GDPR Data Protection Policy

Document Reference:
Killer-Byte Ltd GDPR
Revision Date:
25/5/2018
Revision Number:
001
Classification:
Open

KILLER-BYTE LTD
Your Local, Friendly IT Support

Lifestyle House, 157-163 Sheffield Road, Killamarsh, S21 1DY Telephone: 0114 276 4983

51 Chesterfield Road, Dronfield, S18 2XA Telephone: 01246 906 124

Table of Contents

Contents

KILLER-BYTE LTD
Your Local, Friendly IT Support

Lifestyle House, 157-163 Sheffield Road, Killamarsh, S21 1DY Telephone: 0114 276 4983

51 Chesterfield Road, Dronfield, S18 2XA Telephone: 01246 906 124

Introduction

Killer-Byte Ltd is committed to conducting its business in accordance with all applicable Data Protection laws and regulations and in line with the highest standards of ethical conduct.

This policy sets forth the expected behaviours of Killer-Byte Ltd Employees and Third Parties in relation to the collection, use, retention, transfer, disclosure and destruction of any Personal Data belonging to a Killer-Byte Ltd Contact (i.e. the Data Subject).

Personal Data is any information (including opinions and intentions) which relates to an identified or Identifiable Natural Person. Personal Data is subject to certain legal safeguards and other regulations, which impose restrictions on how organisations may process Personal Data. An organisation that handles Personal Data and makes decisions about its use is known as a Data Controller. Killer-Byte Ltd, as a Data Controller, is responsible for ensuring compliance with the Data Protection requirements outlined in this policy. Non-compliance may expose Killer-Byte Ltd to complaints, regulatory action, fines and/or reputational damage.

Killer-Byte Ltd's leadership is fully committed to ensuring continued and effective implementation of this policy, and expects all Killer-Byte Ltd Employees and Third Parties to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action or business sanction.

This notice provides you with the information on what personal data we capture and how we use it.

This policy has been approved by Killer-Byte Ltd Director, Andrew J. Coy.

2. Definitions

Employee - An individual who works part-time or full-time for Killer-Byte Ltd under a contract of employment, whether oral or written, express or implied, and has recognised rights and duties. This Includes temporary employees and independent contractors.

Third Party - An external organisation with which Killer-Byte Ltd conducts business and is also authorised to, under the direct authority of Killer-Byte Ltd, Process the Personal Data of Killer-Byte Ltd Contacts.

Personal Data - Any information (including opinions and intentions) which relates to an identified or Identifiable Natural Person.

Contact - Any past, current or prospective Killer-Byte Ltd customer.

Identifiable Natural Person - Anyone 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 one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Data Controller - A natural or legal person, Public Authority, Agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

Killer-Byte Ltd Entity - A Killer-Byte Ltd establishment, including subsidiaries and joint ventures over which Killer-Byte Ltd exercise management control.

Data Subject - The identified or Identifiable Natural Person to which the data refers.

Process, Processed, Processing - Any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means. Operations performed may include collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Protection - The process of safeguarding Personal Data from unauthorised or unlawful disclosure, access, alteration, Processing, transfer or destruction.

Data Protection Authority - An independent Public Authority responsible for monitoring the application of the relevant Data Protection regulation set forth in national law.

Data Processors - A natural or legal person, Public Authority, Agency or other body which Processes Personal Data on behalf of a Data Controller.

Consent - 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.

KILLER-BYTE LTD
Your Local, Friendly IT Support

Lifestyle House, 157-163 Sheffield Road, Killamarsh, S21 1DY Telephone: 0114 276 4983

51 Chesterfield Road, Dronfield, S18 2XA Telephone: 01246 906 124

Special Categories of Data - Personal Data pertaining to or revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.

Profiling - Any form of automated processing of Personal Data where Personal Data is used to evaluate specific or general characteristics relating to an Identifiable Natural Person. In particular to analyse or predict certain aspects concerning that natural person's performance at work, economic situations, health, personal preferences, interests, reliability, behaviour, location or movement.

