Lowndes Halsden

Independent Personal Financial Planning Specialists

Privacy Policy

CLIENTS AND PROSPECTS (CURRENT AND PREVIOUS); INTERMEDIARIES; AND ASSOCIATED PARTIES.

Executive Summary

This is a summary of how Lowndes Halsden & Partners Limited processes personal data.

Who this privacy policy is for: This privacy policy applies to current or previous clients, prospective clients, intermediaries or clients of intermediaries, and any associated parties.

Why we collect personal data: We collect your personal data in the course of providing our services.

Where we collect personal data from: We may collect personal data directly from you, our staff, third parties, or our clients. This is likely to be done face-to-face, by post, over the phone, or online.

What personal data do we collect: The types of data that we collect include personal details, financial data, ID and verification documents, special category and sensitive data, and any other information which you choose to provide.

What we use personal data for: We only use personal data for necessary and proportionate purposes. These include advising clients from the time they are a prospective client to the time we onboard them as our client, carrying out suitability assessments and anti-money laundering checks, managing and administering your accounts, managing relationships with intermediary firms, recording calls for regulatory compliance reasons, handling feedback, requests, queries and complaints, and improving the quality of our products and services.

Our legal basis for processing personal data: As a controller, we ensure that we and our processors process personal data lawfully. Most commonly, we will process data to perform a contract with you, to comply with a legal or regulatory obligation, in our or your legitimate interests or with your consent. We may rely on other lawful bases from time to time, including where we process sensitive or special categories of data.

Who we may share personal data with: We will not share your information with any third parties for direct marketing purposes. Any third party data processors we use who provide elements of our services for us will have a contract in place with our data processors. This means they cannot do anything with your personal information unless we have instructed them to do it. They will not share your personal information with any organisation apart from us. They will hold it securely and retain it for the period we instruct. In some circumstances, we are legally obliged to share information, for example, under a court order or where we cooperate with other regulatory bodies in handling complaints or investigations. We might also share information with other regulatory bodies to further their or our objectives. In any scenario, we'll satisfy ourselves that we have a lawful basis on which to share the information and document our decision making showing how we have a legal basis on which to share the information.

How long we keep personal data for and our security measures: We keep your data until the purpose for which it was collected is fulfilled and in line with our data retention. We may need to keep certain data for longer to fulfil any legal, regulatory or reporting requirements. Your data is processed and stored securely in our systems, and in the unlikely event of a data breach, we will take appropriate steps to notify the regulator or you where applicable.

Your rights and making queries or complaints: You can exercise your rights to make a query or complaint about how we handle personal data by using the contact details in the "Contact Us" section of our Privacy Policy.

1. About this Privacy Policy

This privacy policy applies to current or previous clients, prospective clients, intermediaries or clients of intermediaries, and any associated parties, and it explains how Lowndes Halsden & Partners Ltd processes personal data.

The purpose of this Privacy Policy is to outline how we process personal data, including special categories of data, and the legal basis on which we process personal data. It is important that those whose personal data we process read and understand this Privacy Policy.

Please note that this Privacy Policy provides an overview of how we process personal data and we may provide further information in just-in-time privacy statements during the course of your interactions with our staff and services.

2. Data controller

For the purposes of applicable data protection law, in particular the General Data Protection Regulation ("GDPR") and the UK GDPR, your data will be controlled by Lowndes Halsden & Partners Ltd.

Our Data Protection Officer is Spencer Drew. You can contact him via one of the methods listed below. If you do make contact via the post, please mark the envelope with 'FAO Data Protection Officer'.

There are many ways you can contact us, including by phone, email and post.

Our postal address:

Lowndes Halsden and Partners Ltd
Holt House
184 – 190 Caerphilly Road
Birchgrove
Cardiff
CF14 4NR

Helpline number: 02920 694242

For general contact please use this page on our website.

