

Alston Gayler & Co Limited/Miller Group

Data Privacy Notice

Introduction

This Privacy Notice explains how we (Alston Gayler & Co Limited and the Miller Group entities referred to in the “About us” section below) process your personal data.

Please take the time to read this Privacy Notice carefully as it explains how we collect, use and store your personal data, and the rights you have in relation to the protection of your personal data. If, at any time, you have any concern about how your personal data is being processed by us, please let us know at info@agcover.co.uk.

About us

The entities that are the controllers responsible for processing your personal data are:

- Alston Gayler & Co Limited, 70 Mark Lane, London, EC3R 7NQ, info@agcover.co.uk (“AG”)
- Miller Insurance Services LLP, 70 Mark Lane, London, EC3R 7NQ, info@miller-insurance.com (“Miller”); and
- Miller Europe SPRL, Val d’Or, Gulledelle, 96 1200, Brussels Belgium, info@miller-insurance.com (“Miller Europe”).

As such, in this Privacy Notice references to “AG”, “Miller” “we”, “us” or “our” in this privacy notice, are to AG, Miller and/or Miller Europe as applicable in the circumstances, depending on which entity/entities is/are providing the services that you are receiving or benefitting from.

Miller Insurance Services LLP is the controller that is responsible for the website, www.alstongayler.com.

We are responsible for ensuring compliance with data protection laws and we take your privacy and our obligations very seriously.

Information that we collect about you

We receive contact details, medical/health information and other information that you may be required to provide to us, or our clients, including when you register for our Online Services.

Information that you provide to us, or that we collect from you, if you apply for a job vacancy listed on our website or make a speculative application to our HR team. To find out more about the personal data that we collect in connection with job applications, please see “Information for Job Applicants” section below.

How we use your information

We use information about you:

- in order to deliver broking, consultancy and claims handling services to our clients, and to provide our Online Services;
- in order to comply with our legal obligations and applicable regulatory requirements;

- to facilitate the effective management, development or operation of AG/the Miller Group;
- in connection with negotiating, maintaining or renewing your insurance policies;
- to create anonymised industry or sector-wide statistics;
- in line with the London Insurance Market Core Uses Information Notice (which is available at <http://www.lmalloyds.com/GDPR>). We recommend that you review this notice;
- to manage our ongoing business relationship and any claim made under the contract of insurance;
- to undertake statistical analysis, business reporting and marketing;
- to recover debts and prevent fraud; and
- to carry out credit scoring and in connection with other automated decision making systems, for example, to generate quotations for insurance cover.

For information about how we use personal data relating to job applicants, please click see “Information for Job Applicants” section below.

We use "cookies" on our website in accordance with our Cookie Policy (which is available at www.alstongayler.com/cookie-policy).

Sharing your personal data

General disclosures

We may share your personal data in the following circumstances:

- to police and other law enforcement agencies, local and central authorities, AG/Miller’s regulators and other third parties where we are required to do so by law or a regulator or to comply with legal or regulatory requirements. This can be for a range of purposes such as preventing or detecting crime, fraud, apprehending or prosecuting offenders, assessing or collecting tax, investigating complaints or assessing how well a particular industry sector is working;
- to third parties and/or where permitted to do so in accordance with industry rules or where the information is publicly available;
- to resellers, distributors and agents to help us provide services to clients;
- to insurers, surveyors, loss adjustors, IT service providers, call centre providers and administrative support service providers, to the extent necessary to provide our services to you in a timely manner;
- to loss assessors, lawyers, and other like persons to the extent necessary to enable such third parties to provide information or services you have requested;
- to premium finance companies to the extent necessary to enable them to provide you with greater choice in making premium payments;

- to other companies in AG/the Miller Group to the extent necessary to facilitate the effective management, administration, or operation of those businesses; and
- to anyone to whom you authorise us to give such information to.

Insurance specific disclosures

We:

- share information concerning your insurance arrangement with insurers where this is necessary to enable insurers to decide whether to participate in any arrangement whereby participating insurers agree to automatically insure (wholly or partly) a portfolio of risks by delegating to us their authority to bind individual risks within such portfolio to the lead insurer;
- share anonymised information concerning payment or settlement of your insurance claims with third parties to assist our other clients with payment, negotiation and settlement of their claims with the same or different insurers; and share information about your insurance placements, which may include client names, types of policy, premium and renewal dates, with insurers to enable them to provide and improve their services to you..

