All3Media GDPR Compliance Programme

July 2020

All3Media GDPR Compliance Programme

Introduction

The General Data Protection Regulation ("**GDPR**") replaces the current Data Protection Act and comes into force on 25 May 2018 and will apply to all controllers and processors of Personal Data.

This Handbook has been compiled to ensure that all Operating Companies are compliant with GDPR and includes policies and guidance to be adopted and followed across the All3Media Group.

We are yet to be issued with any definitive industry wide guidance regarding GDPR compliance as such, we will need to also take into account any additional instructions and guidance provided by the relevant broadcasters, therefore there may be changes to this handbook in the future as working practices become clear and industry guidelines develop.

Definitions

The definitions below apply throughout this Handbook.

"**All3Media Group**" means DLG Acquisitions Limited and each of its direct and indirect subsidiary undertakings from time to time;

"**Company Information"** means all information relating to the All3Media Group and each Operating Company including all confidential information, information owned or produced by or on behalf of an Operating Company or any of its Staff and/or Freelancers or of which they become aware of during the course of their engagement/employment with the All3Media Group;

"**Data Controller**" means the organisation that (either alone or with others) decides the purpose of processing and the way it will be done;

"**Data Processor**" means the organisation that processes personal data on behalf of the data controller;

"**Data Protection Legislation**" means Data Protection Act 1998, the EU Data Protection Directive 95/46/EC, the General Data Protection Regulations (being EC Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the movement of such data) (when in force), the Privacy and Electronic Communications (EC Directive) Regulations 2003 and all applicable laws and regulations relating to the processing of personal data and privacy, including where applicable, any guidance notes and codes of practice issued by the European Commission and applicable national regulators including the UK Information Commissioner;

"Freelancer" means individuals who are engaged on a temporary or fixed term basis solely to provide services on a production;

"**Handbook**" means this GDPR compliance handbook as amended, updated or supplemented from time to time;

"**Operating Company**" means each operating company within the All3Media Group;

"**Personal Data**" means any information relating to an identified or identifiable natural person (the data subject), including non-sensitive personal data, confidential data and sensitive data;

"**Policies and Procedures Manual**" means the All3Media Group policies and procedures as amended or supplemented from time to time;

"**Processing**" means any operation or set of operations performed on personal data, whether or not by

automated means. Examples include, storing of personal data on a hard drive or server, using personal data to send to communications to recipients, amending or deleting personal data;

"**Sensitive Personal Data**" means any personal data relating to a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade and union membership, genetic data, biometric data, data concerning health and data concerning a person's sex life or sexual orientation and data relating to criminal convictions and offences; and

"**Staff** means all employees of the All3Media Group and all clerical and administrative staff engaged on a fixed term basis other than Freelancers;

Contents

This Handbook contains the following:

1. Data Security Policy
2. Data Management Policy
3. Data Breach Protocol
4. Data Breach Protocol- guidance for notification to the ICO
5. Release forms and filming notice guidance
6. Workplace Privacy Notice
7. Cast, Crew and Talent Privacy Notice
8. Contributor Privacy Notice
9. Recruitment Privacy Notice
10. Prospective Cast, Crew and Talent Privacy Notice
11. Prospective Contributor Privacy Notice
12. Arrangements with Staff and Freelancers
13. Third Party Contracts Guidance
14. Website Privacy Policy
15. Website Terms & Conditions

Checklist

In respect of the documents contained in this Handbook, the checklist below describes, at a high level, the action to be taken in respect of each of them. However, you should in all cases read the relevant policies before taking any action.

Document/policy	Description	Action
Policies		
Data Security Policy	This policy covers the way in which we need to treat personal data to ensure it is secure, including the use of hardware, software, work devices and personal devices.	• To be adopted by all Operating Companies • To be read by all Staff and Freelancers • To be made available on the intranet
Data Management Policy	This policy covers the length of time for which data should be kept, the role of an Information Officer and transfers of personal data both within the All3Media Group and outside.	• To be adopted by all Operating Companies • To be read by all Staff and Freelancers • To be made available on the intranet
Data Breach		