3. Sources of data collection

Personal data is collected through paper or web forms or in face-to-face, phone or e-mail communications. During our client onboarding process and throughout our relationship with you, it may be necessary for you to provide personal data, including special categories of data relating to other people. Where this occurs, you must ensure that they understand how their information will be used, that they have given you their permission to disclose it for these purposes, and that they allow us to process their data as set out in this Privacy Policy. Our services are generally not directed towards children, and so we typically only process children's personal data where they are named on a portfolio as dependants, are beneficiaries, or with regards to trusts or Junior ISA's.

Most of the personal information we process is provided to us directly by you for one of the following reasons:

- You wish to attend, or have attended, an appointment.

- You have applied for a job with us.
- You are representing your organisation.
- You have made an enquiry to us.
- You have made an information request to us.

We may also receive personal information indirectly, in the following scenarios:

- We have contacted an organisation about a product you may have, and it gives us your personal information in its response.
- An existing client refers to you in their correspondence.
- We have seized personal information as part of an investigation.
- From other regulators or law enforcement bodies.
- An employee of ours gives your contact details as an emergency contact or a referee.

If it is not disproportionate or prejudicial, we'll contact you to let you know we are processing your personal information.

4. Types of personal data

The type of personal data we collect will depend on the product or service we provide. We will only collect information that is adequate, relevant, and limited to what is necessary in relation to the purpose identified with this Privacy Policy.

The table below outlines the categories of personal data we may process, with common examples. Please note that this is an indicative, non-exhaustive list, and the personal data we use may change over time.

Data category	Common examples
Personal details	Biographical Contact details Gender Marital Status Official identification documents Internal client identification numbers Family circumstances and background Behavioural and lifestyle Education and employment history Organisational roles including trusteeships, directorships and partnerships Records of communications and correspondence Client contact and communication preferences Any other personal information that you choose to share with us during communications
Financial data	Current financial situation Financial history Financial planning

	Source of wealth and source of funds Billing and banking Tax Pension Insurance policies and positions Credit Status Risk appetite and score Portfolio position and performance Ethical and investment restrictions Any other financial information that you choose to share with us
Special category and sensitive data	Mental and physical health, including vulnerability Nationality Any other personal information that you choose to share with us, such as political or religious views and criminal convictions and judgements
Anti-money laundering ("AML") data	Official documentation to verify identity including: Identification documents (which may include photographic identification and signatures) Other official documentation on request Official documentation to verify address including: Bank Statements Utility bills Other official documentation on request Source of wealth and source of funds Details for conducting Politically Exposed Person and Sanctions checks against relevant lists Criminal convictions and judgements relation to, or resulting from, the above checks or which you have told us about
Cookies and technical data	We collect cookies from your device when you access and use our website. For more information, please see our Cookie Policy

5. Purposes for processing

Our primary purpose of processing personal data is to provide our services to our clients. This includes onboarding clients, assessing suitability for financial products and service, providing investment advice, and sending information. We will take steps to ensure that personal data is handled only by personnel that have a need to do so for the purposes described in this policy.

The table below provides examples of the purposes for which we process personal data and the lawful basis we rely on under Article 6, Article 9 and Article 10 GDPR and UK GDPR. Please note that this is an indicative, non-exhaustive list.

Process	Purpose of processing	Law basis for processing
Prospective clients	To take steps, at your request, prior to entering a contract with us in order to begin the process of onboarding you as a client	Article 6 (1) (a) – Consent Article 6 (1) (b) – Performance of a contract Article 6 (1) (f) – Legitimate interests
Client onboarding	To onboard you as our client, and set up a file with your documentation, including information relating to vulnerability or health position if applicable, and to verify your identity. To execute our business relationship with you. For example, we ask you to complete a client attitude to risk questionnaire, before risk discussions in order to generate a risk appetite score (which is regularly reviewed and agreed by you) on which to base our services during the course of your relationship with us	Article 6 (1) (b) – Performance of a contract Article 6 (1) (f) – Legitimate interests Article 9 (2) (a) – Explicit consent Article 9 (2) (g) – Substantial public interest
Attend an appointment or event	Our purpose for collecting this information is so we can facilitate the event and provide you with an acceptable service.	Article 6 (1) (a) – Consent Article 6 (1) (f) – Legitimate interests Article 9 (2) (a) – Explicit consent
Register for a webinar or online meeting	Our purpose for collecting this information is so we can facilitate the meeting and provide access to it.	Article 6 (1) (a) – Consent Article 6 (1) (f) – Legitimate interests
Client Contact	To send appropriate communications, knowledge, knowledge and insight and recommend products and services that we think might be suitable for you or that we think is of importance, interest or relevance, including in response to requests from you via our webform, email or telephone. To invite you to your periodic financial review, this will include key information such as date, time and location	Article 6 (1) (a) – Consent Article 6 (1) (c) – Compliance with a legal obligation Article 6 (1) (f) – Legitimate interests

