PRIVACY POLICY

DATA AND SECURITY POLICY

1. INTRODUCTION

This Data Protection Policy sets out how Kaboom LLC ("the Company") handles the personal data of our customers, suppliers, employees, workers and other third parties ("Data Subjects"). We are the data controller of all personal data relating to Data Subjects and the personal data used in our business for our own commercial purposes.

1.1. This policy applies to all personal data (any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access) the Company Processes regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users, or any other Data Subject.

1.2. This policy applies to all employees, workers, contractors, agency workers, consultants, directors, members, and others.

1.3. You must read, understand and comply with this policy when processing personal data on the Company's behalf and attend training on its requirements. This policy sets out what we expect from you in order for the Company to comply with applicable law. Your compliance with this policy is mandatory. Any breach of this policy may result in disciplinary action.

1.4. This policy is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the Compliance Manager.

1.5. This policy does not form part of any contract of employment or contract for services and we may amend it at any time without notice.

1.6. This Policy does not override any applicable national data privacy laws and regulations in countries where the Company operates.

2. SCOPE

2.1. We recognise that the correct and lawful treatment of personal data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of personal data is a critical responsibility that we take seriously at all times. The Company is exposed to potential fines for failure to comply with the provisions prevalent regulation such as GDPR and other national equivalents.

2.2. All levels of management are responsible for ensuring you comply with this Policy and need to implement appropriate practices, processes, controls and training to ensure such compliance.

2.3. Please contact the Compliance Manager with any questions about the operation of this policy or the prevailing Data Protection Regulation or other data protection laws or if you have any concerns that this Policy is not being or has not been followed. In particular, you must always contact the Compliance Manager in the following circumstances:

2.3.1. if you are unsure of the lawful basis which you are relying on to process personal data (including the legitimate interests used by the Company) (see section 5.1 below);

2.3.2. if you need to rely on consent and/or need to capture explicit consent;

2.3.3. if you need to draft privacy notices (see section 5.3 below);

2.3.4. if there has been a personal data Breach (section 10.2 below);

2.3.5. if you need any assistance dealing with any rights invoked by a Data Subject (see section 12);

2.3.6. whenever you are engaging in a significant new, or change in, processing activity which is likely to require a Data Protection Impact Assessment ("DPIA") (see section 13.4 below) or plan to use personal data for purposes others than what it was collected for;

2.3.7. you need help complying with applicable law when carrying out direct marketing activities (see section 13.6 below); or

4. PERSONAL DATA PROTECTION PRINCIPLES

1. We have elected and adhere to the principles relating to processing of personal data set out in the GDPR, which are set out within sections 5 to 13 this policy. We are responsible for and must be able to demonstrate compliance with these principles.

2. LAWFULNESS, FAIRNESS, TRANSPARENCY

2.1. Lawfulness and fairness

2.1.1. Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

2.1.2. You may only collect, process and share personal data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding personal data to specified lawful purposes. These restrictions are not intended to prevent processing but ensure that we process personal data fairly and without adversely affecting the Data Subject.

2.1.3. The GDPR allows processing for specific purposes, some of which are set out below:

(a) the Data Subject has given his or her consent;

(b) the processing is necessary for the performance of a contract with the Data Subject;

(c) to meet our legal compliance obligations.;

(d) to protect the Data Subject's vital interests;

(e) to pursue our legitimate interests for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process personal data for legitimate interests need to be set out in applicable privacy notices.

5.1.4 You must identify and document the legal ground being relied on for each processing activity.

2.2. Consent

2.2.1. A Data Controller must only process personal data on the basis of one or more of the lawful bases set out in the GDPR, which include consent.

2.2.2. A Data Subject consents to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If consent is given in a document which deals with other matters, then the consent must be kept separate from those other matters.

2.2.3. Data Subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to process personal data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

2.2.4. Unless we can rely on another legal basis of processing, explicit consent is usually required for processing sensitive personal data, for automated decision-making and for cross border data transfers. Usually we will be relying on another legal basis (and not require explicit consent) to process most types of sensitive data. Where explicit consent (in writing) is required, you must issue a consent notice to the Data Subject to capture explicit consent.

2.2.5. You will need to evidence consent captured and keep records of all consents so that the Company can demonstrate compliance with consent requirements.

2.3. Transparency (notifying data subjects)

2.3.1. The GDPR requires data controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate privacy notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

2.3.2. Whenever we collect personal data directly from Data Subjects, including for human resources or employment purposes, we must provide the Data Subject with all the information required by the GDPR including the identity of the data controller, how and why we will use, process, disclose, protect and retain that personal data through a privacy notice which must be presented when the Data Subject first provides the personal data

2.3.3. When personal data is collected indirectly (for example, from a third party or publicly available source), you must provide the Data Subject with all the information required by the GDPR as soon as possible after collecting/ receiving the data. You must also check that the personal data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed processing of that personal data.

3. PURPOSE LIMITATION

3.1. Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

3.2. You cannot use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have consented where necessary.

4. DATA MINIMISATION

4.1. Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

4.2. You may only process personal data when performing your job duties requires it. You cannot process personal data for any reason unrelated to your job duties.

