
	Version: <b>2.6</b>
	Last Amendment: <b>May 2024</b>
	Next Review: <b>April 2025</b>
<b>Data Protection Policy</b>	Department: <b>Information Security   Global Privacy Office</b>
	Contact: privacy@keywordsstudios.com
To be read in conjunction with: General Information Security Policy	
<b>CONFIDENTIAL AND PROPRIETARY</b>	


## EXECUTIVE SUMMARY

- Ensuring continued compliance with global Data Protection Laws demands a sustained, collaborative effort that transcends individual studios or any form of legal entity within the Keywords Studios group (“**Entities**”) or Group Functions within the Keywords Studios group.
- This Policy comprehensively details all data protection and privacy compliance requirements applicable to Keywords Studios. Its purpose is twofold: to showcase Keywords Studios’ grasp of these regulations and its strategy to address them, essential for potential requests from regulators and clients, and to clearly delineates Keywords Studios’ expectations for Processing Personal Data, assigning specific roles and responsibilities within the organization.
- Failure to adhere to this Policy, and consequently, Data Protection Laws, can result in regulatory action, which could result in fines of up to 4% of total global turnover being imposed and cause significant reputational damage. Therefore, strict adherence from all is imperative.
- Of particular importance is the '*Principles for Processing of Personal Data*' section, as it is foundational to the entire Policy. These principles must guide all initiatives involving Personal Data, including but not limited to processing Employee Data, implementing new systems or software, engaging new service providers, conducting marketing activities, or utilising Personal Data for new purposes such as AI applications. Consulting this Policy and engaging the Global Privacy Office is mandatory before proceeding with any such initiatives.
- All Employees must grasp the concept of data subject rights requests and Personal Data Breaches, promptly referring to this Policy for guidance and involving the Global Privacy Office when necessary.
- To foster a collective and continuous commitment to data protection and privacy, Entity and Group Function Directors must diligently review their respective roles and responsibilities outlined in this Policy to ensure their teams are equipped to meet the requisite standards.
- Moreover, this Policy will be complemented by the rollout of a 'Global Data Protection Program,' designed to support Entities and Group Functions in fully integrating all aspects of this Policy into their operations.

 <b>Keywords Studios</b> Imagine More	Document Title	Document No. <i>Click to enter Doc No.</i>	Version <b>2.6</b>
	Data Protection Policy	Last Revision Date Apr. 25, 24	Page 1 of 30

## Table of contents

1.	Management of the Policy .....	2
1.1.	Nature of the Document .....	2
1.2.	Purpose.....	2
1.3.	Scope .....	2
1.4.	Definitions .....	2
1.5.	Policy Governance .....	2
1.6.	Policy Breaches.....	2
1.7.	Document Classification and Languages .....	3
1.8.	Follow-up and Questions.....	3
2.	Principles for the Processing of Personal Data.....	4
3.	Compliance and Group Standards.....	5
3.1.	Records of Processing Activities .....	5
3.2.	Lawful Basis for Processing Personal Data .....	6
3.3.	Consent Management .....	7
3.4.	Transparency.....	8
3.5.	Personal Data Access Rights.....	10
3.6.	Portability Rights .....	10
3.7.	Rectification Rights .....	11
3.8.	Data Deletion Rights.....	12
3.9.	Restriction Rights.....	13
3.10.	Right to Object.....	14
3.11.	Automated Decision Making and Profiling .....	14
3.12.	Selling, Sharing and Targeted Advertising.....	15
3.13.	Appeals.....	16
3.14.	Data Protection Complaints .....	16
3.15.	Data Protection by Design and Default.....	17
3.16.	Data Protection Impact Assessments.....	18
3.17.	Data Minimisation.....	19
3.18.	Storage Limitation.....	19
3.19.	Purpose Limitation.....	20
3.20.	Personal Data Breaches.....	20
3.21.	Transfers of Personal Data to Third Countries.....	21
3.22.	Third Party Engagements and Contracts .....	22
3.23.	Security, Technical and Organisational Measures .....	23
3.24.	Cookies.....	23
3.25.	Marketing .....	24
3.26.	Training .....	25
3.27.	Data Protection Officer .....	25
3.28.	Data Protection Regulators and Government Agencies .....	25
3.29.	Privacy and Data Protection Risk Management .....	26
3.30.	Accountability .....	26
3.31.	Reporting .....	27
	Glossary and Definitions .....	28
	Document History.....	30

 <b>Keywords Studios</b> Imagine More	Document Title	Document No. <i>Click to enter Doc No.</i>	Version <b>2.6</b>
	Data Protection Policy	Last Revision Date Apr. 25, 24	Page 2 of 30

# 1. Management of the Policy

## 1.1. Nature of the Document

This Data Protection Policy (the “**Policy**”) is to be considered a compliance policy and sets the minimum data protection and privacy baselines for any other policies, standards, and procedures that govern the Processing of Personal Data. In any event of conflict or where applicable laws or contractual agreements are more stringent than the requirements set in this Policy, the more stringent requirements should be adopted. If there is any uncertainty, please consult [privacy@keywordsstudios.com](mailto:privacy@keywordsstudios.com).

## 1.2. Purpose

Keywords Studios Plc and its subsidiaries from time to time (“**Keywords Studios**”) understand that safeguarding Personal Data is a key pillar to securing the trust of our Employees, clients and stakeholders.

This Policy outlines the measures that Keywords Studios shall take to comply with Data Protection Laws.

Keywords Studios recognises that, due to the global nature of our business, Entities and Group Functions shall Process Personal Data in scope for GDPR and as such this set of laws is our baseline standard. We also acknowledge that some Data Protection Laws may slightly diverge from GDPR and have incorporated such nuance in this Policy by:

- Explicitly stating what the expectation is when Processing Personal Data inside the scope of GDPR and outside the scope of GDPR.
- Adding key sections for global requirements, which do not have any equivalent under GDPR.

## 1.3. Scope

This Policy applies to all Personal Data Processing at Keywords Studios and should be adhered to by all Employees within Keywords Studios.

Where the sections state that Personal Data is in scope for GDPR, this means that an Entity or Group Function are processing the Personal Data of individuals who are in the European Union (“**EU**”) or in the United Kingdom (“**UK**”).

Where the sections state that Personal Data is in scope for Data Protection Laws outside the scope of GDPR, this means that an Entity or Group Function are processing the Personal Data of individuals who are outside the EU or UK.

## 1.4. Definitions

For reference, please see the Definitions in the [Glossary and Definitions](#) section below relating to some of the terms used in this Policy. All capitalized terms in this document will refer to a term defined in the [Glossary and Definitions](#) section of this document.

## 1.5. Policy Governance


This Policy has been created by the Global Privacy Office in conjunction with the Global Legal Team and is:

- Owned by the Global Head of Privacy.
- Managed under the authority of the Risk and Compliance Committee.

This Policy shall be reviewed annually.

## 1.6. Policy Breaches

Adherence to this Policy is mandatory and non-compliance could lead to appropriate disciplinary action, including employment termination.

	Document Title  <i>Data Protection Policy</i>	Document No. <i>Click to enter Doc No.</i>	Version  <b>2.6</b>
		Last Revision Date Apr. 25, 24	Page 3 of 30


### 1.7. **Document Classification and Languages**

Document classification: "KWS-INTERNAL": the information contained in this document is accessible to all Employees of Keywords Studios and authorised third parties. It should not be otherwise disclosed outside of Keywords Studios.

The Policy will be available in English, French, LATAM Spanish, Chinese (Simplified), Japanese, German, Italian, Polish, Russian, Portuguese.

### 1.8. **Follow-up and Questions**

All questions regarding this Policy should be addressed to [privacy@keywordsstudios.com](mailto:privacy@keywordsstudios.com).

	Document Title  <i>Data Protection Policy</i>	Document No. <i>Click to enter Doc No.</i>	Version  <b>2.6</b>
		Last Revision Date Apr. 25, 24	Page 4 of 30

## 2. Principles for the Processing of Personal Data


Keywords Studios must align with the following principles when Processing Personal Data:

- Personal Data shall be Processed lawfully, fairly and in a transparent manner in relation to the individual.
- Personal Data shall be collected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes.
- Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are Processed.
- Personal Data should be accurate and, where necessary, kept up to date; every reasonable step shall be taken to ensure that Personal Data that is inaccurate are erased or rectified without delay.
- Personal Data shall be kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the Personal Data is Processed.
- Personal Data shall be Processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful Processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The above principles shall be adhered to for the entire lifecycle of Processing Personal Data, including but not limited to:

- The design and implementation of all products, services, policies, procedures and processes involving the use of Personal Data.
- The implementation of any tools, systems and platforms that involve Processing of Personal Data.

The rest of this Policy outlines the detailed compliance requirements to meet the above principles and roles and responsibilities for executing the compliance requirements.

 <b>Keywords Studios</b> Imagine More	Document Title	Document No. <i>Click to enter Doc No.</i>	Version <b>2.6</b>
	Data Protection Policy	Last Revision Date Apr. 25, 24	Page 5 of 30

## 3. Compliance and Group Standards

### 3.1. Records of Processing Activities

#### Compliance requirements

When Processing Personal Data is in scope for GDPR, it is a requirement for Keywords Studios to meet the requirements laid out by [Article 30](#) of the GDPR, which requires organisations to maintain Records of Processing Activities.

