GRAVITY MEDIA PRIVACY STANDARD

GRAVITY MEDIA GROUP LIMITED, TRADING AS GRAVITY MEDIA

PRIVACY STANDARD

CONTENTS

1. INTRODUCTION

This Privacy Standard sets out how Gravity Media Group Limited, trading as Gravity Media ("**we**", "**our**", "**us**", "**Gravity Media**") handle the Personal Data of our employees, workers and other third parties such as contractors. This policy applies across all companies within the Gravity Media Group.

This Privacy Standard applies to all Personal Data we Process, regardless of the media on which that data is stored or whether it relates to past or present employees, workers, contractors, and shareholders.

This Privacy Standard applies to all Gravity Media Personnel ("**you**", "**your**"). You must read, understand, and comply with this Privacy Standard when Processing Personal Data on our behalf and attend training on its requirements. This Privacy Standard sets out what we expect from you in order for Gravity Media to comply with applicable law. Your compliance with this Privacy Standard is mandatory. Related Policies and Privacy Guidelines are available to help you interpret and act in accordance with this Privacy Standard. You must also comply with all such Related Policies and Guidelines, which consist of the following: Retention Guidelines (Schedule 2), Retention Schedule (Schedule 3) and the Information Security Policy. Any breach of this Privacy Standard is a disciplinary matter.

This Privacy Standard (together with Related Policies and Privacy Guidelines listed above) is an internal document and cannot be shared with third parties, clients, or regulators without prior authorisation from the Data Protection Officer.

The capitalised terms throughout this policy are as defined in the following clause 2.

2. DEFINITIONS:

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The UK GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

Company Personnel: all employees, workers, contractors, agency workers, consultants, directors, freelancers, members, and others.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Data Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the UK GDPR. We are the Data Controller of all Personal Data relating to our Gravity Media Personnel and Personal Data used in our business for our own commercial purposes.

Data Protection Officer (DPO): the person responsible for overseeing data protection strategy and implementation to ensure compliance with data protection regulations such as the UK General Data

Protection Regulation (UK GDPR) and the EU GDPR. Gravity Media's DPO can be contacted at *grp-uk-data_protection@gravitymedia.com*.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.

EEA: the 27 countries in the EU, and Iceland, Liechtenstein, and Norway.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

EU General Data Protection Regulation (EU GDPR): the General Data Protection Regulation ((EU) 2016/679). Personal Data is subject to the legal safeguards specified in the EU GDPR.

UK General Data Protection Regulation (UK GDPR): means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location, or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity, or availability of Personal Data or the physical, technical, administrative, or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure, or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the UK GDPR.

Privacy Guidelines: The Company privacy/UK GDPR related guidelines provided to assist in interpreting and implementing this Privacy Standard and Related Policies, available in this document.

Privacy Notices: separate notices setting out information that may be provided to Data Subjects when Gravity Media collects information about them.

Processing: any activity that involves the use of Personal Data. It includes obtaining, recording, or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing, or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

3. SCOPE

We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. Gravity Media is exposed to potential fines of up to EUR20 million (approximately £18 million) or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the UK GDPR.

All directors, managers, and heads of business units are responsible for ensuring all Gravity Media Personnel comply with this Privacy Standard and need to implement appropriate practices, processes, controls and training to ensure such compliance.

The Data Protection Officer (DPO) is the person required to be appointed under the UK GDPR. They are responsible for overseeing this Privacy Standard and, as applicable, developing Related Policies and Privacy Guidelines. Contactable on *grp-uk-data_protection@gravitymedia.com*.

Please contact the DPO with any questions about the operation of this Privacy Standard or the UK GDPR or if you have any concerns that this Privacy Standard is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances:

- if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by the Company)
- if you need to rely on Consent and/or need to capture Explicit Consent
- if you need to draft Privacy Notices
- if you are unsure about the retention period for the Personal Data being Processed
- if you are unsure about what security or other measures you need to implement to protect Personal Data
- if there has been a Personal Data Breach
- if you are unsure on what basis to transfer Personal Data outside the EEA
- if you need any assistance dealing with any rights invoked by a Data Subject
- whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA
- If you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making
- If you need help complying with applicable law when carrying out direct marketing activities
- if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors).