4.3. You may only collect personal data that you require for your job duties: do not collect excessive data. Ensure any personal data collected is adequate and relevant for the intended purposes.

4.4. You must ensure that when personal data is no longer needed for specified purposes, it is deleted or anonymized in accordance with the Company's data retention guidelines.

5. ACCURACY

5.1. Personal data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

5.2. You will ensure that the personal data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any personal data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or outof-date personal data.

6. STORAGE LIMITATION

6.1. Personal data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

6.2. You must not keep personal data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

6.3. The Company will maintain retention policies and procedures to ensure personal data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time.

6.4. You will take all reasonable steps to destroy or erase from our systems all personal data that we no longer require in accordance with all the Company's applicable records retention schedules and policies. This includes requiring third parties to delete such data where applicable.

6.5. You will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable privacy notice.

7. SECURITY INTEGRITY AND CONFIDENTIALITY

7.1. Protecting personal data

7.1.1. Personal data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

7.1.2. We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of personal data that we own or maintain on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of personal data. You are responsible for protecting the personal data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorized processing of personal data and against the accidental loss of, or damage to, personal data. You must exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure.

7.1.3. You must follow all procedures and technologies we put in place to maintain the security of all personal data from the point of collection to the point of destruction. You may only transfer personal data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

7.1.4. You must maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

(a) Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it.

(b) Integrity means that personal data is accurate and suitable for the purpose for which it is processed.

(c) Availability means that authorised users are able to access the personal data when they need it for authorised purposes.

7.1.5. You must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPR and relevant standards to protect personal data.

7.2. Reporting a personal data breach

7.2.1. The GDPR requires data controllers to notify any personal data breach to the applicable regulator and, in certain instances, the Data Subject.

7.2.2. A "personal data breach" means any act or omission that compromises the security, confidentiality, integrity or availability of personal data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of personal data is a personal data breach.

7.2.3. We have put in place procedures to deal with any suspected personal data breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

7.2.4. If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the Compliance Manager for personal data breaches. You should preserve all evidence relating to the potential personal data breach.

8. DATA SUBJECT'S RIGHTS AND REQUESTS

8.1. Data Subjects have rights when it comes to how we handle their personal data. These include rights to:

8.1.1. withdraw consent to processing at any time;

8.1.2. receive certain information about the Data Controller's processing activities;

8.1.3. request access to their personal data that we hold;

8.1.4. prevent our use of their personal data for direct marketing purposes;

8.1.5. ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;

8.1.6. restrict processing in specific circumstances;

8.1.7. challenge processing which has been justified on the basis of our legitimate interests or in the public interest;

8.1.8. object to decisions based solely on automated processing, including profiling;

8.1.9. prevent processing that is likely to cause damage or distress to the Data Subject or anyone else;

8.1.10. be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;

8.1.11. make a complaint to the supervisory authority; and

8.1.12. in limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format.

8.2. You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing personal data without proper authorisation).

8.3. You must immediately forward any Data Subject request you receive to Compliance Manager.

9. ACCOUNTABILITY

9.1. The data controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The data controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

9.1.1. The Company must have adequate resources and controls in place to ensure and to document GDPR compliance including:

(a) appointing an executive accountable for data privacy;

(b) implementing privacy by design when processing personal data and completing data protection impact assessments (DPIAs) where processing presents a high risk to rights and freedoms of Data Subjects;

(c) integrating data protection into internal documents including this Policy, any related documents or privacy notices;

(d) regularly training you on the GDPR, internal policies and procedures, and data protection matters including, for example, Data Subject's rights, consent, legal basis, DPIA and personal data breaches. The Company must maintain a record of training attendance by everyone it employs and engages; and

(e) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

9.2. Record keeping

9.2.1. The GDPR requires us to keep full and accurate records of all our data processing activities.

9.2.2. You must keep and maintain accurate corporate records reflecting our processing including records of Data Subjects' consents and procedures for obtaining consents.

9.2.3. These records should include, at a minimum, the name and contact details of the data controller, clear descriptions of the personal data types, Data Subject types, processing activities, processing purposes, third-party recipients of the personal data, personal data storage locations, personal data transfers, the personal data's retention period and a description of the security measures in place. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

9.3. Training and audit

9.3.1. We are required to ensure you have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

9.3.2. You must undergo all mandatory data privacy related training and ensure your team undergo similar mandatory training.

9.3.3. You must regularly review all the systems and processes under your control to ensure they comply with this Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of personal data.

9.4. Privacy by design and DPIAs

9.4.1. We are required to implement privacy by design measures when processing personal data by implementing appropriate technical and organisational measures (like pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

9.4.2. You must assess what privacy by design measures can be implemented on all programs/systems/processes that process personal data by taking into account the following:

(a) the state of the art;

(b) the cost of implementation;

(c) the nature, scope, context and purposes of processing; and

(d) the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the processing

9.4.3. Data controllers must also conduct DPIAs in respect to high risk processing.

9.4.4. You should conduct a DPIA (and discuss your findings with the Compliance Manager) when implementing major system or business change programs involving the processing of personal data including:

(a) use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

(b) Automated processing including profiling and auto-mated decision making;

c) large scale processing of sensitive data; and

(d) large scale, systematic monitoring of a publicly accessible area.