Credit scoring and credit reference agencies

We sometimes use a credit scoring or other automated decision making system, for example, to generate quotations for insurance cover when processing information provided. We may disclose this information to other departments within the AG/Miller Group, to advisers, agents, banks, credit reference and fraud prevention agencies or anyone to whom we propose to transfer any of our rights and/or responsibilities under this agreement, each of whom may also use such information in the ways described in this Privacy Notice.

We share financial data to credit reference agencies (“**CRAS**”). Each organisation that shares financial data with the CRAs is also entitled to receive similar kinds of financial data contributed by other organisations. These organisations are typically banks, building societies, and other lenders, as well as other credit providers like utilities companies and mobile phone networks. As such, the financial data that we share with CRAs will also be visible to other organisations.

Fraud prevention

If we believe that fraud has been or might be committed, we may share data with fraud prevention agencies (“**FPA**”s). These FPAs collect, maintain and share data on known and suspected fraudulent activity. Some CRAs also act as FPAs.

Job applications

For information about how we use personal data relating to job applicants, please see “Information for Job Applicants” section below.

Transferring your personal data overseas

AG/Miller is based in the UK and Belgium and keeps its main databases there. Sometimes we will need to send or allow access to personal data from elsewhere in

the world. This might be the case, for example, when a processor or client of AG/Miller is based overseas or uses overseas data centres.

While countries in the European Economic Area all ensure a high standard of data protection law, some parts of the world may not provide the same level of legal protection when it comes to personal data. As a result, when AG/Miller does send personal data overseas it will make sure suitable safeguards are in place in accordance with European data protection requirements, to protect the data. For example, these safeguards might include:

- sending the data to a country that's been approved by the European authorities as having a suitably high standard of data protection law. Examples include the Isle of Man and Switzerland.
- putting in place a contract with the recipient containing terms approved by the European authorities as providing a suitable level of protection.
- sending the data to an organisation which is a member of a scheme that's been approved by the European authorities as providing a suitable level of protection. One example is the Privacy Shield scheme agreed between the European and US authorities. Another example is Binding Corporate Rules.

If your data has been sent overseas like this, you can find out more about the safeguards used by contacting us at info@agcover.co.uk.

Changes to this Data Protection Notice

From time to time, we may make minor changes to this Privacy Notice. We will notify you of these changes by posting the revised Privacy Notice on our website. If we make significant changes, we will take additional steps to inform you of these.

What are our legal grounds for handling personal data?

Legitimate interests

Data protection law allows the use of personal data where necessary for legitimate purposes as long as this isn't outweighed by the interests, fundamental rights or freedoms of data subjects.

The law calls this the Legitimate Interests condition for personal data processing.

The Legitimate Interests being pursued here are:

- promoting the responsible selection of relevant products;
- helping prevent and detect crime and fraud and anti-money laundering services and verify identity;
- supporting tracing and collections;
- supporting compliance with legal and regulatory requirements.

Consent

We will obtain consent for distribution of marketing information where we do not have an existing relationship with you, or where we are otherwise required to do so by law.

Where your consent is required, we will ask you for it at the relevant time. You do not have to provide your consent, and you may withdraw it at any time. If you choose not to give your consent (or to withdraw it), this may prevent us from providing our services to you or progressing your application.

Contractual obligations

We are permitted to use personal data where processing is necessary for the performance of a contract to which you are a party, or in order to take steps at your request prior to entering into a contract.

Legal obligations

We are permitted to use personal data where necessary in order to comply with our legal or regulatory obligations in respect of insurance, data protection and other regulators which may, for example, include disclosure to insurers, auditors and the police.

Substantial public interest (insurance purposes)

The UK Data Protection Act 2018 contains an 'insurance purposes ground', so that classes of special category personal data (e.g. relating to health, as well as data relation to criminal convictions and offences) may be processed where this is necessary for an insurance purpose (within the terms of the Act) without your consent.

Our use of your personal data is subject to an extensive framework of safeguards that help make sure that people's rights are protected. These include the information given to people about how their personal data will be used and how they can exercise their rights to obtain their personal data, have it corrected or restricted, object to it being processed, and complain if they're dissatisfied. These safeguards help sustain a fair and appropriate balance, so our activities don't override the interests, fundamental rights and freedoms of data subjects.

