



# Privacy Policy and GDPR

## **POLICY STATEMENT**

Blackout Limited needs to collect personal information to effectively and compliantly carry out our everyday business functions and activities and to provide the products and services defined by our business type. Such data is collected from employees, freelancers, customers, suppliers and clients and includes (*but is not limited to*), name, address, email address, telephone numbers, date of birth, proof of eligibility to work, National Insurance number, private and confidential information, sensitive information and bank details.

In addition, we may be required to collect and use certain types of personal information to comply with the requirements of the law and/or regulations, however we are committed to collecting, processing, storing and destroying all information in accordance with the General Data Protection Regulation, UK data protection laws and specific data protection codes of conduct (*herein collectively referred to as 'the GDPR'*).

Blackout Limited has developed policies, procedures, controls and measures to ensure maximum and continued compliance with the GDPR and its principles, including staff training, procedure documents, audit measures and assessments. Ensuring and maintaining the security and safety of personal and/or special category data belonging to the individuals with whom we deal is paramount to our company ethos and Blackout Limited adheres to the GDPR and its associated principles in every process and function.

*We are proud to operate a 'Privacy by Design' approach and aim to be proactive, not reactive; assessing changes and their impact from the start and designing systems and processes to protect personal information at the core of our business.*

## **THE GDPR PRINCIPLES & OBJECTIVES**

We are committed to ensuring that all personal data obtained and processed by Blackout Limited is done so in accordance with the GDPR and its principles, along with any associated regulations and/or codes of conduct laid out by the Supervisory Authority and local law. We are dedicated to ensuring the safe, secure, ethical and transparent use of all personal data and to uphold the highest standards of data processing.

Blackout Limited uses the below objectives to meet the regulatory requirements of the GDPR and to develop measures, procedures and controls for maintaining and ensuring compliance.

*Blackout Limited ensures that: –*

- We protect the rights of individuals with regard to the personal information known and held about them by Blackout Limited in the course of our business.
- We develop, implement and maintain a data protection policy, procedure, audit plan and training program for compliance with the GDPR.
- Every business practice, task and process carried out by Blackout Limited, is monitored for compliance with the GDPR and its principles.
- Data is only obtained, processed or stored when we have met the lawfulness of processing requirements
- We record consent at the time it is obtained and evidence such consent to the Supervisory Authority where requested. (oral or written)
- All relevant employees (including new starters) are competent and knowledgeable about their GDPR obligations and are provided with training in the GDPR principles, regulations and how they apply to our business and services.
- Internal and external customers feel secure when providing us with personal information and know that it will be handled in accordance with their rights under the GDPR.
- We maintain a continuous program of monitoring, review and improvement with regards to compliance with the GDPR and to identify gaps and non-compliance before they become a risk.
- We monitor the Supervisory Authority, European Data Protection Board (EDPB) and GDPR news to stay abreast of updates, notifications and additional requirements.
- We have a Complaint Handling and Breach Incident Policy to ensure controls and procedures are in place for identifying, investigating, reviewing and reporting any breaches or complaints with regards to data protection.
- We have appointed a Compliance Officer who takes responsibility for the overall supervision and implementation of the GDPR and its principles and remains informed on the regulations and how they relate to Blackout Limited
- We have a dedicated Audit & Monitoring Program in place to perform regular checks and assessments on how the personal data we process is obtained, used, stored and shared. The audit program utilises this policy and procedure and the GDPR itself to ensure continued compliance.
- We provide clear lines of reporting and supervision with regard to data protection compliance.

- Develop and maintain strict and robust DPA procedures, controls and measures to ensure continued compliance with the Act.
- We store and destroy all personal information, in accordance with the GDPR timeframes and requirements.
- Any information provided to an individual in relation to personal data held or used about them, will be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
- Employees are aware of their own rights under the GDPR and are provided with the Article 13 & 14 information disclosures

### **THE INFORMATION COMMISSIONERS OFFICE (ICO)**

Blackout Limited are registered with ICO and appear on the Data Protection Register as a controller and processor of personal information.

Our Data Protection Registration Number is **PZ796034X**

### **DATA RETENTION & DISPOSAL**

Blackout Limited have defined procedures for adhering to the retention periods as set out by the relevant laws, contracts and business requirements, as well as adhering to the GDPR requirement to hold and process personal information only for as long as is necessary. All personal data is disposed of in a way that protects the rights and privacy of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion) and prioritizes the protection of the personal data at all times.

Please refer to our Data Retention Policy for full details on our retention, storage, periods and destruction processes.

### **CONSENT & THE RIGHT TO BE INFORMED**

The collection of personal and sometimes special category data is a fundamental part of the services offered by Blackout Limited and we, therefore, have specific measures and controls in place to ensure that we comply with the conditions for consent under the GDPR.

The GDPR defines consent as; 'Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'.