4. PERSONAL DATA PROTECTION PRINCIPLES

We adhere to the principles relating to Processing of Personal Data set out in the UK GDPR which require Personal Data to be:

- Processed lawfully, fairly and in a transparent manner **(Lawfulness, Fairness and Transparency).**
- Collected only for specified, explicit and legitimate purposes **(Purpose Limitation).**

- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed **(Data Minimisation).**
- Accurate and where necessary kept up to date **(Accuracy).**
- Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed **(Storage Limitation).**
- Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage **(Security, Integrity and Confidentiality).**
- Not transferred to another country without appropriate safeguards being in place **(Transfer Limitation).**
- Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data **(Data Subject's Rights and Requests).**
- We are responsible for and must be able to demonstrate compliance with the data protection principles listed above **(Accountability).**

(a) Lawfulness, Fairness, and Transparency

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

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

The UK GDPR allows Processing for specific purposes, some of which are set out below:

- the Data Subject has given their Consent;
- the Processing is necessary for the performance of a contract with the Data Subject;
- to meet our legal compliance obligations;
- to protect the Data Subject's vital interests; or,
- to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices.

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

Transparency (Notifying Data Subjects)

The UK GDPR requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them. A template Privacy Notice is at Schedule 1.

Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we must provide the Data Subject with all the information required by the UK GDPR including the identity of the Data Controller and DPO, how and why we will use, Process, disclose, protect and retain that Personal Data through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data.

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

(b) Purpose Limitation

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

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

(c) Data Minimisation

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

You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties.

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

You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Data Retention Guidelines and Retention Schedule at Schedules 2 and 3.

(d) Accuracy

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

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

(e) Storage Limitation

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

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

Gravity Media will maintain the Data Retention Guidelines and Retention Schedule at Schedules 2 and 3 to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time.

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

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

(f) Security Integrity and Confidentiality

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

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

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

You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

- Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it.
- Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.
- Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

You must comply with all applicable aspects of our Information Security Policy.

Reporting a Personal Data Breach

The UK GDPR requires Data Controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject.

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

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact:

- The DPO at *grp-uk-data_protection@gravitymedia.com*
- The information technology department; and
- The legal department.

You should preserve all evidence relating to the potential Personal Data Breach.

(g) Transfer Limitation

The UK GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

The limitation on transferring Personal Data outside the EEA is covered in Schedule 1.

You may only transfer Personal Data outside the EEA if one of the following conditions applies:

- the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms;
- appropriate safeguards are in place such as binding corporate rules (BCR), an International Data Transfer Agreement (IDTA), or the international data transfer addendum to the European Commission's standard contractual clauses for international data transfers, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;
- the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or
- the transfer is necessary for one of the other reasons set out in the UK GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

For further guidance on cross border data transfers, please refer to Schedule 1.

(h) Data Subject's Rights and Requests

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

- withdraw Consent to Processing at any time;
- receive certain information about the Data Controller's Processing activities;
- request access to their Personal Data that we hold;
- prevent our use of their Personal Data for direct marketing purposes;

- ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;
- restrict Processing in specific circumstances;
- challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;
- request a copy of an agreement under which Personal Data is transferred outside of the EEA;
- object to decisions based solely on Automated Processing, including profiling (ADM);
- prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;
- be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
- make a complaint to the supervisory authority; and
- in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

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

You must immediately forward any Data Subject request you receive to the Data Protection Officer (DPO), who can be contacted at *grp-uk-data_protection@gravitymedia.com*.