Data Breach - A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

Encryption - The process of converting information or data into code, to prevent unauthorised access.

Pseudonymisation - Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) without a "key" that allows the data to be re-identified.

Anonymisation - Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) by any means or by any person.

3. Scope

This policy applies to all Killer-Byte Ltd Entities where a Data Subject's Personal Data is processed:

- In the context of the business activities of the Killer-Byte Ltd Entity.
- For the provision or offer of goods or services to individuals (including those provided or offered free-of-charge) by a Killer-Byte Ltd Entity.

This policy applies to all Processing of Personal Data in electronic form (including electronic mail and documents created with word processing software) or where it is held in manual files that are structured in a way that allows ready access to information about individuals.

This policy has been designed to establish a nationwide baseline standard for the Processing and Protection of Personal Data by all Killer-Byte Ltd Entities. Where national law imposes a requirement which is stricter than imposed by this policy, the requirements in national law must be followed. Furthermore, where national law imposes a requirement that is not addressed in this policy, the relevant national law must be adhered to.

3.1 Policy Dissemination & Enforcement

The management team of each Killer-Byte Ltd Entity must ensure that all Killer-Byte Ltd Employees responsible for the Processing of Personal Data are aware of and comply with the contents of this policy.

In addition, each Killer-Byte Ltd Entity will make sure all Third Parties engaged to Process Personal Data on their behalf (i.e. their Data Processors) are aware of and comply with the contents of this policy. Assurance of such compliance must be obtained from all Third Parties, whether companies or individuals, prior to granting them access to Personal Data controlled by Killer-Byte Ltd.

3.2 Compliance Monitoring

To confirm that an adequate level of compliance that is being achieved by all Killer-Byte Ltd Entities in relation to this policy, the Data Protection Officer will carry out an annual Data Protection compliance audit for all such Entities. Each audit will, as a minimum, assess:

- Compliance with Policy in relation to the protection of Personal Data, including:
  - The assignment of responsibilities.
  - Raising awareness.
  - Training of Employees.

3.3 Data Protection Principles

Killer-Byte Ltd has adopted the following principles to govern its collection, use, retention, transfer, disclosure and destruction of Personal Data:

- Principle 1: Lawfulness, Fairness and Transparency - Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. This means, Killer-Byte Ltd must tell the Data Subject what Processing will occur (transparency), the Processing must match the description given to the Data Subject (fairness), and it must be for one of the purposes specified in the applicable Data Protection regulation (lawfulness).

- Principle 2: Purpose Limitation - Personal Data shall be collected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes. This means Killer-Byte Ltd must specify exactly what the Personal Data collected will be used for and limit the Processing of that Personal Data to only what is necessary to meet the specified purpose.

- Principle 3: Data Minimisation - Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This means Killer-Byte Ltd must not store any Personal Data beyond what is strictly required.

- Principle 4: Accuracy - Personal Data shall be accurate and, kept up to date.
This means Killer-Byte Ltd must have in place processes for identifying and addressing out-of-date, incorrect and redundant Personal Data.

- Principle 5: Storage Limitation - Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is processed. This means Killer-Byte Ltd must, wherever possible, store Personal Data in a way that limits or prevents identification of the Data Subject.

- Principle 6: Integrity & Confidentiality - Personal Data shall be processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful Processing, and against accidental loss, destruction or damage. Killer-Byte Ltd must use appropriate technical and organisational measures to ensure the integrity and confidentiality of Personal Data are maintained at all times.

- Principle 7: Accountability

The Data Controller shall be responsible for, and be able to demonstrate compliance. This means Killer-Byte Ltd must demonstrate that the six Data Protection Principles (outlined above) are met for all Personal Data for which it is responsible.

4. Who is Killer-Byte Ltd?

Killer-Byte Ltd is a provider of IT products and services to the public / domestic, Commercial and Education Sectors. We work with numerous suppliers, partners and contractors to provide such services to a geographically and organisationally diverse client base.

