



Privacy Statement W.A. Hienfeld BV

This Privacy Statement applies to W.A. Hienfeld Holding B.V. (hereinafter 'Hienfeld'), including W.A. Hienfeld B.V. and its affiliates.

On this page we inform you in a transparent way about the way in which we handle the personal data entrusted to us. Let's start by announcing that we are very careful with the processing of your personal data and will never share your data with others without your permission (unless your health is at risk and/or the laws & regulations oblige us to do so). We will only use your data for the purpose for which you have provided it to us.

What are personal data?

When you apply to us for insurance or submit a claim for damages, you disclose information about yourself to us. And if you visit our websites, we may collect personal data from you, such as your computer's IP address.

Personal data is all data that can be traced directly or indirectly to a natural person. This means that a piece of data is personal data as soon as it can be traced back to you.

When are we allowed to process personal data?

We only process your personal data if we have a legitimate reason to do so, which is stated in the law. We will only use your data for the following purposes:

1. To deliver our Products & Services to you

This is the case as soon as you have or want to enter into an agreement with us. In order to be able to advise you properly about your insurances or to assist your financial advisor to do so and to manage your insurances, we need your personal data.

2. In order to comply with a Legal obligation

Partly for your own safety, we are obliged to ask for your personal data in order to establish your identity.

For the execution of a number of products, we are obliged to share your data with the tax authorities.

In exceptional cases, we are obliged to provide your personal data to other parties such as regulators, the police, the judiciary or intelligence services.

3. For a Legitimate and shared Interest

We keep your details in our records so that we can see what products you have, so that we can respond quickly to your questions and be of service to you.

We also use your data to continuously improve our services and to match them even better to your personal situation.

Your interest is our interest and in order to look after your interests properly, we use your data:

o For marketing & communication activities

To draw your attention to products and services that suit your specific situation.

To draw up profiles based on analyses of the data in our administration in order to provide you with an even better service.

For contact, to keep you informed via our website, Apps, letters or e-mail.

o To resolve and prevent production disruptions

To provide you with an uninterrupted service, we train our staff and test in advance and afterwards in a shielded part of the production environment how to resolve and prevent potential disruptions.

We emphasise that the protected test environment is separate from our development environment. We never use your data in the development environment; we make sure this data is anonymised.

o To prevent fraud and abuse

We can exchange your data within Hienfeld, with other financial institutions or with external research agencies. In the event of a personal investigation in connection with an insurance policy, we will comply with the rules set out in the 'Code of Conduct for Personal Investigations'.

o In order to better assess risks

We process your data using statistical analysis in order to better assess risks and determine the prices of our products.

o For processing third party data

In some cases, we record information about persons other than our clients, such as injured parties, administrators, beneficiaries and people who have provided security for a client. We only do this to the extent necessary for the performance of the agreement with the client.

4. If you have given us consent to do so

If we want to use your data for something other than what we have collected it for (see 1 to 3), your consent is always required first. Consent will always be requested from you in advance. Have you given your consent and you want to undo it, then that is very easy to do, for example by clicking on a link at the bottom of an e-mail.

What personal data do we process about you?

You can apply for our products and services through an advisor, broker or intermediary and for some products and services you can use an online form on our website. We use the following data:

Personal data for the execution of the agreement

We get most personal information directly from you or your financial advisor. If you are insured with Hienfeld through your employer, we get your data from your employer or sometimes through a central database. If necessary in the execution of an agreement, we can also receive data from other insurers. We process the following data:

- General data such as your name, address, phone number, email address and date of birth.
- Data to identify you.
- Your account number to receive payments from you or to make payments to you.
- Financial data. In some cases we ask for this when you apply for insurance.
- Data that we need for a specific product, think of a license plate with a car insurance.
- For certain products, specifically when handling claims, we sometimes need your Social Security Number.
- For the risk assessment with non-life insurance we can ask if there is a criminal past.



Personal Health Information

For the acceptance or execution of insurance such as accidents, travel and liability as well as for the settlement of personal injury, we need information about your health. We receive this information from you, your employer or - with your consent - from a physician.

The processing of your medical records takes place under the responsibility of the medical advisor (physician). Medical records are only provided by the medical advisor to others within the company if they need the data for the execution of their work. In such a case, these other persons are subject to the same duty of confidentiality as the medical advisor by virtue of his or her medical professional confidentiality.

Additional information

Additional information refers to data that we have not received from you or your advisor, but that we obtain from other (public) sources. For example, the consultation of information to combat terrorism and money laundering. In some cases, we do this to assess a risk or to comply with our legal obligations.

In addition, we may, where necessary, verify data on social media (Facebook, LinkedIn, Instagram and Twitter) or other public sources, such as newspapers, when handling claims to prevent fraud.