(i) Accountability

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

Gravity Media must have adequate resources and controls in place to ensure and to document UK GDPR compliance including:

- appointing a suitably qualified DPO (where necessary) and an executive accountable for data privacy;
- implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;
- integrating data protection into internal documents including this Privacy Standard, Related Policies, Privacy Guidelines, Privacy Notices;
- regularly training Gravity Media Personnel on the UK GDPR, this Privacy Standard, Related Policies and Privacy Guidelines and data protection matters including, for example, Data Subjects' rights, Consent, legal basis, DPIA and Personal Data Breaches. The Company must maintain a record of training attendance by Gravity Media Personnel; and
- regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

5. CONSENT

A Data Controller must only process Personal Data on the basis of one or more of the lawful bases set out in the UK GDPR, which include Consent.

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

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

Unless we can rely on another legal basis of Processing, Explicit Consent is usually required for Processing Sensitive Personal Data, for Automated Decision-Making and for cross border data transfers. Usually, we will be relying on another legal basis (and not require Explicit Consent) to Process most types of Sensitive Data. Where Explicit Consent is required, you must issue a Privacy Notice to the Data Subject to capture Explicit Consent.

You will need to evidence Consent captured and keep records of all Consents so that the Group can demonstrate compliance with Consent requirements.

6. RECORD KEEPING

The UK GDPR requires us to keep full and accurate records of all our data Processing activities. You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents.

7. TRAINING AND AUDIT

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

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

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

8. PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENT (DPIA)

We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

You must assess what Privacy by Design measures can be implemented on all programs/systems/processes that Process Personal Data by taking into account the following:

- the state of the art;
- the cost of implementation;
- the nature, scope, context and purposes of Processing; and
- the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

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

You should conduct a DPIA (and discuss your findings with the DPO) when implementing major system or business change programs involving the Processing of Personal Data including:

- use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
- Automated Processing including profiling and ADM;
- large scale Processing of Sensitive Data; and
- large scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

- a description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate;
- an assessment of the necessity and proportionality of the Processing in relation to its purpose;
- an assessment of the risk to individuals; and
- the risk mitigation measures in place and demonstration of compliance.

9. AUTOMATED PROCESSING (INCLUDING PROFILING) AND AUTOMATED DECISION-MAKING

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

- a Data Subject has Explicitly Consented;
- the Processing is authorised by law; or
- the Processing is necessary for the performance of or entering into a contract.

Sensitive Data can be Processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

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

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

A DPIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

10. DIRECT MARKETING

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

The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information. A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

11. SHARING PERSONAL DATA

Generally, we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

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

You may only share the Personal Data we hold with third parties, such as our service providers if:

- they have a need to know the information for the purposes of providing the contracted services;
- sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;
- the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- the transfer complies with any applicable cross border transfer restrictions; and
- a fully executed written contract that contains UK GDPR approved third party clauses has been obtained.

12. CHANGES TO THIS PRIVACY STANDARD

We reserve the right to change this Privacy Standard at any time without notice to you so please check back regularly to obtain the latest copy of this Privacy Standard. This Privacy Standard does not override any applicable national data privacy laws and regulations in countries where a particular company of Gravity Media operates.

13. COMPLIANCE WITH THIS PRIVACY STANDARD

You must comply with all clauses contained in this Privacy Standard and follow the guidelines contained in supporting documents (the Data Retention Guidelines, the Information Security Policy).

SCHEDULE 1: WHAT DATA CAN BE TRANSFERRED OUTSIDE THE EEA

At the moment, the following countries outside the EEA that Gravity Media do business with are recognised as having adequate privacy protection in place from the UK government are:

- Andorra
- Argentina
- Canada (commercial organisations only)
- Guernsey
- Isle of Man
- Israel
- Jersey
- New Zealand
- Switzerland
- Uruguay
- Faroe Islands
- Japan
- Gibraltar

For these countries, the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms.

