backup or technically immutable copies cannot be removed immediately, they remain protected and subject to the applicable expiry or deletion schedule.

Retention periods depend on the category of record, its purpose and applicable legal requirements. Different parts of the same client or claims file may therefore have different retention periods.

- **KYC and AML records**
  Where the Norwegian Anti-Money Laundering Act (hvitvaskingsloven) applies, Section 30 generally requires information and documents obtained or prepared for customer due diligence, ongoing monitoring, investigations and reporting to be retained for five (5) years after the business relationship ends or the relevant transaction is completed.
  Under Section 6-4 of the Anti-Money Laundering Regulations (hvitvaskingsforskriften), the retention period is ten (10) years where the relationship was subject to enhanced customer due diligence at its termination, or the relevant transaction was subject to enhanced due diligence. The Regulations allow a documented assessment of earlier deletion after five (5) years in specified circumstances. Other transaction records subject to the AML retention requirements are generally retained for five (5) years after the transaction.
  Personal data is deleted when the applicable AML retention period expires, unless a separate applicable requirement or lawful purpose justifies retaining the relevant information. Such retention is assessed separately and does not authorize indefinite preservation or unrelated reuse of the AML file.

Classified as Internal - This content is proprietary information intended for employees and partners only.

- **Accounting, premiums and payments**
  Under Section 13 of the Norwegian Bookkeeping Act (bokføringsloven), primary accounting records, including relevant accounting entries, supporting vouchers and required financial reporting, are generally retained for five (5) years after the end of the financial year. Certain supplementary records covered by that provision are retained for three (3) years and six (6) months after the end of the financial year. Specific statutory requirements or lawful retention orders may require longer periods for particular records.

- **Insurance, advisory and claims records**
  Insurance placement, advisory and claims records are retained for as long as necessary to administer the relevant arrangements and establish, exercise or defend legal claims. We assess the applicable periods under the Norwegian Limitation Act (foreldelsesloven), relevant insurance legislation, the governing law and contractual terms, including any applicable Nordic Marine Insurance Plan provisions. The assessment takes account of the relevant starting date, extensions or interruption of limitation periods, and unresolved claims or disputes. There is no single ten-year minimum applying to all such personal data.

- **Correspondence and promotional records**
  Business correspondence and contact information are retained for as long as necessary for the relevant relationship or another documented purpose. Promotional contact records are reviewed when consent is withdrawn. A limited suppression record may be retained to prevent further marketing.

- **Preservation and disposal**
  Relevant deletion is suspended where records must be preserved for an investigation, dispute, regulatory request or other applicable preservation requirement. The scope and duration are documented and reviewed; preservation does not authorize unrelated use.

Personal data no longer required is securely deleted or effectively anonymized. Pseudonymized data remains personal data. Synthetic data is not automatically anonymous: we assess whether individuals remain identifiable before treating the resulting dataset as outside data protection requirements. Creating synthetic data does not, by itself, justify retaining the original personal data.

We maintain a retention schedule identifying the applicable periods or criteria, their starting points and any justified extensions. Longer retention is limited to the records and purposes for which it is necessary.

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 using the contact details provided at the end of this Notice.

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.
You may request confirmation of whether we process your personal data, access to that data and the information about its processing required by applicable law.
We will promptly acknowledge receipt of your request, confirm the date it was received and indicate the expected response date. We will respond without undue delay and normally no later than one month after receiving the request. The acknowledgement does not restart or extend that period.
Where an extension is permitted and necessary because of the complexity or number of requests, we may extend the response period by up to two further months.
We will notify you of the extension and its reasons within one month of receiving your request.
Where we refuse or limit a request, we will explain the reasons to the extent permitted by law and inform you of the available complaint and judicial remedies.

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 processing based on legitimate interests.
Where we rely on legitimate interests, you may object on grounds relating to your particular situation. We will stop the processing unless we demonstrate compelling legitimate grounds that override your interests, rights and freedoms, or the processing is necessary for the establishment, exercise or defense of legal claims. You may also request restriction while we assess whether our grounds override yours.

You can request **restriction of processing**.
This right is not limited to processing based on legitimate interests. You may request restriction where the applicable legal conditions are met, including:

- While we verify the accuracy of personal data you dispute.
- Where processing is unlawful and you request restriction instead of deletion.
- Where we no longer need the data, but you require it for the establishment, exercise or defence of legal claims.
- While we assess whether our legitimate grounds override yours following an objection.

Classified as Internal - This content is proprietary information intended for employees and partners only.

During restriction, we may retain the data, but other processing is permitted only under the conditions allowed by applicable law. We will inform you before lifting a restriction.

You may **withdraw** your consent at any time, where consent is the applicable legal basis for the specific processing activity.
Withdrawal does not affect the lawfulness of processing carried out before consent was withdrawn. Where processing has a valid legal basis independent of consent, including an applicable legal obligation or necessity for the establishment, exercise or defense of legal claims, that processing may continue to the extent permitted by law.
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, where consent is the applicable legal basis, please contact us using the contact details provided at the end of this Notice.
Where you have separately consented in writing to marketing or promotional communications, you may withdraw that consent at any time, without giving reasons. We will stop sending the communications covered by that consent. Withdrawal does not affect our insurance-related services.

You can request the **portability** of part of your personal data.
Where processing is carried out by automated means and is based on consent or a contract with you, you may request the personal data you have provided to us in a structured, commonly used and machine-readable format. Where technically feasible, you may request direct transmission to another controller. This right is subject to applicable conditions and the rights and freedoms of others.

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 reach out to us directly to address any complaints or concerns you may have. If you would like to exercise the rights outlined in Section 8, have questions about our use of your personal data as described in this Privacy Notice, or seek information regarding our human rights impacts, please refer to the details provided below for your convenience.

The Wilhelmsen Group Data Protection Officer	data.privacy@wilhelmsen.com	The Wilhelmsen Group *Media Contacts*	www.wilhelmsen.com/media-news-and-events/
The Wilhelmsen Group *Privacy statement*	wilhelmsen.com/disclaimer/	The Wilhelmsen Group *Wilhelmsen whistleblowing channel*	www.wilhelmsen.com/about-wilhelmsen/wilhelmsen-group-compliance-channel/
WIS Compliance team	wis.osl.compliance@wilhelmsen.com	Information requests relating to human rights, decent working conditions, etc.	humanrights@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 legislation, and we will annually 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.

Classified as Internal - This content is proprietary information intended for employees and partners only.