Contact details

Are you a contact person working for insurance brokers, insurers, collection agencies and expertise bureaus? In that case we will process your contact details.

Digital services

Hienfeld digitizes its processes by developing Webpages, Apps and with Extranet we make digital portals (API) available to our relations.

Via your IP address, we record your data about your visit to our websites or apps. For example, which pages you visited or which search query you entered. With this we make the site work better and give you a personal experience. We do this by placing cookies.

o Message boards

On our website you can use public message boards. The information you share on these boards is publicly accessible. Hienfeld does not store or supervise this online communication. We are not responsible for incorrect use of the message board or possible damage resulting from its use.

o Business Travel App

Hienfeld cooperates with various international emergency centres for fast, reliable and effective help where it is needed. For example, the insured client receives a handy travel pass (the size of a credit card) with alarm and policy number. In addition, the Hienfeld Business Travel App is available to be better prepared for your trip.

In order for the Business Travel App to function properly, we collect your name, address, place of residence, policy number and location information (GPS). You can control the location tracker yourself through the settings of the App.

o Extranet

The purpose of the Extranet is to make a secure part of the Hienfeld company network available to our relations, brokers and intermediaries. In addition to application forms, we have the following portals:



SIX API

Via the so-called SIX platform, intermediaries can directly fill in an application for the Employer Liability Insurance, Travel and Abroad. Here the same data is collected as in the regular application process (see above).

API Mobile Guarantee (MG)

Via the so-called MG-platform, dealers can directly apply for warranty insurance. Here the same data is collected as in the regular application process (see above).

To whom do we disclose information about you?

We do not disclose personal or financial information about you unless the disclosure is necessary to conduct our services. We do not disclose any non-public personal or financial information about our clients or former clients except as permitted by law. That may mean that we will make disclosures to the following types of third parties without your consent: This can be the following parties:

- Our affiliated companies.
- Your agent or broker.
- Parties who perform a business, professional or insurance function for our company, including our reinsurance companies.
- Independent claims adjusters, appraisers, investigators, and attorneys who need the information to investigate, defend, or settle a claim involving you.
- Businesses that help us with dataprocessing.
- Businesses that conduct scientific research, including actuarial or underwriting studies.
- Other insurance companies, agents, or consumer reporting agencies as reasonably necessary in connection with any application, policy, or claim involving you.
- Insurance support organizations which are established to collect information for the purpose of detecting and preventing insurance crimes or fraudulent claims.
- Medical care institutions or medical professionals to verify coverage or conduct an audit of services.
- Insurance regulatory agencies in connection with the regulation of our business.
- Law enforcement or other governmental authorities to protect our legal interest or in cases of suspected fraud or illegal activities.
- Authorized persons as ordered by a subpoena, warrant, or other court order as required by law.
- Certificate holders or policyholders for the purpose of providing information regarding the status of an insurance transaction.
- Lienholders, mortgagees, lessors, or other persons shown on our records as having legal or beneficial interest in your policy.
- External (mostly Dutch) registers such as CIS, CRA, External Referral Register (ERR)*.
- The Social Security Administration.

* When assessing an application for insurance or in claim handling, we also use various sources such as the Centraal Informatie Systeem (CIS) Foundation, Credit Registration Agency, Chamber of Commerce and fraud registers including the Fraud Information System Holland (FISH). In this system all damage reports are recorded, as well as all driving cancellations, proven fraud cases, etc. With this we check if you are telling the truth when you apply for a new insurance and report that you have never had a claim before.



Cookies

Through our websites, cookies are placed by the U.S.-company Google, as part of the "Analytics" service. We use this service to track and get reports on how visitors use the website. Google may provide this information to third parties if Google is legally required to do so, or if third parties process the information on Google's behalf. We have no influence on this. We have not allowed Google to use the obtained analytics information for other Googleservices. The information Google collects is anonymized as much as possible. Your IP address is explicitly not given. The information is transferred to and stored by Google on servers in the United States. Google declares on its website that it uses the model contract clauses for the transfer of data outside the EEA.

(<https://www.google.com/policies/privacy/frameworks/>).

How do we treat your personal data?

Certified Security: ISO 27001

We spend a lot of time and attention on the security of our systems, applications and Apps and the personal data stored there in. We ensure that all data is both technically and organisationally secure and comply with the highest security standards. Hienfeld periodically has its security tested externally and has been officially ISO 27001 certified since 2022.

