C. BASTOCK (CONTRACTS) LTD

General Data Protection Regulation (GDPR) Statement

Introduction
This is the GDPR Statement for C. Bastock (Contracts) Ltd, referred to in this statement as 'We'. The EU General Data Protection Regulation (GDPR) came into force across the European Union on 25th May 2018, to meet the requirements of the digital age and affording individuals stronger, more consistent rights to access and control their personal information.

Our Commitment
We are committed to ensuring the security and protection of the personal information that we process and to provide a compliant and consistent approach to data protection. GDPR enabled us to build on and expand our existing robust and effective systems, which comply with existing law and abide by data protection principles.

We have developed a data protection regime that is effective, fit for purpose and demonstrates an understanding of and appreciation for GDPR Regulation. Our objectives for GDPR compliance have been summarised in this statement and include the development and implementation of new data protection roles, policies, procedures, controls and measures to ensure maximum and ongoing compliance.

GDPR Compliance
We already have a consistent level of data protection and security across our company. Our preparation for GDPR Regulation included a comprehensive Information Audit to identify and assess:

- What personal information we hold
- Where it comes from
- How and why it is processed
- If and to whom it is disclosed

As a result of this audit we implemented new physical, electronic and managerial data protection procedures to meet the requirements and standards of the GDPR and any relevant data protection laws.

Data Protection:
Our focus is on privacy by design and the rights of our individual clients and service providers. Accountability and governance measures are in place to ensure that we understand, adequately disseminate and evidence our obligations and responsibilities. We have published a clear list of what specific personal information we may gather and hold, why this is used (for the necessary operation and fulfilment of a service requested by the client) and how it is specifically collected.

Confidentiality:

- We limit access to the personal information of data subjects to those employees, agents, contractors and other third parties who have a business need to know. They will only process personal information on the instructions of the Managing Director and they are subject to a duty of confidentiality.
- All of our employees are responsible for making all data subjects aware of our data protection procedures and securing their consent, prior to us collecting or processing personal information from them.
- We specify details of third party organisations/individuals to whom personal information may be passed, and the reasons for this. We obtain consent from the data subject in every instance. We always ensure that any external organisation asked to provide a service for us has appropriate security measures in place.

Information Security & Technical and Organisational Measures:

We take the privacy and security of individuals and their personal information very seriously and take every reasonable measure and precaution to protect and secure the personal data that we process. In order to prevent unauthorised access, alteration, disclosure or loss/destruction of information, we have several layers of robust information security policies and procedures in place:

- Computer servers & CCTV systems protected with HTTPS and SSL technology
- Password protection on all hardware & software (PCs, smartphones, CCTV, email,etc)
- Encryptions on company software and call systems
- Authentication for all electronic payments (online or card machines)
- Restriction of data (eg. credit card details are not stored)
- Access controls for employees (see above)
- Access controls for third parties (personal information is not shared with any third party for commercial reasons)
- GDPR Roles
- Paper files secured in locked locations with restricted employee access.
- Archived records kept in a secure location offsite

Data Retention & Erasure:

We have a commitment to ensuring that all personal information is stored, archived and destroyed compliantly and ethically. All of the procedures below are clearly set out for all data subjects:

- We ensure that we meet the 'data minimisation' principle by limiting the collection of personal information to that which is directly relevant and necessary to fulfill our service.
- We also ensure that we meet the 'storage limitation' principles, as all personal data is only processed for as long as is necessary to allow us to fulfil our services. It is stored indefinitely on our computer system and in paper format for seven years.
- We have dedicated procedures in place to meet the 'Right to Erasure' obligation and are aware of when this and other data subject's rights apply, along with any exemptions, response timeframes and notification responsibilities.

Data Breaches:
Our breach procedures ensure that we have safeguards and measures in place to identify, assess, investigate and report any personal data breach at the earliest possible time. Our procedures are disseminated to all employees, making them aware of the reporting lines and steps to follow.

Consent:
- Our procedures ensure that we only use personal information for the purposes for which we collect it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. Or unless use of personal information is required by law.
- We provide all data subjects with clear, defined ways to actively consent to us processing their information, with the ability to withdraw consent at any time.
- We ensure that individuals understand what information they are providing, why and how we use it. Our processes allow us to effectively record consent, making sure that we can evidence an affirmative opt-in, along with time and date records.

Data Transfers Outside the EU:
If we seek to transfer data outside the EU (European Economic Area) such data will only be transferred to countries deemed by the European Commission to provide adequate data protection. Furthermore, we will obtain the prior consent of all individuals whose data is likely to be transferred.

Subject Access Request (SAR):
Any data subjects who make a SAR to us are entitled to receive the requested information within one month. This provision will be free of charge.
We will verify the data subject, processing the access request via appropriate steps, decide what exemptions apply and overall, ensure that communications with data subjects are compliant, consistent and adequate.

Legal Basis for Processing:
In our capacity as both Data Controller and Data Processor, our legal basis for processing is clearly stated in our Privacy Policy. We ensure that each basis is appropriate for the activity it relates to.
Where applicable, we also maintain records of the processing activities under our responsibility, ensuring that our obligations under Article 30 of the GDPR are met.

Privacy Policy:
We have revised our Privacy Policy to comply with GDPR, ensuring that all individuals whose personal information we process have been informed of why we need it, how it is used, what their rights are, who the information is disclosed to and what safeguarding measures are in place to protect their information.
This policy is publicly available on our website
https://www.cbastock.co.uk/uploads/1/9/9/4/19948103/privacy_policy.pdf

Direct Marketing:
We have clear opt-in / opt-out mechanisms in place for marketing subscriptions and defined methods for unsubscribing or restricting collection/use of personal information.

Processor Agreements:
In the rare occasion that we use any third party to process personal information on our behalf (eg. Payroll, Recruitment, Hosting, etc) we employ due diligence procedures to ensure that they are compliant and that they (as well as we), meet and understand their/our GDPR obligations. These measures include initial and ongoing reviews of the service provided, the necessity of the processing activity and the technical and organisational measures in place.

Special Categories Data:
- Special category data is only processed where necessary and is only processed where we have first identified the appropriate Article 9(2) basis.
- Where we obtain and process any special category information, we do so in complete compliance with the Article 9 requirements and have high-level encryptions and protections on all such data.
- The two special categories of personal data concerned are published in our Privacy Policy.
- Where we rely on consent for processing, this is explicit and is verified by a signature via our Arrangement Forms, with the right to modify or remove consent being clearly signposted.

Further Compliance Measures

We have designated a Data Protection Officer, who is responsible for promoting awareness of the GDPR across the organisation, assessing our GDPR readiness, identifying any gap areas and implementing the new policies, procedures and measures.

We understand that continuous employee awareness and understanding is vital to the continued compliance of the GDPR. Employees are involved from the outset by the inclusion of our GDPR procedures and controls within our staff induction and training programme.

We have a clear and published procedure to enable individuals to easily contact us with any queries, or should they wish to make a complaint. As well as our own contact details and our ICO Registry Record link below, we publish contact details of the GDPR supervisory authority on our website.

Our ICO registry record can be found at https://ico.org.uk/ESDWebPages/Entry/ZB021279