	To notify you and associated parties about important changes to our services, products or offerings and provide non-marketing communications about valuations, statements and account information	
Make an information request	We need information from you to respond to you and to locate the information you are looking for. This enables us to comply with our legal obligations under the legislation we are subject to: • General Data Protection Regulations (2016) • Data Protection Act (2018) • Freedom of Information Act (2000) • Environmental Information Regulations (2004)	Article 6 (1) (a) – Consent Article 6 (1) (c) – Compliance with a legal obligation Article 6 (1) (f) – Legitimate interests
Make an enquiry	We need enough information from you to answer your enquiry, if you call us, we won't make an audio recording of it, but in some circumstances we may make notes to provide you with a further services as required.	Article 6 (1) (a) – Consent Article 6 (1) (c) – Compliance with a legal obligation Article 6 (1) (f) – Legitimate interests
AML checks	To verify your identity and comply with legal obligations under AML legislation where applicable. To prevent, detect and report fraud, money laundering and other offences To protect our business and for risk management	Article 6 (1) (c) – Compliance with a legal obligation Article 6 (1) (f) – Legitimate interests Article 9 (2) (g) – Substantial public interest Article 10 – Schedule conditions for processing
Suitability assessments	To ensure suitability for financial products and services, including information relating to vulnerability or health position if applicable. Suitability is regularly reviewed throughout your relationship with us	Article 6 (1) (c) – Compliance with a legal obligation Article 6 (1) (f) – Legitimate interests Article 9 (2) (a) – Explicit consent

		Article 9 (2) (g) – Substantial public interest
Management and administration of accounts, systems, services, products and offerings, including via online and digital platforms	To provide services, products or offerings, including online and digital, as requested To provide investment management and financial planning services to you directly To effectively manage, administer and operate contractual agreements and comply with instructions or requests on your behalf. We may use providers such as DocuSign to securely exchange information with you To analyse and report on the effectiveness of our operations and growth strategies to increase efficiency, innovation and maintain a competitive edge To administer fees and charges	Article 6 (1) (b) – Performance of a contract Article 6 (1) (c) – Compliance with a legal obligation Article 6 (1) (f) – Legitimate interests
Management and transfers of pensions	To manage and administer pensions or transfer your pension to or from a third-party pension provider	Article 6 (1) (a) – Consent Article 6 (1) (b) – Performance of a contract Article 6 (1) (f) – Legitimate interests
Handling complaints, queries and legal claims	To respond to complaints, legal claims, data breaches or data protection rights requests	Article 6 (1) (c) – Compliance with legal obligation Article 6 (1) (f) – Legitimate interests Article (9) (2) (f) – Legal claims or judicial acts
Management and operations of technology and systems	To maintain security of our systems and prevent fraud and offer proactive, up-to-date security for our technology services To obtain further knowledge of current threats to network security in order to update our security solutions To analyse, test, develop and improve our systems and services	Article 6 (1) (f) – Legitimate interests

Regulatory and internal compliance	To comply with regulatory audit and report requirements To monitor the use of our copyrighted materials and comply with internal policies and procedures	Article 6 (1) (c) – Compliance with legal obligation Article 6 (1) (f) – Legitimate interests
Cookies and technical data	To collect, analyse and report on technical information about the services that you interact with when visiting our website. For more information, please see our Cookie Policy	Article 6 (1) (a) – Consent Article 6 (1) (f) – Legitimate interests

6. Sharing of data

We will not share your information with any third parties for the purposes of direct marketing. We use data processors who are third parties who provide elements of services for us. We have contracts in place with our data processors. This means that they cannot do anything with your personal information unless we have instructed them to do it. They will not share your personal information with any organisation apart from us. They will hold it securely and retain it for the period we instruct.

