

LBA BOOKS PRIVACY NOTICE

1. INTRODUCTION

- 1.1. This privacy notice (**Privacy Notice**) sets out the ways in which we, LBA Books (**we, us, our**), collect and use your personal data (your personal information) in connection with our business. It also explains what rights you have to access or change your personal data.
- 1.2. Our website is not intended for children. We do not knowingly collect or maintain the personal information of children under the age of 13 . If you are under the age of 13, please do not access our website at any time or in any manner. We will take appropriate steps to delete the personal information of persons under the age of 13 .

2. ABOUT US

- 2.1. We are a company registered in England under company number 5304335, with our registered address as set out below.
- 2.2. You can contact us as follows:

FAO: Office Manager

Address: LBA Books, 91 Great Russell Street, London, WC1B 3PS, UK

Email: info@lbabooks.com

3. INFORMATION WE MAY COLLECT ABOUT YOU

3.1. Information that you provide to us.

- 3.1.1. We will collect any information that you provide to us when you:
 - (a) make an enquiry over the phone, by email, in writing or on our website;
 - (b) submit manuscripts or other content to us by post, email or via our website;
 - (c) enter into a contract with us to represent you;
 - (d) submit an application to a job vacancy;
 - (e) 'follow', 'like', post to or interact with our social media accounts, including Facebook, LinkedIn, Twitter, Pinterest, Instagram and Google+.
- 3.1.2. The information you provide to us will include (depending on the circumstances):
 - (a) **Identity and contact data:** Title, names, addresses, email addresses and phone numbers;
 - (b) **Financial and contract data:** If we represent you, you may also provide us with your bank details, VAT and tax information, immigration and residency information, your existing contracts (and related correspondence) with publishers or other licensees of your work;

- (c) **Employment and background data:** If you are submitting a manuscript for review or a job application, you may also provide additional information about your academic and work history, qualifications, skills, projects and research that you are involved in, references, proof of your entitlement to work in the UK, your national security number, your passport or other identity document details, your current level of remuneration (including benefits), and any other such similar information that you may provide to us.

3.2. Information we collect about you:

- (a) **Information contained in correspondence:** We will collect any information contained in any correspondence between us. For example, if you contact us using a query button on our website or by email, post or telephone, we may keep a record of that correspondence;

3.3. Information we receive from third parties

3.3.1. In certain circumstances, we will receive information about you from third parties. For example:

- (a) **Employers, recruitment agencies and referees:** If you are a job applicant we may contact your recruiter, current and former employers and/or referees, who may be based inside or outside the EU, to provide information about you and your application;
- (b) **Publishers and other licensees of your work:** If we represent you, you will normally authorise us to receive information about you from your publishers and other licensees such as information about your contracts, performance, royalties and other payments;
- (c) **Third parties who can verify submitted information:** If you submit a manuscript to us for our review, we may use third party providers to verify the information that you provide to us in connection with that submission. For example, we will use third-party databases or websites (including but not limited to Google and Amazon) to confirm your publication history;
- (d) **Website security:** We will collect information from our website security service partners who are based inside the EU, about any misuse to the website, for instance, the introduction of viruses, Trojans, worms, logic bombs, website attacks or any other material or action that is malicious or harmful.

3.3.2. We might also receive information about you from third parties if you have indicated to such third party that you would like to hear from us.

4. HOW WE USE INFORMATION ABOUT YOU AND RECIPIENTS OF YOUR INFORMATION

4.1. We will use your information for the purposes listed below either on the basis of:

- 4.1.1. performance of your contract with us and the provision of our services to you;
- 4.1.2. your consent (where we request it);

- 4.1.3. where we need to comply with a legal or regulatory obligation; or
- 4.1.4. our legitimate interests or those of a third party (see paragraph 4.3 below).