For any data protection related queries, we can be contacted directly here:

- GDPR@killer-byte.co.uk
- 0114 276 49 83

The personal data we collect is:

Personal Data Type	**Source (***Where Killer-Byte Ltd obtained the data if not collected from you directly, the data subject then from publically accessible sources***)**
Business contact details; Names, Job titles, Email address, Phone Numbers (landline/mobile), Delivery / Billing address	*Indirect:* LinkedIn, Facebook, Customer Websites, Public Directories. *Direct:* Job Sheets (point of contact), Telephone Prospecting, Networking Events
Incidental information; Annual leave, Birthdays, Social Events, Opinions	Directly from customer or informed customer Employee / Colleague.
Credit/debit details, bank details	Directly from Customer

The personal data we collect will be used for the following purposes:

- Facilitating business transactions
- Delivery of purchased goods
- Marketing and promotion of our goods and services
- General customer service/relationship management

Our legal basis for processing for the personal data:

- Contractual obligation
- Legal obligation
- Legitimate business interest

Any legitimate interests pursued by Killer-Byte Ltd are as follows:

- Business development (lead generation, relationship management)
- To improve our service offering
- Marketing purposes

The special categories of personal data concerned are:

- We do not currently collect any special categories of personal data of any kind

4.1 Disclosures

Killer-Byte Ltd will pass on your personal data to third parties. The following third parties will receive your personal data for the following purpose(s) as part of the processing activities:

Third Party	Processing Activity
Distribution partners	Facilitating business transactions
Logistics	Delivery of purchased goods
HMRC	Legal obligation
Auditors	Legal obligation
Legal representatives	Legal obligation
Support partners	Delivery of purchased goods & services

All appropriate disclosures will be made, in a manner that draws attention to them, unless one of the following applies:

- The Data Subject already has the information
- A legal exemption applies to the requirements for disclosure and/or Consent.

The disclosures may be given orally, electronically or in writing. If given orally, the person making the disclosures should use a suitable script or form approved in advance by the Office of Data Protection. The associated receipt or form should be retained, along with a record of the facts, date, content, and method of disclosure.

4.2 Data Retention Period

Killer-Byte Ltd will process customers' personal information for as long as they are a viable / potential customer. Killer-Byte Ltd will store the personal data for this period unless a legitimate or contractual / legal obligation requires us to remove / destroy it. To ensure fair Processing, Personal Data will not be retained for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further Processed. All Personal Data should be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

Type	Customer	Prospective Customer
Definition	A business who has transacted with us for the provision of goods or services.	A business who's contact details we have legitimately gained through sources defined in table 2.1 and who we would like to transact with.
Retention Period	**Contact information:** Between 2 Years – Indefinitely (or until request for the data to be removed) **Financial information:** 7 Years Minimum	**Contact information:** We only retain data relating to a business, this is held indefinitely. A contact from a prospective business can request to be removed.

4.3 Your Rights – If we hold your Personal Data

At any point while we are in possession of, or processing your personal data, you, the data subject, have the following rights:

- Right of access – you have the right to request a copy of the information that we hold about you.
- Right of rectification – you have a right to correct data that we hold about you that is inaccurate or incomplete.
- Right to be forgotten – in certain circumstances you can ask for the data we hold about you to be erased from our records.
- Right to restriction of processing – where certain conditions apply to have a right to restrict the processing.
- Right of portability – you have the right to have the data we hold about you transferred to another organisation.
- Right to object – you have the right to object to certain types of processing such as direct marketing.
- Right to judicial review

All of the above requests will be forwarded on should there be a third party involved in the processing of your personal data.

Each Killer-Byte Ltd Entity will, when required by applicable law, contract, or where it considers that it is reasonably appropriate to do so, provide Data Subjects with information as to the purpose of the Processing of their Personal Data.

4.4 Complaints Handling

In the event that you wish to make a complaint about how your personal data is being processed by Killer-Byte Ltd (or third parties as described in 4.1 above), or how your complaint has been handled, you have the right to lodge a complaint directly with the supervisory authority and Killer-Byte Ltd.