9.4.5. A DPIA must include

(a) a description of the processing, its purposes and the data controller's legitimate interests if appropriate;

(b) an assessment of the necessity and proportionality of the processing in relation to its purpose;

(c) an assessment of the risk to individuals; and

(d) the risk mitigation measures in place and demonstration of compliance.

9.5. Automated processing (including profiling) and automated decision-making (ADM)

9.5.1. Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

9.5.2. If certain types of sensitive data are being processed, then grounds (b) or (c) will not be allowed but such sensitive data can be processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

(a) a Data Subject has explicitly consented;

(b) the processing is authorised by law; or

(c) the processing is necessary for the performance of or entering into a contract.

9.5.3. If a decision is to be based solely on automated processing (including profiling), then Data Subjects must be informed when you first communicate with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

9.5.4. We must also inform the Data Subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

9.5.5. A DPIA must be carried out before any automated processing (including profiling) or ADM activities are undertaken.

9.6. Direct marketing

9.6.1. We are subject to certain rules and privacy laws when marketing to our customers.

9.6.2. For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

9.6.3. The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

9.6.4. A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

9.7. Sharing personal data

9.7.1. Generally we are not allowed to share personal data with third parties unless certain safeguards and contractual arrangements have been put in place.

9.7.2. You may only share the personal data we hold with another employee, agent or representative of our group (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

9.7.3. You may only share the personal data we hold with third parties, such as our service providers if:

(a) they have a need to know the information for the purposes of providing the contracted services;

(b) sharing the personal data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's consent has been obtained;

(c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

(d) the transfer complies with any applicable cross border transfer restrictions; and

(e) a fully executed written contract that contains GDPR approved third party clauses has been obtained.

COMPLAINTS POLICY

Kaboom LLC seeks to provide high quality services and therefore is committed to being responsive to the needs and concerns of its customers and to resolving any complaint as quickly as possible. The purpose of this policy is to provide guidance to both of our customers and staff on the manner in which we receive and manage a complaint. We are committed to being consistent, fair and impartial when handling a complaint. For the purposes of this Policy the term “complaint” means an expression and/or statement of dissatisfaction addressed to Kaboom LLC by a client relating to the provision of the services offered by Kaboom LLC.

Procedure

The procedure which shall be followed by Kaboom LLC when handling with a client’s complaint is as follows:

FILING COMPLAINTS

Any client who wishes to submit a complaint is advised to send a complaint to Kaboom LLC in the following way: Email to: support@kaboom.world

The client can submit complaints free of charge.

Receiving Complaints

When a complaint is received, it is initially handled by a member of staff of Kaboom LLC who shall immediately register the complaint in Kaboom LLC’s internal register and give it a unique reference number. Once a complaint is filed we shall take all necessary actions to ensure that the complaint is properly addressed by forwarding it to the department the complaint concerns and/or is addressed to within 5 working days. We will then inform you that your complaint has been forwarded to the relevant department/personnel, providing all details so that you are aware of who is dealing with your complaint.

Additionally, the employees of Kaboom LLC, shall make all best efforts to ensure that, in case the complaint is of such nature that it is not formal and can be resolved immediately, to do so that your complaint is resolved promptly. However, the member of staff in such a case shall not:

Commit him/herself in any way to the client;

Address any issues in relation to best execution;

Address any issues relating to legal issues;

Commit Kaboom LLC in taking any action prior to examining the issues in a formal manner.

Complaint Details

Upon receiving a written complaint, we will record your name and contact details. We will also record all details of your complaint including the facts and the cause/s of your complaint, the outcome and any actions taken following the investigation of your complaint.

We will also record all dates and times relating to actions taken to resolve the complaint and communications between us. If you file a complaint we will record your personal information solely for the purposes of addressing your complaint. Your personal details will actively be protected from disclosure, unless you expressly consent to its disclosure.

Handling Complaints

The events leading to the complaint shall be examined and assessed by the relevant department of Kaboom LLC based on the information provided by the client. The facts as stated by the client shall be examined and verified with the relevant heads of department and any additional information needed shall be retrieved from Kaboom LLC's archives (electronic mail, IT data, etc.). During the investigation of the complaint, the Company shall inform the complainant of the handling process of his/her complaint. Upon completion of the investigation, Kaboom LLC will prepare a report stating the facts and make recommendations which will be brought to management's attention who will then conclude on the final decision to be made. We are committed to resolving complaints at the first point of contact, however, this will not always be possible especially in circumstances in which a more formal complaints process will be followed. Kaboom LLC shall investigate the complaint and reply, within 1 month, to the complainant about the outcome/decision. In the event when Kaboom LLC is unable to respond within 1 months, it shall inform the complainant of the reasons for the delay and the period of time within which it is expected to complete the investigation. This period of time cannot exceed 3 months from the submission of the complaint.