Where Keywords Studios is a Data Controller, it is requirement for the Records of Processing Activities to contain, as a minimum, the following information:

- The name and contact details of the Data Controller and, where applicable, the Joint Data Controller, the Data Controller's representative, and, where applicable, the Data Protection Officer.
- The purposes of the Processing.
- The categories of individuals whose Personal Data is being Processed.
- The categories of Personal Data Processed.
- The categories of recipients of Personal Data to whom the data shall be disclosed.
- Any Third Country that Keywords Studios transfers Personal Data to.
- The safeguards in place for Personal Data transfers to a Third Country or international organisation where relevant.
- The retention period for the different categories of Personal Data.
- A description of the technical and security measures for protecting Personal Data.

Where Keywords Studios is a Data Processor, it is a requirement for the Records of Processing Activities to contain, as a minimum, the following information:

- The name and contact details of the Data Processor and of each Data Controller on behalf of which Keywords Studios is acting, and, where applicable, of the Data Controller's or the Data Processor's representative, and the data protection officer.
- The categories of Processing carried out on behalf of each Data Controller.
- The Third Country that Keywords Studios transfers Personal Data to.
- The safeguards in place for Personal Data transfers to a Third Country or international organisation where relevant.
- A description of the technical and security measures for protecting Personal Data.

Records of Processing Activities must be updated:

- Annually.
- Prior to the implementation of any new initiative, change or project affecting how Personal Data is Processed.

#### Entity and Group Function Roles and Responsibilities


Each Entity Head and Group Function Director is accountable for:

- Ensuring their teams have completed any assigned training (see section 3.26 **Training**) to understand lawful basis requirements.
- Delegating a person to be responsible for maintaining the Records of Processing Activities with support from the Global Privacy Office.
- Delegating a person to be responsible for providing annual confirmation to the Global Privacy Office that Records of Processing remain accurate and up to date.

#### Global Privacy Office Responsibilities

The Global Privacy Office shall be responsible for:

- Developing and maintaining Group Operating Standards and/or Group Guidelines to support the management of Records of Processing Activities.

 <b>Keywords Studios</b> Imagine More	Document Title	Document No. <i>Click to enter Doc No.</i>	Version <b>2.6</b>
	<i>Data Protection Policy</i>	Last Revision Date Apr. 25, 24	Page 6 of 30

- Providing Records of Processing templates to the Entities and Group Functions.
- Providing advice and support to Entities and Group Functions in completing the Records of Processing Activities as required.

### 3.2. Lawful Basis for Processing Personal Data

#### Compliance requirements

When processing of Personal Data in scope for GDPR, it is a requirement for Keywords Studios to align with [Articles 6, 9](#) and [10](#) of the GDPR, by only Processing Personal Data when there is a Lawful Basis for Processing.

For each Processing activity, Keywords Studios must document the specific Lawful Basis for Processing, upon which the Processing relies.

Keywords Studios must ensure that the Lawful Basis for Processing relied upon is properly considered and only used when appropriate and compatible with Member State Laws and the e-Privacy Directive, regardless of whether Entities are based in the EU, in the UK or elsewhere.

The lawful basis for the of Processing Personal Data by Keywords Studios must be one of the following:


- Consent - the individual has given consent to the Processing of their Personal Data for one or more specific purposes.
- Performance of a contract - Processing is necessary for the performance of a contract to which the individual is party or in order to take steps at the request of the individual prior to entering into a contract.
- Legal obligation - is necessary for compliance with a legal obligation to which the Data Controller is subject.
- Vital interests - Processing is necessary in order to protect the vital interests of the individual or of another natural person.
- Public interests - Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.
- Legitimate Interests - processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the individual.

Where Keywords Studios determines that it relies on legitimate interests as a Lawful Basis for Processing, Keywords Studios must:

- Document the specific legitimate interest relied upon.
- Complete a Legitimate Interest Impact Assessment (“LIA”).

When Processing Special Categories of Personal Data, Keywords Studios must, in addition to ensuring there is a Lawful Basis for Processing, determine and document which of the following [Article 9](#) exemptions for Processing Special Categories of Personal Data apply:

- Explicit consent - the individual has given explicit consent to the Processing of those Personal Data for one or more specified purposes.
- Employment purposes - Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Data Controller or of the individual in the field of employment and social security and social protection law.
- Vital interest - Processing is necessary to protect the vital interests of the individual or of another natural person where the individual is physically or legally incapable of giving consent.
- Public data - Processing relates to Personal Data which is manifestly made public by the individual.
- Legal claims - Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
- Substantial public interest - Processing is necessary for reasons of substantial public interest.

 <b>Keywords Studios</b> Imagine More	Document Title	Document No. <i>Click to enter Doc No.</i>	Version <b>2.6</b>
	<i>Data Protection Policy</i>	Last Revision Date Apr. 25, 24	Page 7 of 30

- Preventative or occupational medicine - Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.
- Public interest in the area of health - Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of domestic law which provides for suitable and specific measures to safeguard the rights and freedoms of the individual, in particular professional secrecy domestic law.
- Archiving in the public interest - Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance.

Keywords Studios may only Process Personal Data about criminal convictions when the Processing is authorised by EU or Member State Laws and by providing appropriate safeguards for the rights and freedoms of individuals, regardless of whether Entities are based in EU, in the UK or elsewhere.

Where Personal Data Processing is in scope Data Protection Laws outside the scope of GDPR, and the Data Protection Law includes need to have a Legal Basis for Processing, it is a requirement for Keywords Studios to document the:

- Applicable Data Protection Laws in scope.
- Legal Basis for Processing relied upon under those Data Protection Laws.

### Entity and Group Function Roles and Responsibilities

Each Entity Head and Group Function Director is accountable for:

- Ensuring their teams have completed any assigned training to understand Lawful Basis for Processing requirements.
- Delegating a person to be responsible for maintaining the documentation with support from the Global Privacy Office.
- Documenting LIAs using templates provided by the Global Privacy Office.

### Global Privacy Office Responsibilities

The Global Privacy Office shall be responsible for:


- Developing and maintaining Group Operating Standards and/or Group Guidelines to support the management of deciding and documenting the Lawful Basis for Processing.
- Providing Lawful Basis for Processing templates to the Entities and Group Functions.
- Providing support to Entities and Group Functions with delivery of LIAs and documenting the Lawful Basis for Processing.
- Approving all Lawful Basis for Processing decisions and LIAs in conjunction with the Global Legal Team.

## 3.3. Consent Management

### Compliance requirements

When Processing Personal Data is in scope for GDPR, it is a requirement for Keywords Studios to align with [Article 7](#) of the GDPR to ensure that where consent is used as a Lawful Basis for Processing, it meets the following obligations:

- Consent is the appropriate Lawful Basis for Processing.
- The request for consent is prominent and separate from other terms and conditions.
- Individuals are asked to positively opt in and pre-ticked boxes or any other type of default consent shall not be used.
- Clear and plain language is used.
- Information about the purpose of Processing is supplied.
- Individuals are given granular options to consent separately to different purposes and types of Processing.

 <b>Keywords Studios</b> Imagine More	Document Title	Document No. <i>Click to enter Doc No.</i>	Version <b>2.6</b>
	<i>Data Protection Policy</i>	Last Revision Date Apr. 25, 24	Page 8 of 30

- Keywords Studios or any third-party Data Controllers relying on the consent are named.
- Consent is as easy to withdraw as it is to give.
- Individuals can refuse consent without detriment.
- Consent is not a precondition of a service.
- Consent is freely given.
- Dark patterns are not used to gain consent.
- Where Keywords Studios is acting as Data Controller in designing services for children, consent shall only be used where there are age-verification measures (and parental-consent measures for younger children) in place.
- There is record of when and how consent was captured.

When Keywords Studios Processes Personal Data that is subject to Data Protection Laws outside the scope of GDPR, it is a requirement to manage consent in line with the applicable Data Protection Laws.

### Entity and Group Function Roles and Responsibilities

Each Entity Head and Group Function Director is accountable for:

- Ensuring their teams have completed any assigned training to understand consent requirements.
- Assigning a person responsible for:
  - Validating that consent is captured in line with the requirements outlined in this Policy.
  - Implementing the technical means to deliver consent management in line with this Policy.
  - Engaging the Global Privacy Office when support or advice is required on consent management practices.

### Global Privacy Office Responsibilities

The Global Privacy Office shall be responsible for:

- Developing and maintaining Group Operating Standards and/or Group Guidelines to support consent management.
- Providing advice and support to the Entity or Group Function.

## 3.4. Transparency


### Compliance requirements

When Processing Personal Data is in scope for GDPR, it is a requirement for Keywords Studios to align with [Articles 12, 13](#) and [14](#) of the GDPR to ensure that the provisions are accounted for in communications to individuals regarding:

- Information related to fair Personal Data Processing.
- Information about their rights and how to exercise them.