The details for each of these contacts are:

	Supervisory authority contact details	**Data controller contact details**
Contact Name:	Information Commissioners office (ICO)	Killer-Byte Ltd
Address Line 1:	Information Commissioners Office	157 – 163 Sheffield Road
Address Line 2:	Wycliffe House	Killamarsh
Address Line 3:	Water Lane	Sheffield
Address Line 4:	Wilmslow	S21 1DY
Address Line 5:	Cheshire	
Email:	casework@ico.org.uk	GDPR@killer-byte.co.uk
Telephone:	0303 123 1113	0114 276 4989

4.5 Breach Reporting

Any individual who suspects that a Personal Data Breach has occurred due to the theft or exposure of Personal Data must immediately notify the Data Protection office providing a description of what occurred. Notification of the incident can me made via e-mail GDPR@killer-byte.co.uk, by calling 0114 276 4983, or by using the anonymous incident reporting form at www.killer-byte.co.uk/contact.

The Data Protection Officer will investigate all reported incidents to confirm whether or not a Personal Data Breach has occurred. If a Personal Data Breach is confirmed, the Office of Data Protection will follow the relevant authorised procedure based on the criticality and quantity of the Personal Data involved.

5. Data Protection

Each Killer-Byte Ltd Entity will adopt physical, technical, and organisational measures to ensure the security of Personal Data. This includes the prevention of loss or damage, unauthorised alteration, access or Processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment.

This is the minimum set of security measures to be adopted by each Killer-Byte Ltd Entity:

- Prevent unauthorised persons from gaining access to data processing systems in which Personal Data are Processed.
- Prevent persons entitled to use a data processing system from accessing Personal Data beyond their needs and authorisations.
- Ensure that Personal Data in the course of electronic transmission during transport cannot be read, copied, modified or removed without authorisation.
- Ensure that access logs are in place to establish whether, and by whom, the Personal Data was entered into, modified on or removed from a data processing system.
- Ensure that in the case where Processing is carried out by a Data Processor, the data can be Processed only in accordance with the instructions of the Data Controller.
- Ensure that Personal Data is protected against undesired destruction or loss.
- Ensure that Personal Data collected for different purposes can and is Processed separately.
- Ensure that Personal Data is not kept longer than necessary.

6. Digital Marketing

As a general rule Killer-Byte Ltd will not send promotional or direct marketing material to a Killer-Byte Ltd Contact through digital channels such as mobile phones, email and the Internet, without first obtaining their Consent. Any Killer-Byte Ltd Entity wishing to carry out a digital marketing campaign without obtaining prior Consent from the Data Subject must first have it approved by the Data Protection Officer.

Where Personal Data Processing is approved for digital marketing purposes, the Data Subject must be informed at the point of first contact that they have the right to object, at any stage, to having their data Processed for such purposes. If the Data Subject puts forward an objection, digital marketing related Processing of their Personal Data must cease immediately and their details should be kept on a suppression list with a record of their opt-out decision, rather than being completely deleted.

It should be noted that where digital marketing is carried out in a 'business to business' context, there is no legal requirement to obtain an indication of Consent to carry out digital marketing to individuals provided that they are given the opportunity to opt-out.

7. Policy Maintenance

All inquiries about this policy, including requests for exceptions or changes should be directed to the Data Protection Officer via e-mail GDPR@killer-byte.co.uk

7.1 Publication

This policy shall be available to all Killer-Byte Ltd Employees through the Killer-Byte Ltd Website www.killer-byte.co.uk or can be accessed via alternative means as deemed appropriate by the Office of Data Protection.

7.2 Effective Date

This policy is effective as of 25/04/2018.

7.3 Revisions

The Data Protection Officer is responsible for the maintenance and accuracy of this policy. Notice of significant revisions shall be provided to Killer-Byte Ltd Employees through email. Changes to this policy will come into force when published on Killer-Byte Ltd Policy website www.killer-byte.co.uk.