4.2. We use your information for the following purposes:

- 4.2.1. **Relationship management:** to manage our relationship with you, which will include notifying you about changes to our terms of use or privacy policy (on the basis of performing our contract with you, to comply with our legal obligations and on the basis of our legitimate interests to keep our records updated and study how our website and services are used);
- 4.2.2. **To conduct business with you:** to contact you and manage and facilitate our business relationship with you, including (if we represent you) the administration of your contract with us (including administration of any contracts with third parties when we represent you on such contracts) (on the basis of our legitimate interests in maintaining our business contacts; on the basis of performing our contract with you);
- 4.2.3. **Recruitment:** to process any job applications you submit to us, whether directly or via an agent or recruiter including sharing this with our third party recruitment agency (on the basis of our legitimate interest to recruit new employees or contractors);
- 4.2.4. **Social media interactions:** to interact with users on social media platforms including Facebook, LinkedIn, Twitter, Pinterest, Instagram and Google+, for example, responding to comments and messages, posting, 'retweeting' and 'liking' posts (on the basis of our legitimate interest in promoting our brand and communicating with interested individuals);
- 4.2.5. **Fraud and unlawful activity detection:** to protect, investigate, and deter against fraudulent, unauthorised, or illegal activity, including identity fraud (on the basis of our legitimate interests to operate a safe and lawful business or where we have a legal obligation to do so);
- 4.2.6. **Compliance with policies, procedures and laws:** to enable us to comply with our policies and procedures and enforce our legal rights, or to protect the rights, property or safety of our employees and share your information with our technical and legal advisors (on the basis of our legitimate interests to operate a safe and lawful business or where we have a legal obligation to do so).

4.3 As outlined above, in certain circumstances we may use your personal information to pursue legitimate interests of our own or those of third parties. Where we refer to using your information on the basis of our "legitimate interests", we mean our legitimate business interests in conducting and managing our business and our relationship with you, including the legitimate interest we have in:

- 4.3.1 personalising, enhancing, modifying or otherwise improving the services and/or communications that we provide to you;
- 4.3.2 detecting and preventing fraud and operating a safe and lawful business;
- 4.3.3 improving security and optimisation of our network, sites and services.

4.3. Where we use your information for our legitimate interests, we make sure that we take into account any potential impact that such use may have on you. Our legitimate interests don't

automatically override yours and we won't use your information if we believe your interests should override ours unless we have other grounds to do so (such as your consent or a legal obligation). If you have any concerns about our processing please refer to details of "Your Rights" in paragraph 9 below.

5. WHO WE MIGHT SHARE YOUR INFORMATION WITH

- 5.1. In connection with the purposes and on the lawful grounds described above and in addition to the recipients of your information as described above, we will share your personal information when relevant with third parties such as:
 - 5.1.1. **Our service providers:** third parties we work with to deliver our business (including, for example, hosting or operating the website and our databases and site analytics);
 - 5.1.2. **Publishers, licensees, sub-agents, advisors and service companies:** if we represent you, any publishers or other licensees of your work (or prospective publishers and licensees) as well as sub- or co-agents, advisors (such as your solicitor or accountant) and editorial service providers, where applicable.
 - 5.1.3. **Prospective sellers and buyers of our business:** any prospective seller or buyer of such business or assets, only in the event that we decide to sell or buy any business or assets; and
 - 5.1.4. **Other third parties (including professional advisers):** any other third parties (including legal or other advisors, regulatory authorities, HMRC, courts, law enforcement agencies and government agencies) where necessary to enable us to enforce our legal rights, or to protect the rights, property or safety of our employees or where such disclosure may be permitted or required by law.
- 5.2. We require third parties to maintain appropriate security to protect your information from unauthorised access or processing.

6. COOKIES

- 6.1. We use cookies to ensure that you get the most out of our website. Cookies are small amounts of information in the form of text files which we store on the device you use to access our website. Cookies allow us to monitor your use of the software and simplify your use of the website.
- 6.2. If you do not wish for cookies to be installed on your device, you can change the settings on your browser or device to reject cookies. For more information about how to reject cookies using your internet browser settings please consult the "Help" section of your internet browser (or alternatively visit <http://www.aboutcookies.org>). Please note that, if you do set your Internet browser to reject cookies, you may not be able to access all of the functions of the website.
- 6.3. Our website may contain content and links to other sites that are operated by third parties that may also operate cookies. We don't control these third party sites or cookies and this Privacy Notice does not apply to them. Please consult the terms and conditions and Privacy Notice of the relevant third party site to find out how that site collects and uses your information and to establish whether and for what purpose they use cookies.

