

Privacy Policy.

INTRODUCTION

FIS is a privately owned company that provides tailored solutions for the insurance industry, government and corporate entities. These solutions range from:

- Investigation services
- Workers compensation claims and support services
- WHS consulting

FIS recognises and understands the importance of maintaining privacy over the information you provide to us, and that is provided by others. We take our responsibility seriously in ensuring that we comply with the:

- Privacy Act 1988
- Privacy Amendment (Enhancing Privacy Collection) Act 2012
- Australian Privacy Principles.

We are committed to protecting the privacy and security of all personal and sensitive information that we collect. Our Privacy Policy is in accordance with the content of private sector provisions of the Privacy Act 1988. We are bound by and comply with the Australian Privacy Principles.

OBJECTIVES

This Privacy Policy explains how FIS collects, uses, holds and discloses your confidential information and the choices you can make about your personal information.

The objectives of this policy are to:

- Identify FIS's obligations for handling personal information of past and present FIS clients and individual's involved, either directly or indirectly in FIS business engagements
- Encourage all FIS personnel to take a proactive privacy approach
- Identify FIS's obligations for responding to complaints about potential privacy breaches.

SCOPE

The principles in this Policy apply to FIS and its controlled entities, including:

- General Managers, Managers and other employees (whether full time, part time, casual, permanent or temporary); and
- Volunteers, contractors and consultants.

These personnel will be referred to as “staff” hereafter.

WHY WE COLLECT PERSONAL INFORMATION

To provide our services to the entity that engages us, we may collect personal and sensitive information from you, or about you, where reasonably necessary to do so.

Information is collected so we can fulfill our client requests and properly investigate matters referred to us by our clients, and subsequently provide them with facts, evidence and information they require to carry out their lawful functions.

Personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- Whether the information or opinion is true or not; and
- Whether the information or opinion is recorded in a material form.

Personal information relating to our clients and our service providers may be used to conduct research to ascertain a better understanding of our clients' needs, to provide information to our clients about our services, and to engage in other business development and marketing activities.

TYPES OF INFORMATION WE COLLECT

When conducting an investigation we may collect and hold the following types of personal information:

- Current and previous name, date of birth, gender and contact details
- Employment history and current employment details
- Underwriting information such as insurance claims history, criminal and traffic histories
- Financial information such as assets and liabilities and bank account details
- Sensitive information such as medical and health information and history, where this is relevant to the investigation of a claim or complaint
- Video or photographic footage of individuals and their activities.

We may also collect personal information from our service providers that are necessary to conduct our business and comply with our licensing and contractual obligations, including:

- Name, address, contact details and business / company details
- License details
- Work history and qualifications

HOW WE COLLECT INFORMATION

We may collect information about you or other individuals in a variety of ways, including, but not limited to:

- Directly from the individual via phone, post, facsimile, email or during an interview
- From our instructing clients of a claim or complaint
- From publicly available sources via the internet, including social media
- From third parties including witnesses, complainants and other parties involved in a claim or investigation, such as medical practitioners and rehabilitation providers
- From entities or people located overseas where that information is relevant to the claim or complaint under investigation
- By formal information requests to various government agencies and departments, such as the Police and other emergency services
- Information Technology service providers
- Service providers or consultants who we engage to conduct specialist tasks as part of our investigative functions, for example forensic accountants
- Investigators, family members or anyone you have authorized to deal with us on your behalf and either our or our legal advisor.

Where reasonable and practicable, we will collect personal information directly from the individuals themselves. Before commencing an interview or statement, our investigator will introduce him/her; explain clearly whom they represent and the reason for their inquiry. Investigators will seek the interviewee's consent to collect, use and disclose their personal information, and will record the person's consent in the statement or interview.

There may be circumstances where we may have to collect information from other sources or third parties. In any case, we will only use lawful and fair means to collect information.

If you ask FIS to provide you with any of our client tailored solutions, we will ask you to provide certain details, such as:

- Your full name
- Your business name (if applicable)
- Your position in the business (if applicable)
- Mailing address
- Phone and facsimile number
- Email address

FIS may also request certain information about you and the reason why you contacted us in order to assist with the selection of the most effective FIS service relevant to your needs.

Where FIS or FIS related entities use your personal information for activities such as, marketing or educational communications, you can choose to opt out at any time by directly notifying us.

We only collect information that is directly relevant to the purpose for which we are collecting it, as well as related purposes where the individual would reasonably expect us to. Personal and sensitive information is only used for the purpose of investigating claims or complaints that are referred to us for investigation, and is not disclosed to any unauthorised party, or used for any other purpose unless Huxley Hill is required by law to do so.