For all other countries, in order to transfer personal data outside the EEA, one of the following options must apply:

- appropriate safeguards are in place such as binding corporate rules (BCR), an International Data Transfer Agreement (IDTA), or the international data transfer addendum to the European Commission's standard contractual clauses for international data transfers, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;
- the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or
- the transfer is necessary for one of the other reasons set out in the UK GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

If we intend to transfer employee or client data outside the UK (for example, to our businesses outside the EEA such as Australia, the US, and Qatar until an adequacy decision has been made by the UK), we must provide the following form to obtain consent for this transfer:

NOTE TO PROVIDE WHEN TRANSFERRING INFORMATION OUTSIDE THE UK

We will transfer the personal information we collect about you to the following *[country OR countries]* outside the UK *[LIST]* in order to perform our contract with you. There *[is OR is not]* an adequacy decision by the UK in respect of *[that OR those] [country OR countries].* This means that the *[country OR countries]* to which we transfer your data are *[deemed OR not deemed]* to provide an adequate level of protection for your personal information.

However, to ensure that your personal information does receive an adequate level of protection we have put in place the following appropriate measures to ensure that your personal information is treated by those third parties in a way that is consistent with and which respects the EU and UK laws on data protection: an International Data Transfer Agreement (IDTA), or the international data transfer addendum to the European Commission's standard contractual clauses for international data transfers.

If you require further information about this protective measure, you can request it from the Data Protection Officer, at *grp-uk-data_protection@gravitymedia.com*.

SCHEDULE 2: DATA RETENTION GUIDELINES

INTRODUCTION

Gravity Media must not retain data for longer than necessary and comply with data protection laws enshrined in the UK General Data Protection Regulation (UK GDPR). Data retention has three main principles:

1. Data must only be retained for its intended purpose
2. Data must be kept accurate and up to date
3. Data must be stored securely, whether electronically or on paper.

Records are the multiple data elements which together make up a transaction we have on the system (e.g. supplier details).

PURPOSE

The purpose of this policy is to detail the procedures for the retention and disposal of information to ensure that we carry this out consistently and that we fully document any actions taken. Unless otherwise specified, the data retention guidelines refer to records kept both electronically and on paper.

REVIEW

Gravity Media will periodically review retained records to determine if they should be destroyed or retained for a further period.

WHERE DO WE STORE OUR RECORDS?

Records are stored electronically in shared folders or in certain business applications (e.g. Insphire or CrewPlanner) which are restricted for use by Gravity Media employees only. Access can only be granted to freelance employees or employees within different departments with managerial approval.

Records in paper form are kept in ring binders or folders within the office, which may be accessed during the day on an employee's desktop. These files must be locked in a cupboard or cabinet when leaving the office overnight and should not be left on a desktop.

HOW LONG WE SHOULD KEEP OUR RECORDS

We should keep any records for as long as they are needed to meet the intended purpose of processing, together with applicable legal and regulatory requirements. We have assessed our records to:

- ascertain whether the documents are valuable as evidence of the activities and purpose of Gravity Media;
- determine their requirement to the business; and,
- establish whether there are any legal or regulatory retention requirements for the records, including the Freedom of Information Act 2000, the Data Protection Act 2018 (the UK's implementation of the General Data Protection Regulation (GDPR), and the Limitation Act 1980.

A table has been provided with guidelines on how long records should be retained.

WHAT YOU SHOULD DO WHEN THE RETENTION PERIOD HAS EXPIRED

If you process data on behalf of any of the companies owned by Gravity Media, and as outlined in the Retention Schedule below, the relevant retention period has expired, you need to review the records you hold and identify whether the data links to a specific client, employee or customer. If it does, you can anonymise or destroy the data.

Data can be anonymised as an alternative to erasing the data completely. This can be done by:

(a) Erasing any identifiers (e.g. contact name, address) which link the data to a specific person, or,

(b) Separating personal data from information which is not unique to a data subject (e.g. having the order number separate from the company name and address).

DESTRUCTION OF DATA

Records can be destroyed in the following ways:

Paper records – placed in a shredder

Electronic records – destroyed on the system and permanently deleted from any backup drives.

DATA SHARING

Multiple copies of the same customer, employee or client data is discouraged and any duplicate copies should be destroyed. In the event that data has to be shared, only original records should be retained.