Data Breach Protocol	The data breach protocol explains what to do in the event of a breach or suspected breach	• To be read by each Information Officer who must understand the requirements and ensure that all of those engaged by their Operating Company is aware of what to do and who to speak to in the event of a data breach or a suspected data breach • To be made available on the intranet
Data breach protocol- guidance for notification to ICO	The guidance explains how and why we would notify the Information Commission Office of a breach	For information purposes only – any communication with the ICO will be co-ordinated by All3Media Group
Release Forms & Filming Notices Guidance		
Release Forms & Filming Notice Guidance	The guidance includes wording for release forms and filming notices.	• All release forms to be updated as per the guidance with the relevant privacy notice links • Filming notices to include links to relevant privacy notices
Privacy Notices		
Workplace Privacy Notice	The Workplace Privacy Notice tells individuals in the workplace how and why we use their data	• To be read by all Staff • To be made available on the intranet • To be made available from HR on request
Cast, Crew and Talent Privacy Notice	The Cast, Crew and Talent Privacy Notice tells Freelancers what we will do with their data, why we need the data and how they can find out further information	• To be sent to Freelancers as part of the new starter process. The easiest way is to attach this as an addendum to their contract or as a terms and conditions document • read by all Staff
Contributor Privacy Notice	The Contributor Privacy Notice tells contributors what we will do with their data, why we need their data and how they can find out further information. It's less detailed than the Cast, Crew and Talent Privacy Notice	• To be sent to contributors or made available on request
Recruitment Privacy Notice	Individuals who wish to work for the All3Media Group will send their data when applying for roles (either for a specific role or speculatively). If the individuals ask we should be able to provide them with a privacy notice telling them how and why we use their data.	• To be retained and made available on request by the individual concerned
Prospective Cast, Crew and Talent Privacy Notice	The Prospective Cast, Crew and Talent Privacy Notice tells prospective Freelancers what we will do with their data, why we need the data and how they can find out further information	• To be retained and made available on request by the individual concerned

Prospective Contributor Notice	The Prospective Contributor Notice tells prospective contributors what we will do with their data, why we need the data and how they can find out further information	• To be retained and made available on request by the individual concerned
Arrangements with Staff and Freelancers		
Arrangements with Staff and Freelancers guidance and addendums	Agreements with Staff and Freelancers will need to be updated in line with the guidance	• Follow the guidance in terms of understanding which agreements are to be updated • Send addendums in line with guidance
Template Agreements	Standard form employment agreements for Staff	• To be circulated separately
Arrangements with Third Parties		
Third party contracts guidance	Agreements with third parties (excluding Freelancers) will need to be updated to include GDPR compliant provisions.	• Follow the guidance to understand which third party contracts require updating to comply with GDPR • Send updated provisions in line with the guidance
Website		
Website privacy policy	Websites operated by members of the All3Media Group should include a privacy policy.	• Privacy policy to be uploaded to all websites operated by members of the All3Media Group
Website terms and conditions	Website terms and conditions have been updated	• The template replaces any existing website terms and conditions of use • Updated terms and conditions to be uploaded to websites operated by members of the All3Media Group
Data Transfer Agreement		
Group Transfer Agreement	The group transfer agreement deals with how we transfer data across the All3Media Group.	For information only.

General provisions

The following provisions apply to all policies included in this Handbook.

The provisions contained in this Handbook supersede any equivalents contained in the Policies & Procedures Manual and in the event of conflict between this Handbook and the Policies & Procedures Manual, the provisions of this Handbook shall apply.

Information Officers

Each Operating Company must have an Information Officer who is primarily responsible for their Operating Company's compliance with all applicable Policies. Staff and Freelancers should refer any questions they have regarding this Handbook to their Information Officer in the first instance.

Monitoring compliance

All Staff must read and comply with the policies relevant and applicable to them and included in this Handbook regardless as to which country they work in and/or any local laws that provide for a less stringent level of

protection. You must also comply with any local legislation which requires a more stringent level of protection and your compliance with the policies included in this Handbook will be subject to periodic checks by the All3Media Group.

Consequences of non-compliance

Breaches of Data Protection Legislation can result in fines up to a maximum of €20million or 4% of worldwide turnover of the All3Media Group, whichever is greater and dependent on the circumstances of the breach. Breaches of Data Protection Legislation may also result in significant harm to the reputation of the All3Media Group and any Operating Company involved as well as the individual whose data has been mismanaged.

Any failure by Staff and, where relevant, Freelancers, to comply with the policies and/or guidance contained in this Handbook may result in disciplinary action in line with their employment or engagement agreements and in line with All3Media Group policy.

Changes to the policies and guidance

All3Media reserves the right to make changes to and update or supplement the provisions of any policy and/or guidance contained in this Handbook.

Questions

You should contact your Operating Company's Information Officer in the first instance should you have any questions. If they are not able to help then please contact compliance@all3media.com.