All Information that we collect is treated as strictly confidential and is generally only disclosed to the instructing client, or where authorised to their legal advisors.

We will only collect your personal and sensitive information if you have provided us with consent to do so, for the purpose for which it was provided to us and as permitted by law. A non-inclusive list of these purposes is:

- In response to your direct enquiries
- To fulfill the terms of engagement of our clients
- Quality assurance and training purposes
- Providing you with marketing information with regards to the full range of our services
- For the purposes of tenders, proposals, accreditation or business development activities
- Any other purposes identified at the time we collected your personal information.

ACCURACY OF YOUR INFORMATION

FIS will take all reasonable precautions to ensure that the personal information we collect is accurate, complete and up-to-date. If you discover or have reason to believe that that the personal information we hold about you is not accurate or complete or you wish to update your information, we will provide you with the opportunity to access the information we hold upon request in accordance with the Australian Privacy Principles.

We will ask you to provide reason why it is incorrect, incomplete and inaccurate. We will amend our records or make a notation of your submission, as relevant and appropriate.

You can request access to the personal or sensitive information we may hold about you. If you wish to make a request for access, you can contact us on 02 4981 5292 during business hours, or email us at service@fisgroup.biz.

We will take all reasonable steps to ensure that your personal information is corrected.

TRANSFER OF DATA OVERSEAS

We may disclose personal information to overseas entities, located in various countries, where necessary for the investigation of a claim or complaint. For example where we are instructed to investigate an incident that happened overseas we may disclose personal information to a service provider in that country so they can conduct local enquiries. The location of those overseas entities will vary depending on the circumstances of each case.

DATA SECURITY

FIS takes all reasonable steps to ensure that all personal information provided to us is securely held to minimize the risk of loss, unauthorized access, destruction, use, modification or disclosure.

FIS uses physical security measures and the latest information technology security to protect the information we hold, such as:

- Firewalls
- Passwords
- Data encryption
- Access card controlled commercial standard locked cabinets.

Access to and use of personal information within FIS is appropriately limited to prevent misuse or unlawful disclosure of the information.

FIS employees receive training on the Australian Privacy Principles. Employees and contractors engaged by FIS are contractually bound to comply with the Australian Privacy Principles and to keep confidential information secure.

We request our contractors to return information to FIS following each engagement. We securely destroy all information that we are not legislatively required or permitted to hold.

Where we disclose personal information to an overseas entity, our contractual arrangements with the service providers generally include an obligation for them to comply with the Australian Privacy laws.

We will retain your personal information for time periods in accordance with the legislation.

FIS employs secure methods to destroy your personal information when no longer required.

FIS employs industry leading security measures and takes every step to protect your personal and sensitive information; however no security measures are completely secure. We cannot 100% guarantee the security of your information, for example, due to illegal actions by others, including use of superior physical methods (illegal entry to FIS premises), interception of mail or due to transmissions over the internet which may be hacked.

FIS urges you to take great care when sending personal and sensitive information to us as well as retention by you of your information. Should you become aware or suspect that a security breach has occurred, please immediately contact us and the police.

COMPLAINTS PROCESS

If you believe FIS has handled your personal and sensitive information in a manner that is not consistent with the Australian Privacy Principles, you can submit a written complaint, with details of the complaint and alleged breach, together with any supporting evidence, to FIS at the following address:

Mr Jeremy Barnes
General Manager – Operations
Factual Investigation Services
PO Box 46, Salamander Bay NSW 2317

P: 0459 095 999
E: jeremy.barnes@fisgroup.biz

We will acknowledge receipt of your complaint, investigate the matter, and determine the steps required to resolve or remedy your complaint. We will provide you with our response at the completion of our investigation, in writing. This will usually not take longer than 30 days. If you are not satisfied with our response, you can refer your complaint to the office of the Australian Information Commissioner via www.oaic.gov.au.

You may also refer to our Complaints Management Policy, which we can provide a copy of upon request.

CONTACT

If you would like more information about our Privacy Policy, please contact FIS:

- P: 0459 095 999
- E: service@fisgroup.biz
- Mail: PO Box 46, Salamander Bay NSW 2317

REVIEW OF POLICY

FIS's General Manager – Investigations is responsible for the content and administration of this Privacy Policy. FIS's General Manager – Investigations will closely monitor compliance with this Privacy Policy, as well as its effectiveness.

The Policy is reviewed every two years, or more frequently in line with changes in legislation.