For information about the legal grounds that we have for processing the information that you provide to us when you apply for a job with please see "Information for Job Applicants" section below.

Rights in respect of personal data

If, having given your consent to the use of your data, you subsequently change your mind, you can stop all, or particular uses of your data by sending an email to info@agcover.co.uk.

Individuals have a right to: (i) request personal data held about them is corrected, supplemented, blocked or deleted if the data is factually incorrect, incomplete or irrelevant for the purposes described in this Privacy Notice, or where it is being processed in a manner which in any way infringes applicable law; and/or (ii) request a copy of the personal data we hold about them. To obtain details of data held by us about you, please write to:

Data Protection, Alston Gayler & Co Limited, 70 Mark Lane, London, EC3R 7NQ.

Your request should make it clear what type of information you are seeking. No fee is payable for such a request. Upon receipt of your request, and where all of our

requirements to process such a request have been met in full, we shall respond within one calendar month of receipt.

Data portability right

New data protection legislation also contains a right to data portability that may give consumers a right in some data processing contexts, to receive their personal data in a portable format when it's processed on certain grounds, such as consent.

Correcting errors

If you think that any personal data we hold about you is wrong or incomplete, you have the right to challenge it. If the data does turn out to be wrong, we will update our records accordingly. If we still believe the data is correct after completing our checks, we will continue to hold and keep it - although you can ask us to add a note to your file indicating that you disagree or providing an explanation of the circumstances.

Objecting to the use of personal data

You have the right to lodge an objection about the processing of your personal data. If you want to do this, you should contact us, using the contact details set out above.

Whilst you have complete freedom to contact us with your objection at any time, you should know that under the General Data Protection Regulation, your right to object doesn't automatically lead to a requirement for processing to stop, or for personal data to be deleted, in all cases.

Right to restrict processing

In some circumstances, you can ask us to restrict how we use your personal data. Your rights are set out at Article 18 of the GDPR. You can find our contact details above.

This is not an absolute right, and your personal data may still be processed where certain grounds exist. This is:

- with your consent;
- for the establishment, exercise, or defence of legal claims
- for the protection of the rights of another natural or legal person;
- for reasons of important public interest.

Only one of these grounds needs to be demonstrated to continue data processing.

We will consider and respond to requests, including assessing the applicability of these exemptions.

Right to Erasure

The right to erasure is also known as 'the right to be forgotten'. Individuals can make a request for erasure verbally or in writing and we have one month to respond to such

a request. The right is not absolute and only applies in certain circumstances. Individuals have the right to have their personal data erased if:

- the personal data is no longer necessary for the purpose for which we originally collected or processed it for;
- we are relying on consent as the lawful basis for holding your data, and you wish to withdraw such consent;
- we are relying on legitimate interests as the basis for handling personal data, you object to the processing of your personal data, and there is no overriding legitimate interest to continue this processing;
- we are processing the personal data for direct marketing purposes and you object to that processing;
- we have processed the personal data unlawfully (i.e. in breach of the lawfulness requirement of the 1st principle);
- we are required to do so to comply with a legal obligation.

For how long is personal data retained?

Identifiers

Identification data like names and addresses are kept while there is a continuing need to keep it. This need will be assessed on a regular basis, and data that is no longer needed for any purpose will be disposed of.

Financial accounts and repayment data

Data about live and settled accounts is kept on credit files for six years from the date they're settled or closed. If the account is recorded as defaulted, the data is kept for six years from the date of the default.

Court judgments, decrees and administration orders

Generally, court judgments and other decrees and orders are kept on credit files for six years from the date of the judgment, decree or order. But, they can be removed if the debt is repaid within one calendar month of the original date or if the judgment is set aside or recalled by the courts.

Bankruptcies, IVAs, debt relief orders and similar events

Data about bankruptcies, IVAs and other insolvency-related events and arrangements are usually kept on credit files for six years from the date they begin. This period is extended if they last longer than six years. Some data, such as a bankruptcy restrictions order, can also remain on the credit file for longer than six years.

Although the start of these events is automatically reported to us, the end (such as a discharge from bankruptcy or completion of an IVA) might not be. This is why people are advised to contact us when this happens to make sure their files are updated accordingly.

Search footprints

We keep most search footprints for one year from the date of the search, although it keeps debt collection searches for up to two years.

