

G J Sladdin & Co Ltd Privacy Policy

Assigned Data Protection Officer: Andrew Sladdin

The Data Protection Officer is responsible for data protection compliance. Any data requests or suspected data breaches should be notified to the Data Protection Officer immediately.

You can contact our Data Protection Officer at:

Address: 17 Clare Road, Halifax HX1 2HZ

Telephone Number: 01422 339147

Email: Andrew@sladdininsurance.com

Data Protection Law' includes the General Data Protection Regulation 2016/679; the UK Data Protection Act 2018 and all relevant EU and UK data protection legislation.

Scope

This policy applies to all personal data processed by G J Sladdin & Co Ltd and is part of G J Sladdin & Co Ltd's approach to compliance with data protection law. All staff are expected to comply with this policy and failure to comply may lead to disciplinary action for misconduct, including dismissal.

Privacy Notice

Your Personal Data

What we need

G J Sladdin & Co Ltd will be what's known as the 'Controller' of the personal data you provide to us. We may need to collect both Personal Data, such as your name, address, date of birth and contact details, and Sensitive Data such as details of your medical, financial and criminal information and history.

Why we need it

We need to know your personal and sensitive data in order to provide you with an insurance quotation, to issue a policy, to manage and administer the policy and to deal with any claims you may have. We will not collect any personal or sensitive data from you that we do not need in order to provide and oversee this service to you.

What we do with it

All the personal and sensitive data we process is processed by our staff in the UK, for the purposes of IT hosting and maintenance this information is located on servers outside of our main office but within the UK & Ireland. The information we hold on you will only be shared with our insurance partners and their authorised claims companies for the purpose of

fulfilling the insurance contract. We may also need to share your information with public bodies, such as the police, in order to prevent fraudulent claims; and regulators such as the FCA in order to respond to any complaints. If you agree to the use of a Third Party Finance provider, such as Close they will be provided with certain personal and sensitive data in order for them to provide a loan. No other 3rd parties have access to your personal data unless the law allows them to do so. We will never sell your personal data. We do not transfer any data outside of the UK and Ireland, should you wish to limit your data transfer to the UK only please contact us.

The above Personal Data Privacy Notice is issued to all clients.

How long we keep it

We are required under UK tax law to keep your basic personal data (name, address, contact details) for a minimum of 6 years after a policy sale, and in addition we must keep any data relative to Lloyd's policy for a minimum of 7years. After this time your data will be destroyed unless you have given us specific permission to hold the data in order to contact you about our products and offers. The information we use for marketing purposes will be kept with us until you notify us that you no longer wish to receive this information.

If at any point you believe the information we process on you is incorrect, you can request to see this information and even have it corrected or deleted. If you wish to raise a complaint on how we have handled your personal data, you can contact our Data Protection Officer who will investigate the matter. If you are not satisfied with our response or believe we are processing your personal data not in accordance with the law you can complain to the Information Commissioner's Office (ICO). Our Data Protection Officer is Mr Andrew Sladdin and you can contact them at Andrew@sladdininsurance.com.

Security

We will ensure that appropriate security measures are in place to ensure that personal data can only be accessed by those who need to access it and that it is held and transferred securely. This will include the use of individual logins and passwords for all staff, which are required to meet minimum password strength requirements and password updates required at least every 90days.

Individual Rights

1. The Right to be Informed

In the event that we suffer a Data Breach of any sensitive data, or data which is likely to risk your freedoms and rights (this includes damage to reputation, financial loss, loss of confidentiality etc) then in addition to informing the ICO (Information Commissioner's Office) we shall let you know within 72hours. E.g. if details of a home address and travel dates are lost in conjunction as this could put you at risk of burglary; or if we lost card/bank details sufficient for someone to start making transaction on your account.

2. The Right of Access

You have the right to request copies of all of the Data we hold on you. We will not charge for any request to provide a copy of the data we hold on you. Your request for data should be directed, in writing to the Data Protection Officer who will arrange for a copy of the data to be sent to you securely and without delay. We may need to verify that you are who you say you are before sending the data, as such we may ask various questions to authenticate your identity. All subject access requests will be provided within one month of your request.

3. The Right of Rectification

In the event that any of the data we hold is incorrect and out of date, please contact us and let us know as this will be rectified upon your instruction. We will follow our internal Data Flow Chart to ensure that all parties in the Data Chain relative to your policy are notified of the correction.