When Personal Data is collected directly from the individual, Keywords Studios must provide the following information at the time the Personal Data is obtained:

- The identity and the contact details of the Data Controller and, where applicable, of the Data Controller's representative.
- The contact details of the Data Protection Officer, where applicable.
- The intended purposes of the Processing of the Personal Data.
- Where relevant, the Lawful Basis for Processing.
- Where relevant, the legitimate interests pursued by the Data Controller or by a third party.
- The recipients or categories of recipients of the Personal Data.
- Information about transfers of Personal Data to a Third Country.
- The period for which the Personal Data shall be stored, or if that is not possible, the criteria used to determine that period.

 <b>Keywords Studios</b> Imagine More	Document Title	Document No. <i>Click to enter Doc No.</i>	Version <b>2.6</b>
	<i>Data Protection Policy</i>	Last Revision Date Apr. 25, 24	Page 9 of 30

- The existence of individual rights and how to exercise them.
- Where applicable, the existence of the right to withdraw consent at any time, without affecting the lawfulness of Processing based on consent before its withdrawal.
- Information about the right to lodge a complaint with a supervisory authority.
- Whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the individual is obliged to provide the Personal Data and of the possible consequences of failure to provide such data.
- The existence of automated decision-making, including profiling and meaningful information about the logic involved and consequences of such Processing for the individual.

Where Personal Data relating to an individual has not been obtained directly from the individual, Keywords Studios must provide the individual with information about which source the Personal Data originated from.

Transparency information must be provided to the individual at the earliest of the following:

- Within one month of obtaining the Personal Data.
- At the first communication with the individual.

When Keywords Studios Processes Personal Data that is subject to Data Protection Laws outside the scope of GDPR, it must provide individuals with information required by GDPR outlined above, together with any further information required by the applicable Data Protection Laws.

The provision of information outlined in this section must be supplied through a Privacy Notice.

- Privacy Notices must be updated annually or prior to the implementation of any new initiative, change or project affecting Personal Data Processing.

Entities may develop specific Privacy Notices, provided compliance with this Policy.

Where the Entity has its own Privacy Notice, the Global Privacy Office shall provide guidance to Entities and advice as required.

Entity specific Privacy Notices shall be approved by the Global Privacy Office.

## Entity and Group Function Roles and Responsibilities

Each Entity Head or Group Function Director is accountable for:

- Ensuring their teams have completed any assigned training to understand transparency requirements.
- Informing the Global Privacy Office if changes are required to the Keywords Studios Privacy Notice because of the implementation of any new initiative, change or project affecting Personal Data Processing.


Each Entity Head is accountable for:

- Engaging the Global Privacy Office to determine whether it is more appropriate to use the global Keywords Studios Privacy Notice or to develop an Entity specific Privacy Notice.
- Making links to the Privacy Notice available on the Entity website at the bottom every web page.
- Developing and maintaining any Entity specific Privacy Notices.
- Obtaining approval from the Global Privacy Office that an Entity Privacy Notice is fit for purpose.

## Global Privacy Office Responsibilities

The Global Privacy Office shall be responsible for:

- Developing and maintaining Group Operating Standards and/or Group Guidelines to support transparency management.
- Developing and maintaining the group Keywords Studio Privacy Notice, annually, or when otherwise required, in collaboration with the Global Legal Team.
- Providing support and advice to Entities and Group Functions on transparency management, as required.
- Approving Entity Privacy Notices.

 <b>Keywords Studios</b> Imagine More	Document Title	Document No. <i>Click to enter Doc No.</i>	Version <b>2.6</b>
	<i>Data Protection Policy</i>	Last Revision Date Apr. 25, 24	Page 10 of 30

### 3.5. Personal Data Access Rights

#### Compliance Requirements

When Processing Personal Data in scope for GDPR, it is a requirement for Keywords Studios to align with [Article 15](#) of the GDPR which gives individuals the right to:

- Obtain from the Data Controller confirmation as to whether Personal Data concerning them are being Processed.
- Access to their Personal Data.
- Obtain additional information about Processing activities.

When Processing Personal Data that is subject to Data Protection Laws outside the scope of GDPR, Keywords Studios will fulfil access requests when the relevant Data Protection Laws mandate this.

Access requests will only be fulfilled subject to the positive identification of the individual.

Access requests must be completed within one month of identity verification, except:

- Where applicable Data Protection Laws mandate it is completed sooner.
- For exceptional circumstances, in which an extension is approved by the Global Head of Privacy and the individual has been informed that an extension is required.

Access requests will not be declined without both:

- Approval from the Global Head of Privacy.
- Evidence and that the request is excessive and unfounded.

Privacy Notices must inform individuals about access rights and how to make a Personal Data access request.

#### Entity and Group Function Roles and Responsibilities

Each Entity Head and Group Function Director is accountable for ensuring their teams:

- Have completed any assigned training to recognise access requests.
- Immediately forward any access request to [privacy@keywordstudios.com](mailto:privacy@keywordstudios.com), unless the Global Privacy Office have approved an alternative process.
- Work with the Group Privacy Office to fulfil access requests within the timelines set out in this Policy.

#### Global Privacy Office Responsibilities


The Global Privacy Office shall be responsible for:

- Managing the end-to-end lifecycle of managing access requests with cooperation from the Entity and Business Function with whom the request is associated.
- Logging and monitoring access requests.
- Developing and maintaining Group Operating Standards and/or Group Guidelines to support the management of Personal Data access requests.
- Providing advice and support to the Entity or Group Function.

### 3.6. Portability Rights

#### Compliance Requirements

When Processing Personal Data in scope for GDPR, it is a requirement for Keywords Studios to align with [Article 20](#) of the GDPR which gives individuals the right to receive the Personal Data concerning them and transmit that data to another Data Controller.

 <b>Keywords Studios</b> Imagine More	Document Title	Document No. <i>Click to enter Doc No.</i>	Version <b>2.6</b>
	<i>Data Protection Policy</i>	Last Revision Date Apr. 25, 24	Page 11 of 30

When Processing Personal Data that is subject to Data Protection Laws outside the scope of GDPR, Keywords Studios shall fulfil portability requests when the relevant Data Protection Laws mandate this, for example certain United States (“US”) state laws.

Portability requests will only be fulfilled subject to the positive identification of the individual.

Portability requests must be completed within one month of identity verification, except:

- Where applicable Data Protection Laws mandate it is completed sooner.
- For exceptional circumstances, in which an extension is approved by the Global Head of Privacy and the individual has been informed that an extension is required.

Portability requests may not be declined without approval from the Global Head of Privacy.

Privacy Notices must inform individuals about portability rights and how to make a portability request.

### Entity and Group Function Roles and Responsibilities

Each Entity Head and Group Function Director is accountable for ensuring their teams:

- Have completed any assigned training to recognise portability requests.
- Work with the Group Privacy Office to fulfil portability requests within the timelines set out in this Policy.
- Immediately forward any portability requests to [privacy@keywordsstudios.com](mailto:privacy@keywordsstudios.com), unless the Global Privacy Office have approved an alternative process.

### Global Privacy Office Responsibilities

The Global Privacy Office shall be responsible for:

- Managing the end-to-end lifecycle of managing all portability requests with cooperation from the Entity and Group Function with whom the request is associated.
- Logging and monitoring portability requests.
- Developing and maintaining Group Operating Standards and/or Group Guidelines to support the management of portability requests.
- Providing advice and support to the Entity or Group Function.

## 3.7. Rectification Rights

### Compliance requirements

When Processing Personal Data in scope for GDPR, it is a requirement for Keywords Studios to align with [Article 16](#) of the GDPR which gives individuals the right to request, without undue delay:

- The rectification of inaccurate Personal Data concerning them.
- For incomplete Personal Data records to be completed.

As a commitment to aligning with the principle of accuracy, Keywords Studios shall extend this right to all individuals outside the scope of GDPR.


Rectification requests will only be fulfilled subject to the positive identification of the individual.

Rectification requests should generally be completed immediately upon request and should always be completed within one month of identity verification, except:

- Where applicable Data Protection Laws mandate it is completed sooner.
- For exceptional circumstances in which an extension is approved by the Global Head of Privacy and the individual has been informed that an extension is required.

Rectification requests may not be declined without approval from the Global Head of Privacy.

Privacy Notices must inform individuals about rectification rights and how to make a rectification request.

 <b>Keywords Studios</b> Imagine More	Document Title	Document No. <i>Click to enter Doc No.</i>	Version <b>2.6</b>
	<i>Data Protection Policy</i>	Last Revision Date Apr. 25, 24	Page 12 of 30

### Entity and Group Function Roles and Responsibilities

Each Entity Head and Group Function Director is accountable for ensuring their teams:

- Have completed any assigned training to recognise rectification requests.
- Manage rectification request in line with this Policy and/or Group Operating Standards and Group Guidelines issued by the Global Privacy Office.
- Obtaining approval from the Global Head of Privacy to decline a request.

### Global Privacy Office Responsibilities

The Global Privacy Office shall be responsible for:

- Forwarding rectification requests received by [privacy@keywordstudios.com](mailto:privacy@keywordstudios.com) to the relevant Entity or Group Function as appropriate.
- Developing and maintaining Group Operating Standards and/or Group Guidelines to support the management of rectification requests.
- Providing advice and support to the Entity or Group Function.