Data Security Policy

1. Purpose and scope

The purpose of this policy is to ensure that all data held by the All3Media Group is dealt with securely no matter what form such data is held in, whether it is in hard copy or digital format and type or form of device it is held on. This policy applies to all Operating Companies and all Staff and Freelancers.

2. Company devices

Where you have been provided with a work device by your Operating Company, you must use this device for your work (and not an equivalent personal device) and comply with this policy.

When using a company device to process and store Personal Data or Company Information, you should only access and use the Company Information that you are authorised to and you must not:

1. copy such Personal Data or Company Information to any personal accounts, including cloud services. All files should be saved in the location as directed by your line manager;
2. make any changes to any IT system, information and/or equipment not authorised by your line manager and/or your IT support team;
3. store (large) personal files on company devices and systems. Your Operating Company reserves the right to delete any or all such files without notice;
4. remove or disable any software that has been installed by your IT support team;
5. install or use non-authorised software except commercially available software such as music or video streaming apps provided in each case that you pay all applicable fees and comply with the terms and conditions of such apps. You must never download or store any software intended for piracy or other illegal practices.

All company devices (including laptops, mobile phones, portable storage devices) must be returned at the end of your engagement with your Operating Company.

3. Personal devices

Where you have not been provided with a company device, you may use an equivalent personal device for your work provided that your use of such device has been authorised by your Operating Company and you comply with this policy including in respect of passwords and passcodes.

When using a personal laptop/computer, you must ensure that the laptop/computer has up to date anti-virus and anti-malware software installed, it is encrypted (where technologically possible), has appropriately licensed software and the most recent operating system patches installed. When using a personal laptop to store Company Information and/or Personal Data, you must not copy such data to any personal accounts (including cloud services).

If you are required to save any Company Information (such as production budgets) to your personal laptop for the purposes of your engagement with your Operating Company, you must delete that information immediately following the end of your engagement.

When using a personal mobile or tablet device to access Company Information, you must not download that information to your personal device and you may never copy such information to any personal account.

4. Passcodes and passwords

All devices (whether work or personal) must be passcode or password protected. Passwords and passcodes satisfying the criteria below will not need to be changed unless they have been compromised or where your IT support team has requested that they be changed.

You should never share a passcode or password with any other person. If you share your password or passcode or if you suspect that it has been compromised, you must immediately: (i) change the password and/or passcode that has been comprised; and (ii) inform your IT support team and follow any instructions they give to you.

Passwords

You must either set or, where you have been provided a device with a pre-existing password, change your password so that it strings together three unrelated words or four letters or more with each word separated with a symbol. An example password is: table&hull%peaches

Passwords meeting the criteria above will not need to be changed unless the password has been compromised.

Passcodes

Mobile devices must be protected using a minimum six non-consecutive digit code and/or letters. You may also use biometrics to protect your phone, such as finger prints.

5. Locking of devices

All devices (whether company devices or personal devices) must be locked when not in use or if left unattended. All devices must auto-lock after five minutes of inactivity.

6. Transportation and storage of devices and company information

All devices must be transported safely and stored securely when not in use. Company Information should only be sent using special delivery, a reputable courier or an equivalent tracked mail service. Where confidential information is particularly sensitive, you should only use a reputable courier.

7. Personal emails

The security measures in a corporate email account (being an email account provided to you by your operating company in the *name.surname@operatingcompany.com* (or co.uk or .tv or similar format) are far more rigorous than a personal email account. For these reasons the use of personal email accounts for operating company duties is strictly limited.

Staff - all Staff must use their work email addresses when carrying out their duties on behalf of their Operating Company and must not use personal email addresses for work purposes for any reason.

Freelancers- the following Freelancers must be given corporate/work email addresses by their Operating Company. These email addresses must be used during their engagement for the purposes of the work they undertake on behalf of that Operating Company:

(i) Producer, Line Producer, Production Manager, Production Co-ordinator and Production Accountant and Production Secretary; and

(ii) anyone else who the Operating Company deems it necessary to have a corporate email address as they will have access to and be required to send significant amounts of Personal Data.

All other Freelancers may use their personal email addresses for the purposes of their engagement where they are not provided with corporate email addresses, however care must be taken when dealing with personal data. Any documents should be password protected with the password sent separately and the recipient of any email should be double checked before sending.

8. Cloud based storage systems

Use of cloud based storage systems (such as dropbox) is only permitted through a business/corporate account (and not a personal account in the name of your Operating Company). If you require the use of a corporate account/service, please contact your IT support team to discuss requirements.