7. HOW WE LOOK AFTER YOUR INFORMATION AND HOW LONG WE KEEP IT FOR

- 7.1. We operate a policy of "privacy by design" by looking for opportunities to minimise the amount of personal information we hold about you. We use appropriate technological and operational

security measures to protect your information against any unauthorised access or unlawful use, such as:

- 7.1.1. ensuring the physical security of our offices, warehouses or other sites;
 - 7.1.2. ensuring the physical and digital security of our equipment and devices by using appropriate password protection;
 - 7.1.3. maintaining a data protection policy for, and delivering data protection training to, our employees; and
 - 7.1.4. limiting access to your personal information to those in our company who need to use it in the course of their work.
- 7.2. We will retain your information for as long as is necessary to provide you with the services that you have requested from us or for as long as we reasonably require to retain the information for our lawful business purposes, such as for the purposes of exercising our legal rights or where we are permitted to do. We operate a data retention policy and look to find ways to reduce the amount of information we hold about you and the length of time that we need to keep it. For example,
- 7.2.1. we retain information relating to submissions and website user queries for up to 5 years; and
 - 7.2.2. we destroy unpublished manuscripts and related correspondence after up to 5 however we may permanently keep a log recording brief details of these in the event of a legal claim.

8. INTERNATIONAL TRANSFERS OF YOUR INFORMATION

- 8.1. Our company is located in the UK.
- 8.2. Some of our external third parties are based outside the European Economic Area (EEA) so their processing of your personal data will involve a transfer of data outside the EEA.
- 8.3. Whenever we transfer your personal data out of the EEA, we ensure a similar degree of protection is afforded to it by ensuring at least one of the following transfer solutions are implemented:
 - (a) We will only transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data by the European Commission. For further details, see [European Commission: Adequacy of the protection of personal data in non-EU countries](#);
 - (b) Where we use certain service providers, we may use specific contracts approved by the European Commission which give personal data the same protection it has in Europe. For further details, [European Commission: Model contracts for the transfer of personal data to third countries](#); and
 - (c) Where we use providers based in the US, we may transfer data to them if they are part of the Privacy Shield which requires them to provide similar protection to personal data shared between the Europe and the US. For further details, see [European Commission: EU-US Privacy Shield](#).

- 8.4. A list of the countries outside of the EEA to which we may transfer your personal information is available [here](#).
- 8.5. Please contact us using the contact details at the top of this Privacy Notice if you want further information on the specific mechanism used by us when transferring your personal data out of the EEA.

9. YOUR RIGHTS TO THE INFORMATION WE HOLD ABOUT YOU

- 9.1. You have certain rights in respect of the information that we hold about you, including:
- 9.1.1. the right to be informed of the ways in which we use your information, as we seek to do in this Privacy Notice;
 - 9.1.2. the right to ask us not to process your personal data for marketing purposes;
 - 9.1.3. the right to request access to the information that we hold about you;
 - 9.1.4. in certain circumstances, the right to receive a copy of any information we hold about you (or request that we transfer this to another service provider) in a structured, commonly-used, machine readable format
 - 9.1.5. the right to request that we correct or rectify any information that we hold about you which is out of date or incorrect;
 - 9.1.6. the right to withdraw your consent for our use of your information in reliance of your consent (refer to paragraph 4 to see when we are relying on your consent), which you can do by contacting us using any of the details at the top of this Privacy Notice;
 - 9.1.7. the right to object to our using your information on the basis of our legitimate interests (refer to paragraph 4 above to see when we are relying on our legitimate interests) (or those of a third party)) and there is something about your particular situation which makes you want to object to processing on this ground;
 - 9.1.8. in certain circumstances, the right to ask us to limit or stop processing information about you, or erase information we hold about you; and
 - 9.1.9. the right to lodge a complaint about us to the UK Information Commissioner's Office (<https://ico.org.uk/>), as well as with the relevant authority in your country of work or residence.
- 9.2. Please note that we may need to retain certain information for our own record-keeping and research purposes.

How to exercise your rights

- 9.3. You may exercise your rights above by contacting us using the details in paragraph 2 of this Privacy Notice, or in the case of preventing processing for marketing activities also by checking certain boxes on forms that we use to collect your data to tell us that you don't want to be involved in marketing [or by updating your marketing preferences via your account with us].
- 9.4. You may contact us via the details at the top of this Privacy Notice if you wish to action any of these additional rights and we will comply with your requests unless we have a lawful reason not to do so.