Scores and ratings

We may keep credit scores and credit ratings for as long as they keep a file about the relevant person.

Derived or created data

We also create data, and links and matches between data. For example, we keep address links and aliases for as long as they are considered relevant for credit referencing purposes.

Links between people are kept on files for as long as we believe those individuals continue to be financially connected. When two people stop being financially connected, either can write to us and ask for the link to be removed. We will then follow a process to check the people are no longer associated with each other.

Job applications data

For information about how we use personal data relating to job applicants, please click see “Information for Job Applicants” section below.

Other data

Other third party supplied data such as politically exposed persons (PEPs) and sanctions data and mortality data will be stored for a period determined by criteria such as the agreed contractual terms.

Archived data

We may hold data in an archived form for longer than the periods described above, for things like research and development, analytics and analysis, (including refining lending and fraud strategies, scorecard development and other analysis such as loss forecasting), for audit purposes, and as appropriate for establishment, exercise or defence of legal claims. The criteria used to determine the storage period will include the legal limitation of liability period, agreed contractual provisions, applicable regulatory requirements and industry standards.

Where do I complain to if I am not happy?

In the first instance, please contact us at info@agcover.co.uk, which has an established complaints handling service.

You can also refer your concerns to the Information Commissioner’s Office (ICO), the body that regulates the handling of personal data in the UK. You can contact them by:

- phone on 0303 123 1113;
- writing to them at Information Commissioner’s Office, Wycliffe House, Water Lane, Wilmslow, SK9 5AF;
- going to their website at www.ico.org.uk.

Information for job applicants

Information that we collect about you

When you apply for a job with us we collect:

- your contact details;
- information that you include on your C.V., and covering letter (if you provide one);
- information collected during interviews, assessments and/or tests that we may ask you to complete as part of the recruitment process; and
- information needed to complete pre-employment checks.

You do not have to give us information that we ask for, but if you choose not to, we may not be able to process your application and/or take it to the next stage.

How we use your information

- to decide if you are suitable for the role;
- to check if you have any unspent convictions;
- to collect references;
- to verify your identity and qualifications;
- to check your immigration status;
- to carry out equal opportunities monitoring;
- to inform you of future vacancies (if you agree to this); and
- to comply with applicable legal or regulatory requirements.

Sharing your personal data

- We will share your personal data with the following third party service providers of pre-employment testing and screening, for the purposes of processing your application:
- We will also share your personal data with other entities within the Miller Group. Please see the “How we use your information” section above for further details.

What are our legal grounds for handling personal data?

- We handle the personal data of job applicants;
 - on the basis that this is necessary to perform a contract or to take steps at your request, before entering a contract;
 - to comply with our legal obligations; and
 - for our legitimate interests in:
 - processing and making decisions in relation to your application;
 - communicating with you;
 - ensure ongoing compliance with requirements in regulatory guidance

- detecting and prevent fraud and other criminal or infringing activity
- facilitating transfers of personal data intra-group for administrative/payroll purposes ; and
- record keeping.

You can object to processing on this basis at any time by contacting us at info@agcover.co.uk.

- We handle the special categories of personal data of job applicants (for example that relating to racial or ethnic origin, religious beliefs, trade union membership, health and sexual orientation):
 - on the basis that you have provided your explicit consent to us doing so. You do not have to provide your consent but if you choose not to, we may not be able to process, or progress your application. **You have the right to withdraw your consent for processing for that purpose at any time, without affecting processing carried out prior to withdrawal. To withdraw your consent, please contact info@agcover.co.uk;**
 - where this necessary for the establishment, exercise or defence of legal claims;
 - where this is necessary for certain prescribed purposes related to employment law;
 - for purposes related to preventive or occupational medicine and assessing working capacity of employees; and
 - where you have obviously made this information public.

For how long is personal data retained?

Should your application be unsuccessful (or successful but you choose not to accept the position), we will, where you have agreed to this, keep your personal data for up to one year after submission of your application so that we can consider you for future vacancies.

If your application is successful, we will carry out online pre-employment screening, which involves checking that you have the right to work in the location where you have applied to work, collecting references and completing other checks for specific roles, which we will inform you about if they are applicable to the role that you have applied for. If this screening is successful and you accept a job with us, we will keep your personal data in accordance with our employee privacy notice, which will be provided to you, once you accept the position. If this screening is unsuccessful, we will keep your personal data for up to one year.