If sharing any personal data outside Gravity Media, ensure that the data is sent securely and that the third party has adequate procedures in place to ensure records are dealt with according to local and national legislation and regulatory guidance.

MONITORING OF DATA RETENTION

Responsibility for monitoring data retention and updating the data retention policy is the responsibility of the Data Protection Officer on *grp-uk-data_protection@gravitymedia.com*, and where appropriate, Gravity Media's Legal Department

This policy will be reviewed annually.

SCHEDULE 3: RETENTION SCHEDULE

Type of Data Record	Department	Retention Period	Manager in Charge of Data Record
FINANCE			
Financial information (e.g. ledger records, financial accounts, invoices and petty cash records)	Accounts and Finance	6 years	Chief Financial Officer
Financial Information (on Accpac/Sage)	Accounts and Finance	6 years	Chief Financial Officer
Expenditure Budgets	Accounts and Finance	6 years (for those submitted to HMRC), 2 years (annual estimates used within company)	Chief Financial Officer
HR			
Employee contracts, Pensions and Retirement information	HR	6 years after the employee has left the organisation or when the pension starts	Chief Human Resources (HR) Officer
Employee salary records	HR	6 years from issue	Chief Human Resources (HR) Officer
Employee training: staff training records	HR	2 years from end of employment	Chief Human Resources (HR) Officer
Employee staff records	HR	6 years after the employee has left the organisation	Chief Human Resources (HR) Officer
Employment recruitment: CVs, JDs, application forms, job offers	HR	Unsuccessful applications – 6 months from job creation date	Chief Human Resources (HR) Officer
Employment: job advertisements	HR	Until superseded	Chief Human Resources (HR) Officer

Legal			
Client contracts (e.g. RFPs and Tenders, service agreements, framework agreements, property owned by Gravity Media)	Legal	6 years after the contract is due to end	Group General Counsel
Litigation with third parties	Legal	Permanent preservation	Group General Counsel
Provision of legal advice	Legal	Permanent preservation	Group General Counsel
Board minutes and agendas	Legal	Whilst active	Group General Counsel
Data Protection: Information rights requests	Legal	6 years from date request satisfied and sent to individual	Group General Counsel/Data Protection Officer
Data Protection: Data incidents and breach management	Legal	6 years from date incident concluded	Group General Counsel/Data Protection Officer
Data Protection: Privacy impact assessments	Legal	6 years from creation date	Group General Counsel/Data Protection Officer
Data Protection: Policies and guidance	Legal	Whilst active	Group General Counsel/Data Protection Officer
Operations			
First Aid/Accident Reports	Office Management/Operations	3 years after the last date of entry	Office Manager
RIDDOR reports	Operations	20 years from creation	Operations Director
Training records	Operations	2 years from end of employment	Operations Director
Risk Assessments	Operations	Whilst active	Operations Director