What we need from you to process your requests

- 9.5. We may need to request specific information from you to help us confirm your identity and to enable you to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.
- 9.6. You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances. We will try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

10. THIRD-PARTY LINKS

- 10.1. The website may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements. When you leave our website, we encourage you to read the privacy notice of every website you visit.

11. CHANGES TO THIS PRIVACY NOTICE AND YOUR DUTY TO INFORM US OF CHANGES

- 11.1. We may make changes to this Privacy Notice from time to time. We will post any changes to our site, or notify you of any material changes by e-mail.
- 11.2. It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your relationship with us by updating your profile account information or contacting us via the contact details at the top of this Privacy Notice.

This Privacy Notice was updated on 24.05.18.

Appendix – Glossary of Commonly Used Data Protection Terms

Article 29 Working Party	a European advisory body made up of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisory and the European Commission. It provides guidelines on the GDPR and data protection matters.
Anonymisation	where Personal Data is processed in such a way that the data can no longer be attributed to a specific Data Subject. When done properly, anonymisation places data outside the scope of the GDPR.
Automated Decision Making	these are decisions which are made following Processing of Personal Data solely by automatic means, (i.e. where no humans are involved in the decision-making process). An example would an individual applying for a personal loan online, then being given a yes/no decision based solely on an automated credit search algorithm.
Consent	defined in the GDPR as “any freely given, specific, informed and unambiguous indication of the Data Subject’s wishes by which he or she by statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her”. Silent, implicit indications of consent, such as leaving pre-ticked web form boxes ticked, will not be sufficient for Consent under the GDPR. Note that “informed” Consent requires that the Data Subject has received all the information about the Processing, in a format intelligible to them so they can make an informed decision about their rights (this is a particular challenge for children’s consent). Some Processing requires the Data Subject’s “explicit Consent”.
Data Subject	means a living person who is the subject of Personal Data. In your business, Data Subjects will likely include your employees, authors, suppliers, website users etc.
Data Subject Rights	the rights that Data Subjects have under the GDPR including the rights in certain circumstances to access information Data Controllers have about them, stop or restrict Processing about them, to withdraw Consent and complain to a Supervisory Authority.

Data Controller	the living person or legal entity which, alone or jointly with others, determines the purposes for which and means of Processing of Personal Data. For example, your business is a Data Controller in respect of the Personal Data it Processes about its employees, customers, authors, suppliers etc (note that the individual employees of the business are not separate Data Controllers).
Data Processor	the living person or legal entity which processes Personal Data on behalf of a data controller. You might use Data Processors in your business to host your website, send email marketing on your behalf etc.
Data Protection Bill	the version of the UK's Data Protection Bill first read before Parliament on 13 September 2017, which is set to replace the Data Protection Act 1998, and which is set to implement parts of the GDPR specific to the UK;
DPA (Data Protection Act)	the Data Protection Act 1998, the UK's existing data protection law;
DPIA (Data Protection Impact Assessment)	known under the existing data protection laws as a "privacy impact assessment" this tool can help you determine if your Processing will affect the rights of any Data Subjects (and how to mitigate that risk). It is a required process in some instances under the GDPR.
DPO (Data Protection Officer)	under the GDPR companies must appoint a DPO in certain circumstances (such as when they are Processing on a large scale or undertaking regular or systematic monitoring).
EEA	European Economic Area. This is the region to which the GDPR primarily applies. Sending or making Personal Data accessible outside of the EEA requires special considerations (see Transfer below).
EU-US Privacy Shield	the framework for transatlantic exchanges of Personal Data for commercial purposes between the European Union and the United States under which US companies can certify compliance.
GDPR	the General Data Protection Regulation (EU) 2016/679. There is an online, searchable version of the GDPR text here: https://gdpr-info.eu/ .

ICO

the UK's data protection regulator, the Information Commissioner's Office. The ICO has GDPR guidance and resources here; <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/>.