In some circumstances, we are legally obliged to share information. For example, under a court order or where we cooperate with other regulatory bodies in handling complaints or investigations. We might also share information with other regulatory bodies in order to further their or our objectives. In any scenario, we'll satisfy ourselves that we have a lawful basis on which to share the information and document our decision making and satisfy ourselves we have a legal basis on which to share the information.

The following table is an indicative, non-exhaustive list to help you understand the types of data sharing activities we undertake.

Third party	Purpose of sharing
Representatives	We may share information with authorised representatives acting on your behalf, such as a family member or legal representative
Suppliers and vendors	We outsource certain functions to third party suppliers and vendors to assist with our business operations and may share certain types of personal data in the course of business. This may include accountants, IT and technical support providers, communications providers and platforms.
Credit reference agencies and AML companies	We may undertake an electronic check to verify the personal identity information you have provided. The check will be undertaken by a reputable referencing agency or AML company which will retain a record of that check according to their retention policy. This information may be used by other firms or financial institutions for fraud prevention purposes.

	For example: GBG ID3Global SmartSearch
Our business partners	We may share data with our business partners including intermediaries, pension or product/service providers, who provide you or your organisation with services alongside or related to those provided by us. We may also share information to cooperate in response to complaints, legal claims, regulatory authority requests, data breaches or data protection rights requests.
Government departments, bodies or agencies	We may disclose information to any court or tribunal or government, regulatory, law enforcement, fiscal or monetary authority or agency where reasonably requested to do so or if required by applicable law, regulations or guidelines or in order to resolve queries, concerns or complaints. For example: HMRC National Crime Agency The police Financial Conduct Authority Information Commissioner's Office Financial Ombudsman Service Central Bank of Ireland recipients may also include tax, law enforcement and regulatory bodies, and courts and judicial bodies in other countries, such as the US, where applicable.

7. Data retention

The duration for which we retain your personal data will vary depending on the type of personal data and our reason for collection and processing. We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including the purposes of satisfying any legal or regulatory reasons. To determine the appropriate retention period for personal data, we consider the following:

- The volume of personal data
- The nature, and sensitivity of the personal data
- Our regulatory obligations and legal requirements to retain your personal data
- The purpose of processing your personal data
- The risk of unauthorised use or disclosure of your personal data

8. Security of personal data

We will take all appropriate technical and organisational steps to safeguard your personal data. In the unlikely event of a data breach, we will contact you in line with our legal obligations. Access to your personal data will be restricted to those who need to use it for legitimate legal and business purposes.

We follow several industry good practices to ensure this protection is fully effective and the appropriate technical and organisational measures are in place. All personal data is provided protection in line with security and data protection policies.

All our employees receive mandatory information security and data protection training on being hired and subsequently on at least an annual basis to ensure that they are aware of the security policies and their specific information security responsibilities. This also ensures that they are properly equipped to perform their duties in maintaining our security posture.

9. Data protection rights

The UK GDPR provides you, the data subject, with a number of rights when it comes to your personal data. On receipt of a valid request to invoke one of your rights, we will do our best to adhere to your request as promptly as reasonably possible.

Access: You have the right to request a copy of the personal data that we hold about you. There are exceptions to this right so that access may be denied if, for example, making the information available to you would reveal personal data about another person or if we are legally prevented from disclosing such information.

Accuracy: We aim to keep your personal data accurate, current, and complete. We encourage you to contact us to let us know if any of your personal data is not accurate or changes, so that we can keep your personal data up to date.

