Team London Bridge

Data Protection Privacy Notice

Team London Bridge (TLB) takes your privacy very seriously. The TLB registered office is at 1 Melior Place, London, England, SE1 3SZ.

We ask that you read this Privacy policy because it gives important information about:

- the data protection principles with which TLB must comply;
- what is meant by personal information (or data) and sensitive personal information (or data);
- how we gather, use and (ultimately) delete personal information and sensitive personal information in accordance with the data protection principles;
- where more detailed privacy information can be found, e.g. about the personal information we gather and use about you, how it is used, stored and transferred, for what purposes, the steps taken to keep that information secure and for how long it is kept;
- your rights.

1 Introduction

1.1 TLB obtains, keeps and uses personal information (also referred to as data) about you for a number specific lawful purposes, as set out in this Privacy Notice.

1.2 This policy sets out how we comply with our data protection obligations and seek to protect personal information relating to our workforce. Its purpose is also to ensure that staff understand and comply with the rules governing the collection, use and deletion of personal information to which they may have access in the course of their work.

1.3 We are committed to complying with our data protection obligations, and to being concise, clear and transparent about how we obtain and use personal information relating to you, and how (and when) we delete that information once it is no longer required.

1.4 Donald Campbell is responsible for data protection compliance within TLB. If you have any questions or comments about the content of this policy or if you need further information, you should contact Donald Campbell.

2 Scope

2.1 This policy applies to information we collect about:

2.1.1 visitors to our website;

2.1.2 people who sign up for updates from the London Bridge Area;

2.1.3 individuals from local businesses that are members of the London Bridge Business Improvement District (BID);

2.1.4 people who sign up for our Deal Card;

2.1.5 people who use the security services forum;

2.1.6 people who ask to receive information about local events.

2.2 We may collect the following information about you:

2.2.1 Your name;

2.2.2 Business contact details (i.e. address, landline and mobile phone numbers, email address);

2.2.3 Occasionally we may receive information about you from other sources (such as local business contacts) which we will add to the information which we already hold about you.

2.3 We will review and update this policy regularly in accordance with our data protection obligations.

2.4 This Privacy Notice applies to all of the processes that Team London Bridge undertakes. This excludes organisations that have separate privacy policies that do not incorporate this Privacy Notice.

3 Cookies

3.1 Our website uses cookies. Cookies are text files placed on your computer to collect standard internet log information and visitor behaviour information. These cookies allow us to distinguish you from other users of the website which helps us to provide you with a positive experience when you browse our website. These cookies also allow us to improve our site.

3.2 We use cookies and collect your IP address for analytical purposes to measure visitor behaviour and to improve our website. We also use cookies to remember your preferences and the way you like to view our website.

4 Definitions

data breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information;
data subject	means the individual to whom the personal information relates;
personal information	(sometimes known as personal data) means information relating to an individual who can be identified (directly or indirectly) from that information;
processing information	means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with it;
pseudonymised	means the process by which personal information is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that the personal information cannot be attributed to an identifiable individual;
sensitive personal	(sometimes known as ‘special categories of personal data’ or ‘sensitive personal data’) means personal information about an

information individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

5 Data protection principles

5.1 TLB will comply with the following data protection principles when processing personal information:

5.1.1 we will process personal information lawfully, fairly and in a transparent manner;

5.1.2 we will collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;

5.1.3 we will only process the personal information that is adequate, relevant and necessary for the relevant purposes;

5.1.4 we will keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal information are deleted or corrected without delay;

5.1.5 we will keep personal information in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the information is processed; and

5.1.6 we will take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

6 Basis for processing personal information

6.1 In relation to any processing activity we will, before the processing starts for the first time, and then regularly while it continues:

6.1.1 review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) for that processing, i.e.:

(a) that the data subject has consented to the processing;

(b) that the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) that the processing is necessary for compliance with a legal obligation to which TLB is subject;

(d) that the processing is necessary for the protection of the vital interests of the data subject or another natural person;

(e) that the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority; or

(f) that the processing is necessary for the purposes of legitimate interests of TLB or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject—see clause 6.2 below.