Lawful Grounds

Processing may take place only when there is a lawful reason to do so. Commonly referred to as the "six lawful grounds" these are specified in the GDPR as: (i) when the Data Subject has given their Consent for one or more specified purposes; or when the Processing is necessary (ii) for performance of or entering into a contract with or at the request of the Data Subject; (iii) for the Data Controller to comply with a legal obligation; (iv) to protect the vital interests (generally a life-or-death situation) of the Data Subject or another person; (v) for performance of a task in the public interest; (vi) for the purposes of Legitimate Interests (see below). It is important to remember that each Lawful Ground is equally valid. Data Controllers must identify the appropriate Lawful Ground for their Processing and specify these in the Privacy Notice.

Legitimate Interests

one of the Lawful Grounds for data Processing under the GDPR. Legitimate Interests refers to your interests in conducting and managing your business and your relationship with Data Subjects but it can only apply if you have made an assessment and determined that the rights and freedoms of Data Subjects are not overridden. It can be a tricky concept to apply but it is helpful to consider the nature of your relationship with the Data Subject and whether the kind of Processing you envisage would be within their reasonable expectations.

Model Contract Clauses

the standard contractual clauses approved by the European Commission as guaranteeing appropriate safeguards under European data protection laws for Personal Data transferred to entities based outside of the EEA.

Personal Data

any information relating to an identified or identifiable natural person who can be identified, directly, or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; there is no exhaustive list of what constitutes Personal Data so it is important to remember that this broad definition may include digital identifiers (such as social media handles) as well as correspondence about (including opinions of) individuals.

Personal Data Breach

a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data.

Phishing

the attempt to obtain confidential or sensitive information such as usernames and passwords, often for malicious reasons, by disguising as a trustworthy entity in an electronic communication. Phishing is an increasingly common cause of Personal Data Breaches.

Portability

the right for an individual to require a Data Controller to give them back a copy of the Personal Data they previously provided or send this data to another organisation so that they can reuse it. The Personal Data has to be provided in a commonly used, machine-readable format and only when the Personal Data has been provided by the Data Subject with their Consent or as part of a contract. This is commonly used in the banking and utilities sectors when individuals switch providers.

Privacy Notice

a common way for Data Controllers to inform Data Subjects about how, when, where and why their Personal Data is being Processed. This is commonly hosted on businesses' websites.

Profiling

any form of automated processing of Personal Data intended to evaluate certain personal aspects of an individual. These aspects can include analysing/predicting someone's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movement. You may be using Profiling in your business to serve marketing and advertising messages. If so, ensure that you describe this Profiling in your Privacy Notice.

Process(ing)

obtaining, recording or holding Personal Data or carrying out any operation or set of operations in relation to it and includes the organisation, retrieval, use of the Personal Data, disclosure, erasure or destruction of the Personal Data. This is a very broad definition and it is important to remember that simply storing Personal Data in any accessible/ordered/structured way will be a form of Processing.

Pseudonymisation

similar to anonymisation, but reversible. This is where Personal Data is processed in such a way that the data can no longer be attributed to a specific Data Subject without the use of 'additional information'. The additional information must be kept separately and be subject to certain measures which ensure that it isn't unduly used to reverse the process. Pseudonymisation is a way to minimise the risk of a Personal Data Breach.

Special Categories of Data /Sensitive Personal Data

Personal Data revealing racial or ethnic origin, political opinions, revealing religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purposes of uniquely identifying a natural person, or concerning health, concerning sexual orientation. Special standards apply to the Processing of Special Categories of Data including: you may only Process this when you have the Data Subject's explicit Consent or it is necessary for employment obligations or where the vital interests of the Data Subject or others are at risk (and the Data Subject cannot give Consent).

Supervisory Authority

a supervisory authority of a European Member State responsible for monitoring the application of data protection laws, which for the UK is the ICO.

Transfer

a transfer of Personal Data will occur when Personal Data is sent, shared, stored, accessed or otherwise used by a third party (whether an individual or a company) in another country or jurisdiction. There are no restrictions of transfers of personal data within the EEA; however safeguards (or "transfer solutions") must be put in place where Personal Data is transferred outside of the EEA to ensure a level of protection for that Personal Data equivalent to the GDPR. Safeguards that may be applicable include the EU-US Privacy Shield and the Model Contract Clauses.