## 3.8. Data Deletion Rights

### Compliance Requirements

When Processing Personal Data in scope for GDPR, Keywords Studios is required to align with [Article 17](#) of the GDPR, which gives individuals the right to obtain from the Data Controller the deletion of Personal Data concerning them without undue delay.

When Processing Personal Data that is subject to Data Protection Laws outside the scope of GDPR, Keywords Studios shall fulfil data deletion requests when the relevant Data Protection Laws mandate this.

Deletion requests will only be fulfilled subject to the positive identification of the individual.

Deletion requests must be completed within one month of identity verification, except:

- Where applicable Data Protection Laws mandate that it is completed sooner.
- For exceptional circumstances in which an extension is approved by the Global Head of Privacy and the individual has been informed that an extension is required.

For requests in scope of GDPR, Personal Data can only be erased if:


- They are no longer necessary in relation to the purposes for which they were collected or otherwise Processed.
- The individual withdraws consent on which the Processing is based and there is no other lawful basis for the Processing.
- The individual objects to the Processing based on legitimate interests and their rights and freedoms override the legitimate interests of Keywords Studios and there is no other Lawful Basis for Processing.
- The individual objects to direct marketing and Keywords Studios are not holding the data for any other purpose.
- The Personal Data has been unlawfully Processed.
- The Personal Data must be erased for compliance with a legal obligation in EU or Member State Laws to which the Data Controller is subject.

Privacy Notices must inform individuals about deletion rights and how to make a deletion request.

### Entity and Group Function Roles and Responsibilities

Each Entity Head and Group Function Director is accountable for ensuring their teams:

- Have completed any assigned training to recognise data deletion requests.
- Immediately forward any deletion requests to [privacy@keywordstudios.com](mailto:privacy@keywordstudios.com), unless the Global Privacy Office have approved an alternative process.
- Work with the Group Privacy Office to fulfil a deletion request within the timelines set out in this Policy.

	Document Title  <i>Data Protection Policy</i>	Document No. <i>Click to enter Doc No.</i>	Version <b>2.6</b>
		Last Revision Date Apr. 25, 24	Page 13 of 30

## Global Privacy Office Responsibilities

The Global Privacy Office shall be responsible for:

- Managing the end-to-end lifecycle of managing data deletion requests with cooperation from the Entity or Group Function with whom the request is associated.
- Logging and monitoring deletion requests.
- Developing and maintaining Group Operating Standards and/or Group Guidelines to support the management of deletion requests.
- Providing advice and support to the Entity or Group Function.

## 3.9. Restriction Rights

### Compliance Requirements

When Processing Personal Data in scope for GDPR, it is requirement for Keywords Studios to align with [Article 18](#) of the GDPR, which gives an individual the right to request that the Data Controller restrict Processing of Personal Data when one of the following apply:

- The accuracy of the Personal Data is contested by the individual, for a period enabling the Data Controller to verify the accuracy of the Personal Data.
- The Processing is unlawful and the individual opposes the erasure of the Personal Data and requests the restriction of use instead.
- The Data Controller no longer needs the Personal Data for the purposes of the Processing, but they are required to retain the Personal Data by the individual for the establishment, exercise or defence of legal claims.
- The individual has objected to Processing pursuant to [Article 21\(1\)](#) pending the verification whether the legitimate grounds of the Data Controller override those of the individual.

When Processing Personal Data that is subject to Data Protection Laws outside the scope of GDPR, Keywords Studios shall fulfil restriction of Processing requests when the relevant Data Protection Laws mandate this, for example the CCPA's right to 'Limit Use and Disclosure of Sensitive Personal Information'.

Restriction of Processing requests will only be fulfilled subject to the positive identification of the individual.

Restriction of Processing requests must be completed within one month of identity verification, except:

- Where applicable Data Protection Laws mandate it is completed sooner.
- For exceptional circumstances, in which an extension is approved by the Global Head of Privacy and the individual has been informed that an extension is required.

Restriction of Processing requests may not be declined without approval from the Global Head of Privacy.

Privacy Notices must inform individuals about the right to restrict Personal Data Processing and how to make a request to restrict Personal Data Processing.

## Entity and Group Function Roles and Responsibilities


Each Entity Head and Group Function Director is accountable for ensuring their teams:

- Have completed any assigned training to recognise restriction of Processing requests.
- Immediately forward any restriction of Processing requests to [privacy@keywordstudios.com](mailto:privacy@keywordstudios.com), unless the Global Privacy Office have approved an alternative Process.
- Work with the Group Privacy Office to fulfil a deletion request within the timelines set out in this Policy.

## Global Privacy Office Responsibilities

The Global Privacy Office shall be responsible for:

- Managing the end-to-end lifecycle of managing restriction of Processing requests with cooperation from the Entity or Group Function with whom the request is associated.

 <b>Keywords Studios</b> Imagine More	Document Title	Document No. <i>Click to enter Doc No.</i>	Version <b>2.6</b>
	<i>Data Protection Policy</i>	Last Revision Date Apr. 25, 24	Page 14 of 30

- Logging and monitoring restriction of Processing requests.
- Developing and maintaining Group Operating Standards and/or Group Guidelines to support the management of restriction requests.
- Providing advice and support to the Entity or Group Function.

### 3.10. Right to Object

#### Compliance Requirements

When Processing Personal Data in scope for GDPR, it is a requirement for Keywords Studios to align with [Article 21](#) of the GDPR which gives the Individual the right to:

- Object to the Processing of Personal Data relying on the Lawful Basis of Processing of legitimate interests.
- Object to direct marketing.

When Processing Personal Data that is subject to Data Protection Laws outside the scope of GDPR, is it a requirement for Keywords Studios to fulfil objections to processing when the relevant Data Protection Laws mandate this.

Objections to processing will only be fulfilled subject to the positive identification of the individual.

Objections to processing must be completed within one month of identity verification, except:

- Where Data Protection Laws mandate it is completed sooner.
- For exceptional circumstances in which an extension is approved by the Global Head of Privacy and the individual has been informed that an extension is required.

Objections to marketing must always be honoured.

Privacy Notices must inform individuals about their right to object to Processing and how to submit a request.

#### Entity and Group Function Roles and Responsibilities

Each Entity Head and Group Function Director is accountable for ensuring their teams:

- Have completed any assigned training to recognise objections to Processing and objections to marketing.
- Put in place unsubscribe options, in line with the marketing section of this Policy, when undertaking marketing.
- Immediately forward all objection to Processing requests, that are not marketing related, to [privacy@keywordsstudios.com](mailto:privacy@keywordsstudios.com), unless the Global Privacy Office has approved an alternative process.

#### Global Privacy Office Responsibilities

The Global Privacy Office shall be responsible for:


- Managing the end-to-end lifecycle of managing objection to Processing requests that are not related to marketing, with cooperation from the Entity or Business Function with whom the request is associated.
- Logging and monitoring all objection to Processing requests not related to marketing
- Developing and maintaining Group Operating Standards and/or Group Guidelines to support the management of objection to Processing requests.
- Providing advice and support to the Entity or Group Function.

### 3.11. Automated Decision Making and Profiling

#### Compliance Requirements

When Processing Personal Data in scope for GDPR, it is a requirement for Keywords Studios to align with [Article 22](#) of the GDPR which states that organisations may not make decisions, based solely on automated Processing, including profiling, which produces legal effects or similar effects, about the individual unless one of the following apply:

- It is necessary for entering into, or performance of, a contract between the individual and Keywords Studios.
- It is authorised by Member State Laws to which Keywords Studios is subject to.

 <b>Keywords Studios</b> Imagine More	Document Title	Document No. <i>Click to enter Doc No.</i>	Version <b>2.6</b>
	<i>Data Protection Policy</i>	Last Revision Date Apr. 25, 24	Page 15 of 30

- The individual has provided explicit consent.

If Keywords Studios is making decisions in line with above then they must:

- Provide the facility for the individual to express their point of view, to contest the decision and to request human intervention to reevaluate the decision.
- Inform the Individual that automated decision making shall be taking place.
- Provide a clear logic behind the decision making.

Where possible, as best practice, Keywords Studios shall also align with the principles outlined above when Processing of Personal Data outside the scope of GDPR.

Where relevant Data Protection Laws apply, for example US state laws, Keywords Studios must also allow users to opt-out of profiling, regardless of whether it produces a legal effect.

Requests relating to automated decision making rights and profiling must be completed within one month of identity verification, except:

- Where applicable Data Protection Laws mandate that the request is completed sooner.
- For exceptional circumstances, in which an extension is approved by the Global Head of Privacy and the individual has been informed that an extension is required.

Privacy Notices must inform individuals about automated decision making rights and how to contest a decision or request human intervention.