Objection: You have an absolute right to object to the processing of your personal data for direct marketing. Opting out of receiving marketing communications will not affect the processing of personal data for the provision of our services. In other cases where the right to object applies, the right is not absolute and only applies in certain circumstances.

Restriction: You have the right to ask us to block or restrict the use of your personal data. The right is not absolute and only applies in certain circumstances.

Portability: You have the right to request to move, copy or transfer personal data from one IT environment to another in a safe and secure way, without affecting its usability.

Erasure: You have the right to ask us to erase personal data we hold about you. The right is not absolute and only applies in certain circumstances.

Right to withdraw consent: If you have provided your consent to the collection, processing and transfer of your personal data, you have the right to fully or partly withdraw your consent. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose(s) to which you originally consented unless there is another legal ground for the processing. If you withdraw your consent, this will not invalidate the lawfulness of any processing carried out on the basis of consent before you withdrew it.

Data Protection Complaints: If you believe that your data protection rights may have been breached, you have the right to lodge a complaint with the applicable supervisory authority (See Section 11) or to seek a remedy through the courts.

Details of how to make a data protection rights request or query are below in the ‘Contact Us’ section

10. Visitors to our website

Analytics

When you visit https://lowndesonline.co.uk, we use a third-party service, Google Analytics, to collect standard internet log information and details of visitor behaviour patterns. We do this to find out such things as the number of visitors to the various parts of the site. This information is only processed in a way that does not identify anyone. We do not make, and do not allow Google to make, any attempt to find out the identities of those visiting our website.

If we do collect personal data through our website, we'll be upfront about this. We'll make it clear when we collect personal information, and we'll explain what we intend to do with it.

Cookies

You can read more about how we use cookies on our Cookies Policy. We use a cookies tool on our website which relies on implied consent of users. In recognition of the fact that the implementation date for the revised e-Privacy Regulation remains unknown, we are taking reasonable steps now to align our use of cookies with the standard of consent required by GDPR.

This means that we are in the process of updating the tool (Cookie Tool), which, by default, requires explicit opt-in action by users of our website. This will apply to the non-necessary cookies. We will ensure any necessary cookies for functionality and security are marked so that they are not deleted by the tool.

The purpose of implementing all of the above is to maintain and monitor the performance of our website and to constantly look to improve the site and the services it offers to our users. The legal basis we rely on to process your personal data is Article 6(1)(f) of the GDPR, which allows us to process personal data when it's necessary for the purposes of our legitimate interests.

11. Visitors to our office

We meet visitors at our office, including:

- dignitaries;
- external training providers;
- job applicants;
- suppliers and tradespeople;
- stakeholders; and
- organisations we may be interviewing about their processing.

If your visit is planned, we'll send your name and visit information to reception before your visit so that they will be ready when you arrive.

If you arrive without an appointment, you may be asked to wait a short time while we gather some personal data for verification.

We ask all visitors to report to reception and show a form of ID. The ID is for verification purposes only, we only record this information, if needed, for regulatory money laundering purposes.

We record the device address and will automatically allocate you an IP address whilst on site. We also log traffic information in the form of sites visited, duration and date sent/received.

We don't ask you to agree to terms, just to the fact that we have no responsibility or control over your use of the internet while you are on site, and we don't ask you to provide any of your information to get this service.

The purpose of processing this information is to provide you with access to the internet whilst visiting our site. The legal basis we rely on to process your personal data is Article 6(1)(f) of the GDPR, which allows us to process personal data when its necessary for the purposes of our legitimate interests.

For information about how long we hold personal data, please see Data retention section.

12. Managing customer contact

Restricted contact

We may impose a restriction on your access to our services if its necessary to protect our staff from unacceptable behaviour.