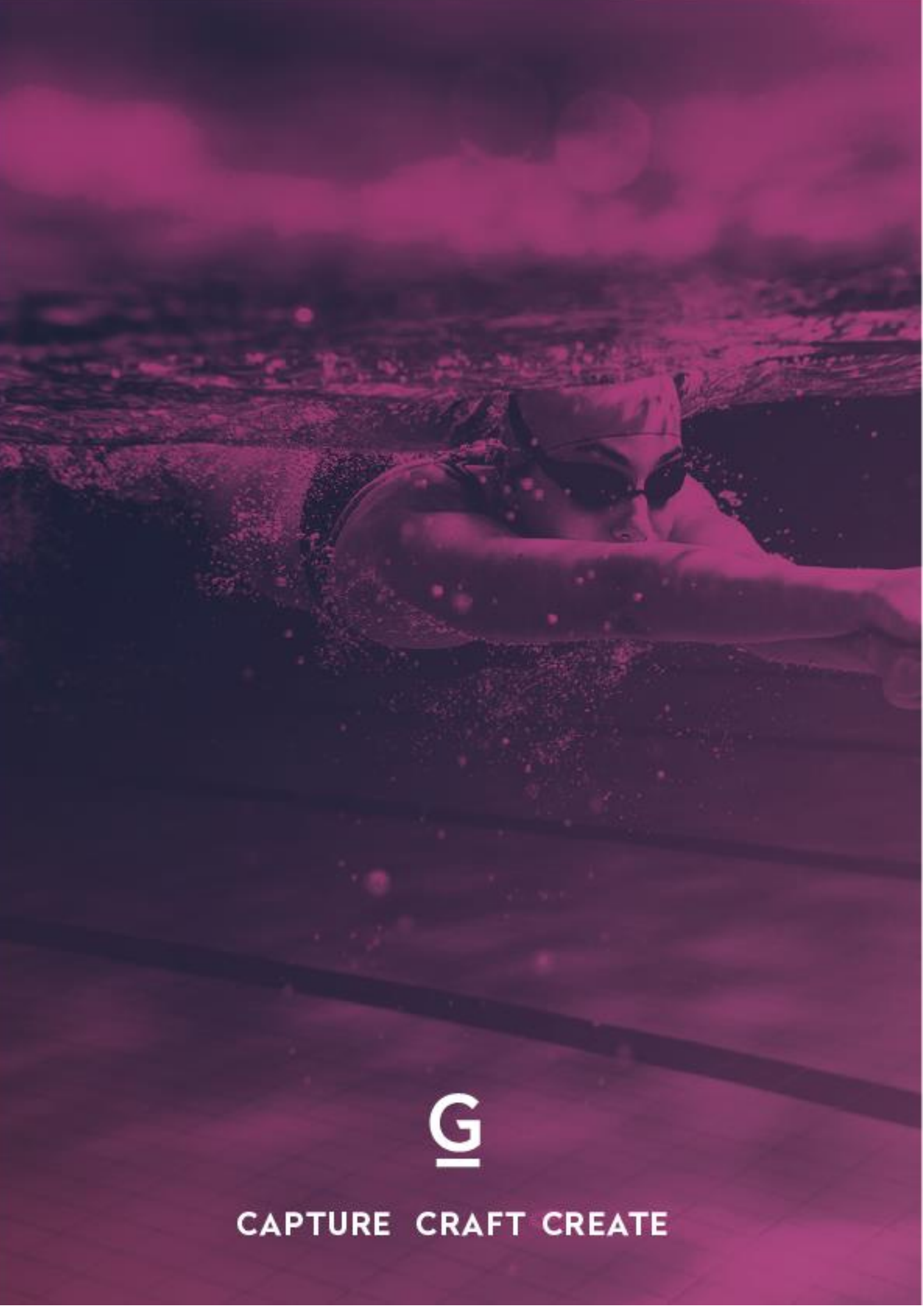
Tax			
Tax records (including income tax records, wages, corporation tax and tax corporate incentives)	Tax/accounts	Up to 3 years after the end of the financial year to which they relate	Tax Director
Projects			
Freelancer contracts	Projects	6 years after contract has ended	Lead Production Manager
Freelancer invoices	Projects	6 years	Lead Production Manager
Staff/Freelancer records: passports, images, new starter forms	Projects	6 years after freelancer has worked for the company	Lead Production Manager
Marketing			
Corporate communications: GMG Live (company news)	Marketing	Business need	Head of Marketing
Corporate communications: staff images	Marketing	30 days from leaving employment	Head of Marketing
General correspondence (via GM website)	Marketing	Business need	Head of Marketing
IT			
Staff email addresses	IT	60 days from leaving date	Head of Corporate IT & Cyber Security

CONTROL SHEET

Document reviewer: Carly Thurgood
Document adopted on: 2018
Next review date: May 2024

REVIEW/CHANGE HISTORY

Date of Review/Change	Summary of changes	Version no.
July 2022	Addition of control sheet, amendments made to reflect UK GDPR, removal of mention of customers and suppliers, amendments made to reflect changes to data transfers outside of EEA, data retention guide amended.	1.1
May 2023	Removal of template privacy notice.	2.0



CAPTURE CRAFT CREATE