### Entity and Group Function Roles and Responsibilities

Each Entity Head and Group Function Director is accountable for ensuring their teams:

- Have completed any assigned training to understand how to recognise requests associated automated decision making rights and profiling.
- Seek approval from the Global Privacy Office before implementing any form of automated decision making or profiling.
- Immediately forward any automated decision-making requests to [privacy@keywordsstudios.com](mailto:privacy@keywordsstudios.com), unless the Global Privacy Office have approved an alternative process.
- Work with the Group Privacy Office to fulfil access requests within the timelines set out in this Policy.

### Global Privacy Office Responsibilities

The Global Privacy Office shall be responsible for:

- Managing the end-to-end lifecycle of requests connected with automated decision-making rights and profiling with cooperation from the Entity or Group Function with whom the request is associated.
- Logging and monitoring automated decision-making rights and profiling requests.
- Developing and maintaining Group Operating Standards and/or Group Guidelines to support the management of requests associated with automated decision-making rights and profiling.
- Providing advice and support to the Entity or Group Function.

## 3.12. Selling, Sharing and Targeted Advertising

### Compliance Requirements

When Processing Personal Data in scope for relevant US state laws, it is a requirement for Keywords Studios to respect the right for a consumer to opt out of the sale of Personal Data about them to third parties.

Keywords Studios understands that sharing Personal Data with a third party "for monetary or other valuable consideration" is considered the same as selling data.

The Global Head of Privacy must approve all decisions to sell Personal Data or to undertake targeted advertising on individuals in the US.

 <b>Keywords Studios</b> Imagine More	Document Title	Document No. <i>Click to enter Doc No.</i>	Version <b>2.6</b>
	<i>Data Protection Policy</i>	Last Revision Date <b>Apr. 25, 24</b>	Page 16 of 30

Privacy Notices connected to such Processing in scope for relevant US state laws must inform individuals about do not sell rights and how to request that their Personal Data is not sold, unless the Entity does not sell Personal Data or share it with third parties for other valuable consideration, in which case it is still best practice to maintain a 'do not sell page' on the relevant website and utilise it to confirm to the user that Personal Data is not sold.

### Entity and Group Function Roles and Responsibilities

Each Entity Head and Group Function Director is accountable for ensuring:

- Their teams have completed any assigned training understand how to manage selling, sharing and targeted advertising.
- Their teams seek approval from the Global Privacy Office before implementing any sale of Personal Data.
- Any US website they manage includes a 'Do not sell my Personal Data' link at the bottom of each page, containing information on consumers' right to opt out of the sale of their data.
- The technical means for the User to opt-out of their personal information being sold or shared are implemented.
- That the Privacy Notice reflects any approved selling or sharing of Personal Data.

### Global Privacy Office Responsibilities

The Global Privacy Office shall be responsible for:

- Developing and maintaining Group Operating Standards and/or Group Guidelines to support the management of requests associated with US do not sale and targeted advertising rights.
- Providing advice and support to the Entity or Group Function.

## 3.13. Appeals

### Compliance Requirements

When Processing Personal Data in scope for relevant US state laws, it is a requirement for Keywords Studios to allow individuals to appeal if Keywords Studios reject or decline a privacy rights request.

Appeals outside the scope of US state privacy laws shall be managed in line with relevant Data Protection Laws.

Information about appeals must be available in all Privacy Notices connected to Processing in scope for relevant US state laws.

### Entity and Group Function Roles and Responsibilities

Each Entity Head and Group Function Director is accountable for ensuring their teams:

- Have completed any assigned training to understand how to recognise appeal requests.
- Immediately forward all appeals to [privacy@keywordstudios.com](mailto:privacy@keywordstudios.com).

### Global Privacy Office Responsibilities


The Global Privacy Office shall be responsible for:

- Managing the end-to-end lifecycle of managing appeals with cooperation from the Global Legal Team as appropriate.
- Logging and monitoring appeals.
- Developing and maintaining Group Operating Standards and/or Group Guidelines to support the management of appeals.
- Providing advice and support to the Entity or Group Function.

## 3.14. Data Protection Complaints

### Compliance Requirements

Keywords Studios must take all complaints about data protection and privacy seriously and deal with them promptly.

 <b>Keywords Studios</b> Imagine More	Document Title  <i>Data Protection Policy</i>	Document No. <i>Click to enter Doc No.</i>	Version  <b>2.6</b>
		Last Revision Date Apr. 25, 24	Page 17 of 30

All complaints must:

- Be logged and acknowledged.
- Responded to within 30 days, or sooner if legislation requires.

### Entity and Group Function Roles and Responsibilities

Each Entity Head and Group Function Director is accountable for ensuring:

- Their teams have completed any assigned training to recognise a complaint.
- All data protection and privacy complaints are immediately sent to [privacy@keywordsstudios.com](mailto:privacy@keywordsstudios.com).
- Their teams collaborate with the Global Privacy Office to investigate and resolve the complaint promptly.
- On the advice of the Global Privacy Office, that action is taken to mitigate future complaints.

### Global Privacy Office Responsibilities

The Global Privacy Office shall be responsible for:

- Managing the end-to-end lifecycle of complaints with cooperation from the Entity or Group Function with whom the request is associated.
- Logging and monitoring complaints.
- Developing and maintaining Group Operating Standards and/or Group Guidelines to support the management of complaints
- Supporting the Entity or Group Function in implementing measures to remediate complaints or mitigate future complaints.
- Providing advice and support to the Entity or Group Function as required.

## 3.15. Data Protection by Design and Default

### Compliance Requirements

It is a requirement for Keywords Studios to adopt a Data Protection by Design approach in the development of:

- All products and services involving the use of Personal Data.
- All Processes involving the use of Personal Data.

Keywords Studios must implement Data Protection by Design in respect of:


- The amount of Personal Data collected.
- The extent of its Processing.
- The period of its storage.
- The accessibility of Personal Data.
- The security and protection of Personal Data.
- The individual's ability to fulfil their individual rights.
- The transparency of the Processing taking place.
- Risks to the rights and freedoms of individuals.

### Entity and Group Function Roles and Responsibilities

Each Entity Head and Group Function Director is accountable for ensuring their teams:

- Have completed any assigned training to understand the concepts and practical application of Data Protection by Design and default.
- Engage the Group Privacy Office at [privacy@keywordsstudios.com](mailto:privacy@keywordsstudios.com) for guidance when implementing systems, developing services and processes involving Personal Data.
- Assess the need for a Data Protection Impact Assessment, as per the next section.
- Ensure all data protection requirements are factored into the initiative or development as a default setting.

### Global Privacy Office Responsibilities

 <b>Keywords Studios</b> Imagine More	Document Title	Document No. <i>Click to enter Doc No.</i>	Version <b>2.6</b>
	<i>Data Protection Policy</i>	Last Revision Date Apr. 25, 24	Page 18 of 30

The Global Privacy Office shall be responsible for:

- Developing and maintaining Group Operating Standards and/or Group Guidelines to the facilitate embedding Data Protection by Design.
- Providing guidance and advice as required.
- Supporting the Entity or Group Function in developing practical solutions to embed Data Protection by Design into their initiatives.

### 3.16. Data Protection Impact Assessments

#### Compliance Requirements

As part of Keywords Studios commitment to Data Protection by Design, the need for a Data Protection Impact Assessment (“**DPIA**”) must be assessed when:

- There is a new initiative or project involving the Processing of Personal Data.
- There is a change in the purpose or method of Processing Personal Data.
- A new service or software provider is engaged.
- An Entity or Group Function becomes aware of a risk or issue which:
  - Triggers the need for a DPIA.
  - Was not considered as part of an original DPIA.

#### Entity and Group Function Roles and Responsibilities

Each Entity Head and Group Function Director is accountable for ensuring their teams:

- Have completed any assigned training to understand when a DPIA is needed.
- Assigning someone responsible for:
  - Keeping track of initiatives involving the Processing of Personal Data.
  - Working with the Global Privacy Office to assess the need for a DPIA.
  - Executing the DPIA in collaboration with the Global Privacy Office and providing enough information to make a meaningful assessment of the data protection and privacy risks.
  - Reviewing DPIAs at least every two years to ensure they remain accurate and up to date.
- Approving the DPIAs and deciding whether Personal Data Processing may proceed when risks are evaluated as low by the Global Privacy Office.


#### Global Privacy Office Responsibilities

The Global Privacy Office shall be responsible for:

- Developing and maintaining Group Operating Standards and/or Group Guidelines on DPIAs.
- Publishing, and maintaining, DPIA templates for use by Entities and Group Functions.
- Maintaining a log of all decisions about whether a DPIA is required, along with the rationale.
- Supporting the business in the execution of DPIAs.
- Identifying risks and possible mitigations, and advising on the level of risk.
- Making recommendations on whether Processing may proceed.
- Advising the business on whether the Processing requires referral to a supervisory authority or government agency.
- Providing advice, support and recommendations to the Entity or Group Function.
- Logging risks associated with the Processing.
- Escalating risks to the Executive Leadership Team for approval if the risk is medium or high.

#### Executive Leadership Team Responsibilities

It is the responsibility of the Executive Leadership Team to:

 <b>Keywords Studios</b> Imagine More	Document Title	Document No. <i>Click to enter Doc No.</i>	Version <b>2.6</b>
	<i>Data Protection Policy</i>	Last Revision Date Apr. 25, 24	Page 19 of 30

- Approve the acceptance of any risks that are evaluated by the Global Privacy office which are medium or high.