6.1.2 except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose);

6.1.3 document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles;

6.1.4 include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s);

6.1.5 where sensitive personal information is processed, also identify a lawful special condition for processing that information, and document it; and

6.1.6 where criminal offence information is processed, also identify a lawful condition for processing that information, and document it.

6.2 When determining whether TLB's legitimate interests are the most appropriate basis for lawful processing, we will:

6.2.1 conduct a legitimate interests assessment (LIA) and keep a record of it, to ensure that we can justify our decision;

6.2.2 if the LIA identifies a significant privacy impact, consider whether we also need to conduct a data protection impact assessment (DPIA);

6.2.3 keep the LIA under review, and repeat it if circumstances change; and

6.2.4 include information about our legitimate interests in our relevant privacy notice(s).

6.3 We will typically collect and use this information for the following purposes:

6.3.1 for the performance of a contract with you, or to take steps to enter into a contract. This applies if you have signed up as a member of BID and sign up for the Deal Card;

6.3.2 for compliance with any legal obligation we are required to fulfil; and

6.3.3 for the purposes of our legitimate interests or those of a third party (such as your PLA), but only if these are not overridden by your interests, rights or freedoms. We have a legitimate interest to encourage networking between businesses in the London Bridge Area by sharing updates on security, news and events in the area.

7 How we may share the information

7.1 We will not share your personal data with third parties unless you have given us permission to do this. We will also send you marketing information but you are able to opt out of this by emailing info@teamlondonbridge.co.uk.

7.2 We will not transfer any personal data outside the European Economic Area (EEA), which comprises the countries in the European Union and Iceland, Liechtenstein and Norway.

8 Special Category Data

8.1 Special Category Data is sometimes referred to as 'sensitive personal data'.

8.2 TLB does not process and special category data but will send you an updated privacy policy if this changes.

9 Data protection impact assessments (DPIAs)

9.1 Where processing is likely to result in a high risk to an individual's data protection rights (e.g. where TLB is planning to use a new form of technology), we will, before commencing the processing, carry out a DPIA to assess:

9.1.1 whether the processing is necessary and proportionate in relation to its purpose;

9.1.2 the risks to individuals; and

9.1.3 what measures can be put in place to address those risks and protect personal information.

9.2 Before any new form of technology is introduced, the manager responsible should therefore contact Donald Campbell in order that a DPIA can be carried out.

9.3 During the course of any DPIA, TLB will seek the advice of Donald Campbell and any other relevant stakeholders.

10 Documentation and records

10.1 We will keep written records of processing activities which are high risk, i.e. which may result in a risk to individuals' rights and freedoms or involve sensitive personal information or criminal records information, including:

10.1.1 the purposes of the processing;

10.1.2 a description of the categories of individuals and categories of personal data;

10.1.3 categories of recipients of personal data;

10.1.4 where possible, retention schedules; and

10.1.5 where possible, a description of technical and organisational security measures.

10.2 As part of our record of processing activities we document, or link to documentation, on:

10.2.1 information required for privacy notices;

10.2.2 records of consent;

10.2.3 controller-processor contracts;

10.2.4 the location of personal information;

10.2.5 DPIAs; and

10.2.6 records of data breaches.

10.3 If we process sensitive personal information or criminal records information, we will keep written records of:

10.3.1 the relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose;

10.3.2 the lawful basis for our processing; and

10.3.3 whether we retain and erase the personal information in accordance with our policy document and, if not, the reasons for not following our policy.

10.4 We will conduct regular reviews of the personal information we process and update our documentation accordingly. This may include:

10.4.1 carrying out information audits to find out what personal information TLB holds;

10.4.2 reviewing our policies, procedures, contracts and agreements to address areas such as retention, security and data sharing.