4. The Right to Erasure

All clients have the 'Right to be Forgotten', unless we are obliged to hold the information for legitimate/contractual means. Any request for erasure should be referred to the Data Protection Officer Andrew Sladdin who will review the request and ensure there is no further legitimate reason for us to store the data. If the data can be deleted then all parties within the Data Chain will be notified.

5. The Right to Restrict Processing

We are required to stop processing your data in the event of any of the following:

- Where the accuracy of the personal data is contested, we will restrict the processing until we have verified the accuracy of the personal data.
- Where you have objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and we are considering whether your organisation's legitimate grounds override those of the individual.

- When processing is unlawful and the individual opposes erasure and requests restriction instead.
- If we no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

6. The Right to Data Portability

Should you request it, the data we hold on you should be in a format that we are easily able to provide information to other parties. This should be done securely and without delay. We may need to verify that you are who you say you are before sending the data, and as such we may ask various questions to authenticate your identity.

7. The Right to Object

You have the right to object to:

- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

8. The Right not to be subject to automated decision making, including profiling

You can request that your data is not subject to automated decision making and profiling. “Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.”

The restriction does not apply if the decision is:

- Necessary for contract;
- Expressly authorised by law; or
- Has the explicit consent of the data subject.

Contact us

If you wish to request your Right of Access; Right of Rectification; Right to Erasure; Right to Restrict Processing; Right to Data Portability; Right to Object; Right not to be subject to automated decision making including profiling; then please contact our office - either by telephone on 01422 362614, email enquiries@sladdininsurance.com or by post to G J Sladdin & Co Ltd, 17 Clare Road, Halifax, HX1 2HZ.

Subject access requests

We will have the right to refuse subject access requests but only if they are manifestly unfounded or excessive, and we must tell you our reason for a refusal. In the event of refusal you have the right to complain to the supervisory authority. All requests, whether accepted or refused, must be dealt with within 1 month of the initial request.

Lawful Basis for processing data

We only collect data that we need for the purpose of quoting, issuing, managing and administering, and dealing with claims for the insurance product you are enquire about. We may also request your consent to contact you about other insurance products we offer.

Consent

Any information we request will be necessary to form a legal contract of insurance, or at least provide a quotation service precedent to a possible contract. Consent for any other use of your data must be freely given, specific, informed and unambiguous. There must be a positive opt-in; consent cannot be inferred from silence, pre-ticked boxes or inactivity. We will therefore ask you to confirm vocally over a recorded telephone call, or physically by tick box and signature if we wish to use your personal data for any other purpose. This may be so that we can contact you in future about other insurance products that we offer. You can withdraw your consent for us to hold your data at anytime provided we do not need it for the purposes of fulfilling a contract with you.

Telephone recording

We record all telephone calls as this protects the interest of our company and staff as well as our clients. We are also obliged under FCA guidelines to record calls leading up to a transaction. We may at certain points turn off the call recording to prevent collection of sensitive data such as bank card details. Our telephone recordings are retained on a secure server and can only be accessed by secure logins which are restricted to certain members of staff and management.

Data Breach Procedure

If we discover a Data Breach then this must be reported to the Data Protection Officer, Andrew Sladdin, immediately. If the Data Protection Officer is unavailable for any reason then the breach should be notified to another senior member of staff.

The ICO need to be contacted with 72 hours of the breach, even if we have very little information at this stage.

The extent of the breach will be investigated to find out what data has been affected, how it has been accessed/leaked, and the risk of the data breach to individuals.

Privacy Impact Assessment

The implementation of any new systems, procedures, or business relationships we will be subject to a Privacy Impact Assessment.

A Privacy Impact Assessment will address the following:

- Identify the need for a PIA
- Describe the information flows
- Identify the privacy and related risks
- Identify and evaluate the privacy solutions
- Sign off and record the PIA outcomes
- Integrate the outcomes into the project plan
- Consult with internal and external stakeholders as needed throughout the process

Your Right to Complain to the ICO (Information Commissioner's Office)

If you are not satisfied with our use of your personal data, our response to any request by you to exercise any of your Individual Rights, or if you think we have breached GDPR, then you have the right to complain to the ICO:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Tel: 0303 123 1113 (local rate) or 01625 545 745 (national rate)
Email: casework@ico.org.uk

Monitoring and review

This policy was last updated on 29th September 2021 and shall be regularly monitored and reviewed, at least every two years.