### 3.17. Data Minimisation

#### Compliance Requirements

When collecting and Processing Personal Data, it is a requirement for Keywords Studios to comply with the GDPR principle of data minimisation, regardless of whether the Processing is in scope of GDPR or other Data Protection Laws.

All Personal Data collected and Processed shall be adequate, relevant and limited to what is necessary.

Data minimisation must be considered at all stages of the end-to-end lifecycle of Personal Data Processing, not just at data capture.

Data minimisation must be considered when implementing access controls.

It is strictly prohibited to collect or retain data 'just in case'. The Entity or Group Function must be able to justify the need for all Personal Data collection, use and access.

#### Entity and Group Function Roles and Responsibilities

Each Entity Head and Group Function Director is accountable for ensuring:

- Their teams have completed any assigned training to understand the concept and application of data minimisation.
- That individuals responsible for implementing processes and systems involving Personal Data Processing understand it is their responsibility to align with the principle of data minimisation.
- Their teams engage the Global Privacy Office when support is required to determine whether Personal Data collected is adequate, relevant, and limited to what is necessary.

#### Global Privacy Office Responsibilities

The Global Privacy Office shall be responsible for:

- Developing and maintaining Group Operating Standards and/or Group Guidelines to support the management of data minimisation.
- Supporting the Entity or Group Function in implementing measures to ensure data minimisation is practiced.

### 3.18. Storage Limitation

#### Compliance Requirements

When collecting and Processing Personal Data, Keywords Studios must align with the GDPR principle of storage limitation, regardless of whether the Processing is in scope of GDPR or other Data Protection Laws.


Personal Data must be anonymised or deleted from all systems, databases and back-ups when it is no longer required for the purpose for which it was collected.

#### Entity and Group Function Roles and Responsibilities

Each Entity Head and Group Function Director is accountable for:

- Ensuring their teams have completed any assigned training to understand the concept and application of storage limitation.
- Putting in place operational and technical means for deleting the Personal Data when it is no longer required for the purpose for which it was collected.
- Validating that Personal Data is deleted securely and in such a way that it cannot be recovered.
- Ensuring their teams engage the Global Privacy Office when support is required.

#### Global Privacy Office Responsibilities

	Document Title	Document No. <i>Click to enter Doc No.</i>	Version <b>2.6</b>
	<i>Data Protection Policy</i>	Last Revision Date Apr. 25, 24	Page 20 of 30

The Global Privacy Office shall be responsible for:

- Developing and maintaining Group Operating Standards and/or Group Guidelines to support the execution of storage limitation.
- Supporting the Entity or Group Function in implementing measures to ensure storage limitation is practiced.

### 3.19. Purpose Limitation

#### Compliance Requirements

When collecting and Processing Personal Data, Keywords Studios must align with the GDPR principle of Purpose Limitation, regardless of whether the Processing is in scope of GDPR or other Data Protection Laws.

Personal Data shall be collected and processed for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes.

In the event Keywords Studios wishes to Process Personal Data for a purpose other than that communicated to the individual, then consent must be obtained if the Processing is not compatible with the original purpose and there is no other lawful basis which can be relied upon.

#### Entity and Group Function Roles and Responsibilities

Each Entity Head and Group Function Director is accountable for:

- Ensuring their teams have completed any assigned training to understand the concept and application of purpose limitation.
- Ensuring their teams engage the Global Privacy Office when support is required to determine whether Personal Data Processing falls within the stated purpose.

#### Global Privacy Office Responsibilities

The Global Privacy Office shall be responsible for:

- Developing and maintaining Group Operating Standards and/or Group Guidelines to support the execution of purpose limitation.
- Supporting the Entity or Group Function in implementing measures to ensure storage limitation is practiced.

### 3.20. Personal Data Breaches

#### Compliance Requirements

When Processing Personal Data in scope for GDPR, it is a requirement for Keywords Studios to align with [Article 33](#) and [34](#) of the GDPR which obliges Keywords Studios to:


- Report Personal Data Breaches to the relevant supervisory authority within 72 hours of becoming aware of the breach, unless the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of natural persons.
- Report Personal Data Breaches to the individual without undue delay when there is a high risk to the rights and freedoms of individuals.

When Processing Personal Data that is subject to Data Protection Laws outside the scope of GDPR, it is a requirement for Keywords Studios to report breaches to authorities and agencies in line with the relevant Data Protection Law.

All Personal Data Breaches and suspected Personal Data Breaches must be treated as the highest priority and handled in line with Keywords Studios' Group Operating Standards in respect of Personal Data Breaches.

#### Entity and Group Function Roles and Responsibilities

Each Entity Head and Group Function Director is accountable for ensuring their teams:

 <b>Keywords Studios</b> Imagine More	Document Title	Document No. <i>Click to enter Doc No.</i>	Version <b>2.6</b>
	<i>Data Protection Policy</i>	Last Revision Date Apr. 25, 24	Page 21 of 30

- Have completed any assigned training to understand how to recognise the different types of Personal Data Breaches.
- Immediately report any suspected Personal Data Breaches to [privacy@keywordstudios.com](mailto:privacy@keywordstudios.com).
- Cooperate with all efforts to investigate, contain, remediate and mitigate Personal Data Breaches, as a priority.

### Global Privacy Office Responsibilities

The Global Privacy Office shall be responsible for:

- Developing and maintaining Group Operating Standards and/or Group Guidelines to manage Personal Data Breaches.
- Maintaining a central log all Personal Data Breaches and suspected Personal Data Breaches.
- Advising on whether the Personal Data Breach is reportable to the authorities and individuals whose Personal Data is involved.
- Making recommendations on the activities required to investigate, contain, remediate and mitigate the Personal Data Breach.
- Cooperating with Information Security when the Personal Data Breach is being handled under the Incident Management Policy.
- Engaging the Global Legal Team as required.
- Coordinating efforts to report to:
  - The supervisory authority.
  - Government agencies.
  - Individuals, as appropriate

## 3.21. Transfers of Personal Data to Third Countries

### Compliance Requirements

When Processing Personal Data in scope for GDPR, it is a requirement for Keywords Studios to align with the requirements laid out by [Article 46](#) of the GDPR which oblige Keywords Studios to implement the appropriate mechanisms for transfers of Personal Data to Third Countries or international organisations.

Mechanisms used by Keywords Studios shall include:

- A Commission decision that the Third Country, a territory or one or more specified sectors within that Third Country, or the international organisation in question, ensures an adequate level of protection.
- Appropriate safeguards.

Any transfer relying on appropriate safeguards must undergo a Transfer Impact Assessment before the transfer is performed.

When Processing Personal Data that is subject to Data Protection Laws outside the scope of GDPR, Keywords Studios shall manage transfers to Third Countries in line with the relevant Data Protection Laws, including gaining consent for the transfer, where required.


Any transfer of Personal Data to Third Countries without an adequacy decision or using appropriate safeguards is strictly prohibited.

### Entity and Group Function Roles and Responsibilities

Each Entity Head and Group Function Director is accountable for ensuring their teams:

- Have completed any assigned training to understand the transfers of Personal Data and the controls required.
- Engage with the Global Privacy Office before initiating any Personal Data transfer to a Third Country.
- Support the delivery of Transfer Impact Assessment working in conjunction with the Global Privacy Office.

### Global Privacy Office Responsibilities

 <b>Keywords Studios</b> Imagine More	Document Title	Document No. <i>Click to enter Doc No.</i>	Version <b>2.6</b>
	<i>Data Protection Policy</i>	Last Revision Date Apr. 25, 24	Page 22 of 30

The Global Privacy Office shall be responsible for:

- Developing and maintaining Group Operating Standards and/or Group Guidelines to manage transfers of Personal Data abroad.
- Developing and maintaining Transfer Impact Assessment templates.
- Conducting a Transfer Impact Assessments in conjunction with Entity of Group Function wishing to make the Personal Data transfer.
- Liaising with the Global Legal Team as appropriate
- Giving advice on appropriate transfer mechanisms and safeguards.
- Maintaining a central log of the transfer of Personal Data and mechanism for transfer.

### 3.22. Third Party Engagements and Contracts

#### Compliance Requirements

When Processing Personal Data in scope for GDPR, it is a requirement for Keywords Studios to align with [Articles 26, 28, and 29](#) of GDPR, which lay out the requirements for engaging with third party Data Controllers, Joint Data Controllers and Data Processors.

When Processing Personal Data that is subject to Data Protection Laws outside the scope of GDPR, Keywords Studios must engage third parties in line with the requirements relevant Data Protection Laws.

Engagements with Data Processors or service providers acting on behalf of Keywords Studios must be governed by Data Processing Agreements, specifying the subject matter and duration of Processing, the nature and purpose of Processing, types of Personal Data, categories of individuals, and obligations and rights of Keywords Studios, in accordance with GDPR and other applicable Data Protection Laws.