10.5 We document our processing activities in electronic form so we can add, remove and amend information easily.

11 Privacy notice

11.1 TLB will issue privacy notices from time to time, informing you about the personal information that we collect and hold relating to you, how you can expect your personal information to be used and for what purposes.

11.2 We will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

12 Individual rights

12.1 You (in common with other data subjects) have the following rights in relation to your personal information:

12.1.1 to be informed about how, why and on what basis that information is processed which is the purpose of this Privacy Notice;

12.1.2 to obtain confirmation that your information is being processed and to obtain access to it and certain other information, by making a subject access request;

12.1.3 to have data corrected if it is inaccurate or incomplete;

12.1.4 to have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as ‘the right to be forgotten’);

12.1.5 to restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased); and

12.1.6 to restrict the processing of personal information temporarily where you do not think it is accurate.

12.2 If you wish to exercise any of the rights in paragraphs 12.1.3 to 12.1.6, please contact Donald Campbell.

13 Information security

13.1 TLB will use appropriate technical and organisational measures to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. These may include:

13.1.1 making sure that, where possible, personal information is pseudonymised or encrypted;

13.1.2 ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

13.1.3 ensuring that, in the event of a physical or technical incident, availability and access to personal information can be restored in a timely manner; and

13.1.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

13.2 Where TLB uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. In particular, contracts with external organisations must provide that:

13.2.1 the organisation may act only on the written instructions of TLB;

13.2.2 those processing the data are subject to a duty of confidence;

13.2.3 appropriate measures are taken to ensure the security of processing;

13.2.4 sub-contractors are only engaged with the prior consent of TLB and under a written contract;

13.2.5 the organisation will assist TLB in providing subject access and allowing individuals to exercise their rights in relation to data protection;

13.2.6 the organisation will assist TLB in meeting its obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments;

13.2.7 the organisation will delete or return all personal information to TLB as requested at the end of the contract; and

13.2.8 the organisation will submit to audits and inspections, provide TLB with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell TLB immediately if it is asked to do something infringing data protection law.

13.3 Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval of its terms by Donald Campbell.

14 Storage and retention of personal information

14.1 Personal information will be kept securely at the offices of TLB.

14.2 Personal information should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained. Where there is any uncertainty, staff should consult Donald Campbell.

14.3 Personal information (and sensitive personal information) that is no longer required will be put beyond use from our information systems and any hard copies will be destroyed securely.

15 Data breaches

15.1 A data breach may take many different forms, for example:

15.1.1 loss or theft of data or equipment on which personal information is stored;

15.1.2 unauthorised access to or use of personal information either by a member of staff or third party;

15.1.3 loss of data resulting from an equipment or systems (including hardware and software) failure;

15.1.4 human error, such as accidental deletion or alteration of data;

15.1.5 unforeseen circumstances, such as a fire or flood;

15.1.6 deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and

15.1.7 'blagging' offences, where information is obtained by deceiving the organisation which holds it.

15.2 TLB will:

15.2.1 make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals; and

15.2.2 notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

16 International transfers

16.1 TLB will not transfer personal information outside the European Economic Area (EEA), which comprises the countries in the European Union and Iceland, Liechtenstein and Norway.

17 Training

TLB will ensure that staff are adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal information, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

18 Consequences of failing to comply

18.1 TLB takes compliance with this policy very seriously. Failure to comply with the policy:

18.1.1 puts at risk the individuals whose personal information is being processed; and

18.1.2 carries the risk of significant civil and criminal sanctions for the individual and TLB; and

18.1.3 may, in some circumstances, amount to a criminal offence by the individual.

18.2 If you have any questions or concerns about anything in this policy, do not hesitate to contact Donald Campbell.

18.3 We hope that Donald Campbell can resolve any query or concern you raise about our use of your information. If not, contact the Information Commissioner at ico.org.uk/concerns/ or telephone: 0303 123 1113 for further information about your rights and how to make a formal complaint.