Supervision

- The Data Protection Authority (DPA) checks whether we comply with the AVG.
- The Dutch Consumer & Market Authority (ACM) supervises how we deal with cookies and (direct) marketing.
- The Dutch Central Bank (DNB), the European Central Bank (ECB) and the Dutch Authority for the Financial Markets (AFM) generally supervise the financial sector, including Hienfeld.
- At sector level, we follow the Code of Conduct for the Processing of Personal Data Insurers of the Dutch Association of Insurers (Verbond van Verzekeraars).
- We have a Data Protection Officer (DPO). The DPO is our internal supervisor who tests, advises and trains Hienfeld.

Signing of Non-Disclosure Agreements

All our employees have signed a non-disclosure agreement. We handle any data you entrust to us with care. Only authorized personnel may access and process your data.

We conclude Data Processor Agreements

With the parties to whom we outsource tasks - such as ICT - and who process your data exclusively for Hienfeld's processes, we conclude data (processor) agreements with which we protect your data outside the borders of Hienfeld.

We keep dataprocessing within the EEA

We see to it that your data will not be processed outside the European Union. Our servers and those of our suppliers are therefore not located outside the European Union.

NB: If we share data with a serviceprovider in a country outside the EU, we will - if necessary - make additional contractual arrangements under which an adequate level of protection applies so that the transfer of personal data can lawfully take place.

What are your rights?

As a client you have a number of rights concerning your personal data. These rights are explained below.



1. You have the right to access

This means that you can request what personal information we have registered about you and what we use it for.

2. You have the right to modification, deletion and limitation

You have the right to have your personal data adjusted if they are incorrect. You also have the right to have your personal data deleted if your personal data have been processed unlawfully, are no longer necessary for the purpose for which they were processed, or because you have withdrawn your consent and Hienfeld no longer has any other valid reason for processing your data. You also have the right to limitation of your personal data. This right means that you can indicate that your data may temporarily not be used. You can make use of this right if your personal data are incorrect, are processed unlawfully, are no longer necessary for the purpose for which they were collected or processed, or if you object to the processing and your objection is still being processed by us.

3. You have the right to transfer data

This means that in certain cases you have the right to ask us to transfer the personal data you have provided to us to yourself or another service provider.

4. You have the right to object

You may object to the processing of your personal data if we use your personal data for purposes other than those necessary for the performance of an agreement or necessary to comply with a legal obligation. We will carefully review your objection and stop processing your personal data if necessary.

Exercising your rights

Contact us by any ways provided at the end of this notice if you have questions about what information we may have on file. Tell us what information you would like to receive. Provide your complete name, address, date of birth, and all policy numbers issued to you by us. Certain types of information generally collected when evaluating claims or possible lawsuits need not be disclosed to you.

Within thirty business days of receipt, we will inform you in writing of the nature and substance of locatable, retrievable, and available recorded personal or financial information about you in our files. We will also identify the person or organizations to which we have disclosed this information within the past two years.

After you have reviewed the personal or financial information about you in our file, you can contact us if you believe it should be corrected, amended, or deleted. Tell us what you think is wrong and why. We will consider your request and within thirty business days, either change our files or advise you that we did not and the reason why.

If we do not make the changes, you will have the right to insert into our file a concise statement containing what you believe to be incorrect, relevant, or fair information and explaining why you believe the information to be improper. We will notify persons designated by you to whom we have previously disclosed information of the change or your statement. Subsequent disclosures we make will also include the change to your file or a copy of your statement.

How long do we retain your personal data?

We will retain the data for as long as we are required to by law and for as long as is necessary for the purpose for which we use the data. This may vary from product to product. We apply the following rules:



Insurance contracts

As long as you are a client with us, we keep your data. We also do this for some time if you no longer have a certain product from us. In that case we use the statutory retention period of seven years. After that, we only store the data for statistical purposes and for the purpose to settle complaints or legal claims. In that case, we keep the data in a closed archive (security area).

Claim settlements

As long as you are a client with us, we keep your data. This also applies if you are not a client and we process your personal data for such purposes as claim settlement. We delete the policy data seven years after termination of the agreement. We delete the claim data seven years after termination of the claim. In the case of personal injury, we retain data for a maximum of forty years after the claim has been settled. After the retention period, we only retain necessary data for statistical purposes.

Modification of this privacy statement

We may amend this privacy statement. We may do so in the event of new developments, for example if something changes in our business activities or in the law or jurisprudence.

We therefore recommend that you regularly review this privacy statement when visiting one of our websites. This text was last amended on March 2023.

Do you have any questions about this privacy statement? Or do you have complaints about how we handle your personal data? Then please contact the Privacy Office of Hienfeld. Send an e-mail to privacy@hienfeld.nl or a letter to:

W.A. Hienfeld Holding B.V.
with regard to the Privacy Office
P.O. Box 75133, 1070 AC Amsterdam
Telephone: +31 (0)20-5 469 469