Engagements with Data Controllers for whom Keywords Studios acts as Data Processor (service provider) must be governed by a Data Processing Agreement, stipulating the subject matter and duration of Processing, the nature and purpose of Processing, types of Personal Data, categories of individuals, and obligations and rights of the Customer, in compliance with GDPR and other relevant Data Protection Laws.

Engagements with Joint Data Controllers shall be governed by written agreements clearly outlining respective responsibilities for compliance with GDPR and other relevant Data Protection Laws.

When Keywords Studios is using a service provider for services involving Personal Data, a third-party privacy assessment must be completed to ensure that the third-party Data Processor offers a suitable level of data protection.

#### Entity and Group Function Roles and Responsibilities


Each Entity Head and Group Function Director is accountable for ensuring their teams:

- Have completed any assigned training to understand data protection and privacy requirements for engaging with third parties.
- Involve the Global Privacy Office when agreeing client contracts or engaging new service providers.
- Ensuring all privacy requirements stipulated by clients in Data Processing Agreements are adhered to operationally and technically.

#### Global Privacy Office Responsibilities

The Global Privacy Office shall be responsible for:

- Developing and maintaining Group Operating Standards and/or Group Guidelines about privacy requirements for third party engagements and contracts.
- Developing and maintaining Data Processing Agreements in conjunction with the Global Legal Team.
- Reviewing Data Processing Agreements and data protection contract clauses.
- Assessing and approving the privacy practices of third-party service providers.

	Document Title  <i>Data Protection Policy</i>	Document No. <i>Click to enter Doc No.</i>	Version  <b>2.6</b>
		Last Revision Date <b>Apr. 25, 24</b>	Page 23 of 30

- Maintaining a central log of all third-party service providers assessed by the Group Privacy Office.
- Providing advice and recommendations for working with third party service providers and tools.
- Supporting the completion of client privacy assessments on Entities.

### 3.23. Security, Technical and Organisational Measures

#### Compliance Requirements

It is a requirement for Keywords Studios to maintain technical and organisational measures to ensure the security of Personal Data being Processing.

Key factors to be taken into consideration when defining an appropriate level of security are the possibility of any of the following occurring in respect of the Personal Data being transmitted, stored or Processed:

- Accidental or unlawful destruction of the Personal Data.
- Loss of the Personal Data.
- Alteration of the Personal Data.
- Unauthorised disclosure of, or access to, Personal Data.

Technical and organisational measures within Keywords Studios shall focus on the following core elements:

- The pseudonymisation and encryption of Personal Data.
- Robust access controls.
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services.
- The ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident.

#### Entity and Group Function Roles and Responsibilities

Each Entity Head and Group Function Director is accountable for ensuring their teams:

- Have completed any assigned training to understand the application of security, technical and organisational measures.
- Comply with the General Information Security Policy.
- Ensure any Processing of Personal Data by service providers is subject to the same level technical and organisational measures as those adhered to by Keywords Studios.
- Engage with the Group Privacy Office when support is required.

#### Global Privacy Office Responsibilities

The Global Privacy Office shall be responsible for:

- Developing and maintaining Group Operating Standards and/or Group Guidelines on technical and organisational measures to protect Personal Data.
- Providing advice and recommendations about technical and organisational for protecting Personal Data.


### 3.24. Cookies

#### Compliance Requirements

It is a requirement that Keywords Studios only use Cookies and other tracking technologies (including pixels, SDKs, location tracking, device fingerprinting, like and share buttons), which are not strictly necessary, with consent from a website user. Such Cookies shall not be placed on a user's device until consent has been provided.

Website owners may not rely on the user to manage Cookies through their browser.

All websites operated by Keywords Studios must have the following place:

 <b>Keywords Studios</b> Imagine More	Document Title	Document No. <i>Click to enter Doc No.</i>	Version <b>2.6</b>
	<i>Data Protection Policy</i>	Last Revision Date <b>Apr. 25, 24</b>	Page 24 of 30

- A Cookies management tool, which allows the user to manage Cookies.
- A Cookies notice, which provides:
  - General information about Cookies and their purpose.
  - Detailed information about the Cookies the site collects, along with their category, use and retention.

Cookies management tools on websites must give equal prominence to ‘accept all’ and ‘reject all’ options without the need for the user to click through several options to reject cookies.

Cookies management tools must not use dark patterns to stop the user from rejecting cookies.

### Entity and Group Function Roles and Responsibilities

Each Entity Head and Group Function Director is accountable for ensuring those responsible for their website or technology:

- Have completed any assigned training to understand the compliant use of Cookies.
- Ensure the use of Cookies aligns with this Policy.
- Publish a Cookies notice using templates provided by the Global Privacy Office.
- Validate the Cookies notice accurately reflects the Cookies used on the site.
- Engage the Global Privacy Office if support is required.

### Global Privacy Office Responsibilities

The Global Privacy Office shall be responsible for:

- Developing and maintaining Group Operating Standards and/or Group Guidelines about Cookies and similar technologies.
- Producing and maintaining a template Cookies notice.
- Providing advice and recommendations about Cookies and similar technologies.

## 3.25. Marketing

### Compliance Requirements

Keywords Studios must align with global Data Protection Laws when undertaking marketing, including B2B marketing and B2C marketing.

Regardless of the applicable Data Protection Laws, all marketing communications must offer mechanisms for the recipient to opt-out of, or unsubscribe from, marketing communications.

### Entity and Group Function Roles and Responsibilities


Each Entity Head and Group Function Director whose Entity or Group Function is involved in marketing (including lead generation and sales) is accountable for ensuring:

- Their teams have completed any assigned training to understand the data protection and privacy requirements in marketing.
- Marketing aligns with Data Protection Laws.
- Ensuring those responsible for marketing activities engage the Global Privacy Office to provide advice on marketing activities.

### Global Privacy Office Responsibilities

The Global Privacy Office shall be responsible for:

- Developing and maintaining Group Operating Standards and/or Group Guidelines about privacy and data protection requirements in marketing.
- Providing advice and recommendations about privacy and data protection compliant marketing.

 <b>Keywords Studios</b> Imagine More	Document Title  <i>Data Protection Policy</i>	Document No. <i>Click to enter Doc No.</i>	Version  <b>2.6</b>
		Last Revision Date Apr. 25, 24	Page 25 of 30

### 3.26. Training

#### Compliance Requirements

It is requirement for all Keywords Studios employees to be trained on Data Protection Laws if their role involves:

- Processing Employee or client Personal Data.
- Making decisions about how Personal Data will be Processed.
- Selecting service providers to Process Personal Data on behalf of Keywords Studios.

It is expected that Employees will complete, and or attend, all data protection training assigned to them.

Failure to complete or attend assigned training could lead to disciplinary action.

#### Entity and Group Function Roles and Responsibilities

Each Entity Head and Group Function Director is accountable for ensuring their teams:

- Have the time to complete available training.
- Complete available training within the required deadline.
- Undertake refresher training annually.

#### Global Privacy Office Responsibilities

The Global Privacy Office shall be responsible for:

- Developing and assigning or delivering training to employees.
- Monitoring training completion.

### 3.27. Data Protection Officer

Where required under applicable Data Protection Laws, Keywords Studios has appointed a 'Data Protection Officer'. Where one has been appointed, contact information will be available in the Privacy Notice.

The Data Protection Officer is a key contributor to ensuring compliance with Data Protection Laws, however, they are not ultimately accountable for data protection.

The Data Protection Officer shall have the following tasks:


- To inform and advise those who carry out Personal Data Processing of their obligations under Data Protection Laws.
- To monitor compliance with Data Protection Laws and with Keywords Studios policies relating to the protection of Personal Data.
- Awareness-raising and training of staff involved in Personal Data Processing operations.
- To provide advice, where requested, about DPIAs and to monitor their performance.
- To cooperate with supervisory authorities or government agency.
- To act as the contact point for supervisory authorities, government agencies and individuals on issues relating to Personal Data Processing.
- Other responsibilities defined by global Data Protection Laws, as appropriate.

The Data Protection Officer may fulfil additional duties as required by the business if those duties do not conflict with the Data Protection Officer position.

At Keywords Studios the Data Protection Officer shall be considered part of the Global Privacy Office and therefore all references to the Global Privacy Office in this Policy include the Data Protection Officer where one has been appointed.

### 3.28. Data Protection Regulators and Government Agencies

#### Compliance Requirements

	Document Title  <i>Data Protection Policy</i>	Document No. <i>Click to enter Doc No.</i>	Version  <b>2.6</b>
		Last Revision Date Apr. 25, 24	Page 26 of 30

When Processing Personal Data in scope for GDPR, Keywords Studios it may need to cooperate with the supervisory authorities in the UK and EU in respect of:

- Enquiries.
- Complaints.
- Personal Data Breaches.

Where supervisory authorities and regulators require organisations to register or pay fees for the Processing of Personal Data, Keywords Studios must ensure the relevant registrations and payments are made and renewed as appropriate.

When Keywords Studios Processes Personal Data that is subject to Data Protection Laws outside the scope of GDPR, it will liaise with the relevant supervisory authorities appointed under the relevant Data Protection Laws.