*Where processing is based on consent, Blackout Limited have reviewed and revised all consent mechanisms to ensure that:*

- Consent requests are transparent, using plain language and is void of any illegible terms, jargon or extensive legal terms
- It is freely given, specific and informed, as well as being an unambiguous indication of the individual's wishes
- Consent is always given by a statement or a clear affirmative action (positive opt-in) which signifies agreement to the processing of personal data
- Consent mechanisms are upfront, clear, granular (in fine detail) and easy to use and understand
- Pre-ticked, opt-in boxes are never used
- Where consent is given as part of other matters (i.e. terms & conditions, agreements, contracts), we ensure that the consent is separate from the other matters and is not be a precondition of any service (unless necessary for that service)
- Along with our company name, we also provide details where possible of any other third party who will use or rely on the consent (or gain consent later in the process if details are required to be shared)
- Consent is always verifiable, and we have controls in place to ensure that we can demonstrate consent in every case
- We keep detailed records of consent and can evidence at a minimum: that the individual has consented to the use and processing of their personal data; that the individual has been advised of our company name and any third party using the data; what the individual was told at the time of consent; how and when consent was obtained
- We have ensured that withdrawing consent is as easy, clear and straightforward as giving it and is available through written request such as email, or verbally when speaking with one of our team.
- Consent withdrawal requests are processed immediately and without detriment
- Controls and processes have been developed and implemented to refresh consent
- For special category data, the consent obtained is explicit (stated clearly and in detail, leaving no room for confusion or doubt) with the processing purpose(s) always being specified

## **THE RIGHT OF ACCESS**

We have ensured that appropriate measures have been taken to provide information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 (collectively, The Rights of Data Subjects),

relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Such information is provided free of charge and is in writing, or by other means where authorised by the data subject and with prior verification as to the subject's identity (i.e. verbally, electronically).

Information is provided to the data subject at the earliest convenience, but at a maximum of 30 days from the date the request was received. Where the retrieval or provision of information is particularly complex or is subject to a valid delay, the period may be extended by two further months where necessary. However, this is only done in exceptional circumstances and the data subject is kept informed in writing throughout the retrieval process of any delays or reasons for delay.

Where we do not comply with a request for data provision, the data subject is informed within 30 days of the reason(s) for the refusal and of their right to lodge a complaint with the Supervisory Authority.

## **THE RIGHT TO ERASURE**

Also, known as 'The Right to be Forgotten', Blackout Limited complies fully with Article 5(e) and ensures that personal data which identifies a data subject, is not kept longer than is necessary for the purposes for which the personal data is processed. All personal data obtained and processed by Blackout Limited is categorised when assessed by the information audit and is either given an erasure date or is monitored so that it can be destroyed when no longer necessary.

These measures enable us to comply with a data subjects right to erasure, whereby an individual can request the deletion or removal of personal data where there is no compelling reason for its continued processing. Whilst our standard procedures already remove data that is no longer necessary, we still follow a dedicated process for erasure requests to ensure that all rights are complied with and that no data has been retained for longer than is needed.

- 1.The request is allocated to the Compliance Manager and recorded on the Erasure Request Register
- 2.The Compliance Manager locates all personal information relating to the data subject and reviews it to see if it is still being processed and is still necessary for the legal basis and purpose it was originally intended
- 3.The request is reviewed to ensure it complies with one or more of the grounds for erasure: –
  - a. the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed
  - b. the data subject has withdrawn consent on which the processing is based and where there is no other legal ground for the processing

- c. the data subject objects to the processing and there are no overriding legitimate grounds for the processing
- d. the personal data has been unlawfully processed
- e. the personal data must be erased for compliance with a legal obligation
- f. the personal data has been collected in relation to the offer of information society services to a child

4.If the erasure request complies with one of the above grounds, it is erased within 30 days of the request being received

5.The Compliance Manager writes to the data subject and notifies them in writing that the right to erasure has been granted and provides details of the information erased and the date of erasure

6.Where Blackout Limited has made any of the personal data public and erasure is granted, we will take every reasonable step and measure to remove public references, links and copies of data and to contact related controllers and/or processors and inform them of the data subjects request to erase such personal data

If for any reason, we are unable to act in response to a request for erasure, we always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy. Such refusals to erase data include: –

- Exercising the right of freedom of expression and information
- Compliance with a legal obligation for the performance of a task carried out in the public interest
- For reasons of public interest in the area of public health
- For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in so far as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing
- For the establishment, exercise or defence of legal claims

### **DUTIES OF THE COMPLIANCE OFFICER**

The Compliance Officer has assumed the below duties in compliance with GDPR Article 39: –

- To inform and advise Blackout Limited and any employees carrying out processing, of their obligations pursuant to the GDPR, the Supervisory Authorities guidelines and any associated data protection provisions
- To monitor compliance with the GDPR, associated data protection provisions and Blackout Limited's own data protection policies, procedures and objectives
- To oversee the assignment of responsibilities, awareness-raising and training of staff involved in processing operations

- To carry out and review audits of the above-mentioned policies, procedures, employee duties and training programs
- To cooperate with the Supervisory Authority where required
- To act as the point of contact for the Supervisory Authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter
- In accordance with Article 35 (type of processing is likely to result in a high risk to the rights and freedoms of natural persons), the Compliance Manager will provide advice where requested with regards to any data protection impact assessment and monitor its performance pursuant
- Have due regard to, and be aware of, the risk associated with processing operations, considering the nature, scope, context and purposes of processing

**Designated Compliance Officer**

NAME: Henrietta Hillman

POSITION: HR Manager

ADDRESS: 280 Western Road, London SW19 2QA

EMAIL: [henriettah@blackout.co.uk](mailto:henriettah@blackout.co.uk)

TEL: 020 8687 8400