If we do this, we'll explain to you the restrictions we have applied and why we feel it's necessary. We'll create a record of the restriction for administrative purposes, so relevant staff members know the restriction is in place. This will include your name, contact details and a description of why we have imposed a restriction. The decision to impose a restriction will be taken and reviewed by a manager. We'll write to you explaining why we've applied the restriction and if it will be reviewed periodically. We'll remove it if we feel your behaviour has changed or if you no longer communicate with us.

Single point of contact

We may provide a single point of contact if you and we (or both) believe it will help to create a better outcome for all concerned.

A decision will be made by a manager to give you a single point of contact. This may be where you have several complaints, and we believe it will be more efficient for us to deal with them in this way. We'll make a record of the fact that you have a single point of contact. All relevant staff will know about using it to manage communications between our office and you. It will include your name, contact details and a description of the need to have a single point of contact. We'll review this requirement from time to time.

13. Applying for a job

Purpose and legal basis for processing

Our purpose for processing this information is to assess your suitability for a role you have applied for.

The legal basis we rely on for processing your personal data is Article 6(1)(b) of the GDPR, which relates to processing necessary to perform a contract or to take steps at your request before entering a contract. The legal basis we rely on to process any information you provide as part of your application which is special category data, such as health, religious or ethnic information, is Article 9(2)(b) of the GDPR, which also relates to our obligations in employment and the safeguarding of

your fundamental rights and Article 9(2)(h) for assessing your work capacity as an employee. In addition, Schedule 1 parts 1(1) and (2)(a) and (b) of the DPA2018 relates to processing for employment, the assessment of your working capacity and preventative or occupational medicine.

What will we do with the information you give us?

We'll use all the information you provide during the recruitment process to progress your application with a view to offering you an employment contract with us, or to fulfil legal or regulatory requirements if necessary.

We will not share any of the information you provide with any third parties for marketing purposes.

We'll use the contact details you give us to contact you to progress your application. We'll use the other information you provide to assess your suitability for the role.

What information do we ask for, and why?

We do not collect more information than we need to fulfil our stated purposes and will not keep it longer than necessary.

The information we ask for is used to assess your suitability for employment. You don't have to provide what we ask for, but it may affect your application if you don't.

Application stage

If you use our online application system, your details will be collected by a data processor on our behalf (please see below).

We ask you for your personal details including name and contact details. We'll also ask you about previous experience, education, referees and answers to questions relevant to the role. Our recruitment team will have access to all this information.

You will also be asked to provide equal opportunities information. This is not mandatory – if you don't provide it, it won't affect your application. We won't make the information available to any staff outside our recruitment team, including hiring managers, in a way that can identify you. Any information you provide will be used to produce and monitor equal opportunities statistics.

Shortlisting

Our hiring managers shortlist applications for interview. They will not be provided with your name or contact details or with your equal opportunities information if you have provided it.

Assessments

We may ask you to participate in assessment days, complete tests or occupational personality profile questionnaires, attend an interview, or a combination of these. Information will be generated by you and by us. For example, you might complete a written test, or we might take interview notes. This information is held by us.

If you are unsuccessful after assessment for the role, we may ask if you would like your details retained in our talent pool. If you say yes, we will proactively contact you should any further suitable vacancies arise.

Conditional offer

If we make a conditional offer of employment, we'll ask you for information so that we can carry out pre-employment checks. You must successfully complete pre-employment checks to progress to

a final offer. We must confirm the identity of our staff and their right to work in the United Kingdom, and seek assurance as to their trustworthiness, integrity and reliability.

You must therefore provide:

• proof of your identity – you will be asked to attend our office with original documents; we'll take copies

• proof of your qualifications – you will be asked to attend our office with original documents; we'll take

• a criminal records declaration to declare any unspent convictions

• your email address, which we'll pass to the Government Recruitment Service, which will contact you to complete an application for a Basic Criminal Record check via the Disclosure and Barring Service, or Access NI, which will verify your declaration of unspent convictions.

• We'll contact your referees, using the details you provide in your application, directly to obtain references

• We'll also ask you to complete a questionnaire about your health to establish your fitness to work.

If we make a final offer, we'll also ask you for the following:

• bank details – to process salary payments + pension if applicable.