### Entity and Group Function Roles and Responsibilities

Each Entity Head is accountable for:

- Ensuring their registrations and payments are up to date.
- Engaging the Global Privacy Office if they have any questions about registrations or payment of fees.
- Ensuring their teams forward all communications from supervisory authorities, regulators and government agencies to [privacy@keywordsstudios.com](mailto:privacy@keywordsstudios.com) unless it relates to a registration or fee payment.

### Global Privacy Office Responsibilities

The Global Privacy Office shall be:

- Responsible for providing advice on registrations and fee payments.

The point of contact for supervisory authorities, regulators and government agencies for all data protection matters, outside registrations, and all communications shall be [privacy@keywordsstudios.com](mailto:privacy@keywordsstudios.com).

## 3.29. Privacy and Data Protection Risk Management

### Compliance Requirements

Keywords Studios must maintain a central register of data protection risks.

### Entity and Group Function Roles and Responsibilities

Each Entity Head is accountable for reporting:

- Non-compliance with this Policy to the Global Privacy Office.
- Reporting risks to the Global Privacy Office.
- Remediating and mitigating risks as agreed with the Global Privacy Office.

### Global Privacy Office Responsibilities

The Global Privacy Office shall be responsible for:


- Logging all data protection risks.
- Reporting key risks to the Executive Leadership Team.
- Proposing mitigation measures.
- Providing studios guidance and advice as required.

Where appropriate the Global Privacy Office may publish Group Operating Standards and/or Group Guidelines to support these activities.

## 3.30. Accountability

### Compliance Requirements

Keywords Studios is fully accountable for complying with Data Protection Laws.

 <b>Keywords Studios</b> Imagine More	Document Title	Document No. <i>Click to enter Doc No.</i>	Version <b>2.6</b>
	<i>Data Protection Policy</i>	Last Revision Date Apr. 25, 24	Page 27 of 30

Compliance with this Policy allows Keywords Studios to demonstrate accountability and meet the requirements of Data Protection Laws globally in an auditable way.

### Executive Leadership Team Responsibilities

The Executive Leadership team must ensure that they:

- Understand the requirements of this Policy.
- Allocate the appropriate budget, time, and resources to the requirements of Data Protection Laws.

### Entity and Group Function Roles and Responsibilities

Each Entity and Group Function is accountable for complying with Data Protection Laws and ensuring all Employees are aware of this Policy.

### Global Privacy Office Responsibilities

The Global Privacy Office shall provide oversight, guidance, and advice to Entities and Group Functions to support the application of this Policy.

## 3.31. Reporting

### Compliance Requirements

To demonstrate accountability, Keywords Studios must report to the Executive Leadership Team on privacy and data protection matters.

Reporting must:

- Inform the Executive Leadership Team of the level to which data protection and privacy are operationally embedded.
- Act as a mechanism to demonstrate compliance with Data Protection Laws.

Reports must be delivered on a quarterly basis and include:

- Key Performance Indicators with a RAG status.
- Key risks.
- Information on studio level compliance.


### Global Privacy Office Responsibilities

The Global Privacy Office shall be responsible for:

- Delivering the quarterly reports to the Executive Leadership Team.
- Closely monitoring the results to:
  - Identify trends.
  - Make recommendations for mitigating action where required.
  - Adopt a culture of continuous improvement.

### Entity and Group Function Roles and Responsibilities

Each Entity Head is accountable for providing agreed information to the Global Privacy Office for quarterly reporting.

	Document Title	Document No. <i>Click to enter Doc No.</i>	Version <b>2.6</b>
	<i>Data Protection Policy</i>	Last Revision Date Apr. 25, 24	Page 28 of 30

## Glossary and Definitions

For the purposes of this Policy:

**CCPA:** The California Civil Code Sec. 1798.100 et seq. (also known as the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 or “**CPRA**”).

**Cookies:** Small text files that are stored on a user's device when they visit a website, which contain information about the user's interaction with the website and which may be used for various purposes such as remembering user preferences, analyzing website traffic, and providing personalised content and advertisements.

**Data Controller:** The organisation responsible for determining the purposes and means of Processing Personal Data. In simpler terms, a Data Controller decides why and how Personal Data should be Processed.

**Data Processing Agreement:** A contract stipulating the subject matter and duration of Processing, the nature and purpose of Processing, types of Personal Data, categories of individuals, and obligations and rights of the Customer, in compliance with GDPR and other relevant Data Protection Laws.

**Data Processor:** The organisation that Processes Personal Data on behalf of a Data Controller. Unlike the Data Controller, the Data Processor does not determine the purposes for which Personal Data is Processed, but rather handles the Personal Data as instructed by the Data Controller.

**Data Protection by Design:** Integrating data protection safeguards into products, services and all Personal Data Processing from the earliest stage of development.

**Data Protection Impact Assessment:** A documented assessment to ensure that the rights and freedoms of individuals are not adversely impacted by the Personal Data Processing in question.

**Data Protection Laws:** GDPR, e-Privacy Directive, applicable US state laws and any other relevant Data Protection Laws and codes of conduct.

**Data Protection Officer:** A data protection officer ensures, in an independent manner, that an organization applies the laws protecting individuals' personal data. The designation, position and tasks of a DPO within an organization are described in Articles 37, 38 and 39 of the GDPR.

**Employees:** All current employees, workers, individual contractors, contingent workers, consultants and directors, permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, freelancers, agency workers, volunteers, interns, agents and third parties whose information provided to us in connection with the employment, other work relationship or engagement with Keywords Studios globally.

**Entity:** Has the meaning given to it in the Executive Summary.


**Entity Head:** Each person who has been delegated with responsibility for managing an Entity.

**Executive Leadership:** The highest level of managers or directors within Keywords Studios who are responsible for determining the strategic direction and making decisions that affect its overall operations.

**GDPR:** The General Data Protection Regulation and the UK Data Protection Act 2018.

**Group Function:** The Global Legal Team, Global Finance Team, Global People And Culture Team, Global Information Security Team, Global Digital IT Team, Global Marketing Team, Facilities Team, Executive Leadership Team, Global People and Culture Team, Global Sales Team.

**Group Function Director:** The person that is the Director or Head of each Group Function.

	Document Title  <i>Data Protection Policy</i>	Document No. <i>Click to enter Doc No.</i>	Version <b>2.6</b>
		Last Revision Date Apr. 25, 24	Page 29 of 30

**Group Guidelines:** Documents which provide drivers and recommended processes or standards to facilitate alignment of operations across Studios, Service Lines, and Functional areas.

**Group Operating Standards:** A document which establishes a common set of processes, standards, and workflows.

**Joint Data Controller:** Refers to a situation in which two or more entities jointly determine the purposes and means of Processing Personal Data.

**Lawful Basis for Processing:** A specific and defined legal justification required to Process Personal Data under GDPR.

**Legitimate Interest Impact Assessment:** A documented balancing test, which assesses whether an organisation's need to Process Personal Data outweighs the risks to, and rights of, individuals whose Personal Data will be Processed.

**Member State Laws:** The body of laws and regulations enacted by the individual countries that are members of the EU.

**Personal Data:** Any information relating to an identified or identifiable natural person; an identifiable natural person is one 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. Note that publicly available data can still be Personal Data.

**Personal 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.

**Privacy Notice:** A document included which details how an individual's Personal Data will be Processed by a particular entity.

**Processing or Processed** (in reference to Personal Data): Any operation or set of operations performed on Personal Data or sets of Personal Data. This in actions such as collecting, recording, organizing, structuring, adapting, retrieving, storing, consulting, using, disclosing by transmission, disseminating, aligning, combining, restricting, erasing, or destroying Personal Data. Essentially, Processing encompasses any conceivable use of Personal Data.

**Records of Processing Activities:** A documented record of Personal Data Processing containing all information required by [Article 30](#) of GDPR.

**Special Categories of Personal Data:** Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the Processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

**Third Country:** Any country or territory outside of the EU and the European Economic Area ("EEA") that the EU has not evaluated as providing an adequate level of data protection.

**Transfer Impact Assessment:** A documented review process used to ensure that Personal Data transferred from the EU to another country is protected adequately. This assessment evaluates the risks and safeguards involved in the Personal Data transfer.

**Transfers of Personal Data to Third Countries:** A transmission of personal data to Third Country or access of personal from a Third Country.

 <b>Keywords Studios</b> Imagine More	Document Title	Document No. <i>Click to enter Doc No.</i>	Version <b>2.6</b>
	<i>Data Protection Policy</i>	Last Revision Date Apr. 25, 24	Page 30 of 30

Document History

Date	Version	Description	Author
2020.12	1.1	Design updated/links added	Ekaterina Ustina
2024.02	2.0	Fully rewritten to create a comprehensive policy covering global regulation. Template design update.	Dominga Leone
2024.04	2.1	Review and comments	Nicolas Liorzou
2024.04	2.2	Updates from Privacy / Legal teams.	Dominga Leone, Oguz Kartoz, James McCarthy
2024.04	2.3	Formatting + proofreading	Nicolas Liorzou
2024.04	2.4	Updates follow DEIB review	Dominga Leone
2024.04	2.5	Legal review	Sabrina Tavormina
2024.05	2.6	Release Candidate	Nicolas Liorzou