• emergency contact details – so we know who to contact in case you have an emergency at work

After your start date

Some roles require a higher level of security clearance – this will be clear on the advert or job description (or both). If so, you will be asked to submit information to the FCA. The FCA will be the data controller for this information.

The FCA will tell us whether your application is successful or not. If it is not, we will not be told the reasons, but we may need to review your suitability for the role or how you perform your duties.

Our Code of Conduct requires all staff to declare if they have any potential conflicts of interest. If you complete a declaration, the information will be held on your personnel file. You will also need to declare any secondary employment

How long is the information kept for?

For information about how long we hold personal data, see our Data retention section.

How do we make decisions about recruitment

Final recruitment decisions are made by hiring managers and members of our recruitment team. We take account of all the information gathered during the application process.

You can ask about decisions on your application by speaking to the office manager Spencer Drew or by emailing sd@lowndesonline.co.uk

Your rights

As an individual, you have certain rights regarding your own personal data.

For more information on your rights, please see 'Your rights as an individual'.

Do we use any data processors?

Yes – we use several processors to provide elements of our recruitment service for us.

We sometimes advertise through An Employment Website or Recruitment Agencies. They will collect the application information and may ask you to complete a work preference questionnaire that is used to assess your suitability for the role; the results are assessed by recruiters. Information collected by them will be kept for 12 months after the end of our agreement. Each website or agency will have their own privacy policy; Details of this can be obtained directly from them.

14. Contact us

Calling us directly

When you call our main line (02920 694242), we collect Calling Line Identification (CLI) information. This is the phone number you are calling from (if it's not withheld). We hold a log of the phone number, date, time and duration of the call, but do not audio-record the call itself. We hold this information for 90 days.

We use this information to understand the demand for our services and to improve how we operate. We may also use the number to call you back if you have asked us to do so, if your call drops, or if there is a problem with the line. We may also use it to check how many calls we have received from it.

We don't audio record any calls, but we might make notes.

We also hold statistical information about the calls we receive for a number of years, but this does not contain any personal data.

Emailing us

We use Transport Layer Security (TLS) to encrypt and protect email traffic in line with government guidance on email security. Most webmail such as Gmail and Hotmail use TLS by default.

We'll also monitor any emails sent to us, including file attachments, for viruses or malicious software.

You must ensure that any email you send is within the bounds of the law.

Making a data protection rights request

To exercise your rights or raise a query about the way we handle personal data, please email us at dataprivacy@lowndesonline.co.uk

Alternatively, write to us at:

Data Privacy Team

Lowndes Halsden & Partners Ltd

Holt House, 184-190 Caerphilly Road

Birchgrove

Cardiff

CF14 4NR

Please provide as much detail as possible to help us deal with your request, such as the context in which we have processed your information and the likely dates when we processed it. We may ask you to provide your ID for identification and verification purposes. If you require any assistance, please email us at dataprivacy@lowndesonline.co.uk

Data Protection Complaints to the relevant Information Commissioner

You have the right to lodge a data protection complaint with the UK Information Commissioner's Office (ICO at https://ico.org.uk). However, we would be grateful for an opportunity to resolve matters with you in the first instance.

Changing your client contact preferences

If you would like to update your contact details or update any of your client contact preferences, please get in touch with us by phone, post or email.

As a provider of services to the public, we have a legal duty to comply with the Equality Act (2010).

This means we need to make service adjustments for anyone with a vulnerability who contacts us in any capacity, to eliminate any barriers to accessing our services.

We'll create a record of your adjustment requirements. Relevant staff can access this to ensure they are communicating with you in the required way.

Compliments

If you think there is something we have done well, please email us at dataprivacy@lowndesonline.co.uk

Our process for dealing with compliments is less formal. If you think there is something we have done well, we would be grateful to hear from you.

15. Changes to this Privacy Policy

This Privacy Policy may be updated from time to time. Please check here for the most recent information on how we process your personal data.

Last updated: October 2024