9. VPNs (virtual private networks)

Access to your Operating Company's network may be provided to you through a VPN using devices provided by your Operating Company. Personal devices are not permitted to access any Operating Company's network through a VPN.

10. Mobile apps

Mobile communication apps, such as WhatsApp and Viber, may be used for making calls. Such apps may also be used for sending messages however they should never be used to send Confidential Information or Personal Data.

Your Operating Company may make mobile apps available to you. Where instructed by your Operating Company, you must use the mobile app made available to you in accordance with any instructions from your Operating Company. You must also comply with all instructions given by your Operating Company in respect of the deletion of any mobile app or other software provided or made available to you during the course of your engagement.

11. Portable storage devices

Portable storage devices, such as USB sticks, SD cards, may be used to store Company information and must be encrypted, where technologically possible, if used to store and/or transport Personal Data or any sensitive or confidential company information.

Only devices provided by your Operating Company may be used to store and/or transport Personal Data. You must ensure that any devices are stored securely when not in used and that all data is deleted from that device as soon as practicable.

12. Third party software or services

Where third party software or service, such as Set Keeper or Yamdu, is used by your Operating Company, an appropriate person within your Operating Company must be responsible for ensuring that such software meets the requirements of the purpose for which it is used, including ensuring that any data uploaded to such software/service is secure and available only to those working on the relevant production as and when required. You should inform your IT support team before acquiring or using such software/service to ensure that appropriate technological measures are in place.

13. Downloading and storage of company information

From time to time, you may need to download company information to a personal device. Where this is the case the device must be password protected, encrypted and have up to date anti-virus software installed and active, such information must only be used for legitimate business purposes and must be deleted as soon as it is no longer required for that business purpose.

14. Compromise of passwords, passcodes, devices, loss of devices and viruses

You must immediately inform your IT support team if you suspect or become aware of:

1 any loss of company information;
2 any loss of any devices (whether company devices or personal devices) storing company information;
3 any personal device holding company information or any company device is infected with a virus;
4 any of your passwords or passcodes being compromised;
5 any unauthorised access to confidential information,

and comply with both the Data Breach Protocol and any instructions given to you by your IT support team.

Policy version:	v.1
Last Updated:	March 2018

Data Management Policy

1. Purpose and scope

The purpose of this policy is to ensure that all data collected, processed and stored by any member of the All3Media Group and all of its Staff is done so in accordance with all applicable legal requirements and business needs.

This policy sets out how data sets out how all data is to be collected, processed and retained and applies to all Operating Companies and all Staff and Freelancers.

2. Data Protection Principles

When processing personal data, each Operating Company and all Staff must comply with the following data protection principles:

(i) the processing of Personal Data must be done fairly, transparently and lawfully;

(ii) Personal Data may only be processed for specific and lawful purposes;

(iii) the Personal Data collected and processed must be accurate and kept for no longer than is necessary and in accordance with section 8 of this policy; and

(iv) in processing Personal Data, any rights of individuals in respect of their data must be upheld.

All data held by an Operating Company must be kept securely and safely.

3. Responsibilities

Each Operating Company must:

(i) ensure that all of its Staff have read and understood this policy and the Data Security Policy;

(ii) ensure that their Information Officer and/or head of legal and business affairs and any other representatives attend data management training sessions offered by All3Media;

(iii) ensure that the Privacy Notices (in the form set out in the GDPR Handbook are displayed prominently around their offices/on the Operating Company intranet);

(iv) notify data security breaches in accordance with the Data Breach Protocol;

(v) ensure that, for each new project (including productions and developments and any new systems or processes):

(a) a kick-off meeting is organised at which the relevant project manager(s) and/or, where relevant, legal and business affairs team(s) specifically address data management during the project and development process including, but not limited to, what Personal Data is to be collected, how it is collected and who should have access to it; and

(b) a process is established for data storage for each project.

4. Information officers

Each Operating Company must have an Information Officer who is primarily responsible for their Operating Company's compliance with all applicable policies. Questions on this policy should be referred to the relevant Information Officer in the first instance.

5. Data security

Data must be stored securely and in accordance with the Data Security Policy.

6. Collection of Personal Data

Data may only be collected, processed and retained for the purposes for which it was created or obtained and not for any other purpose.

7. Transferring Personal Data

Transfers between Operating Companies

Operating Companies may transfer Personal Data to other entities within the All3Media Group where such transfer is based on a business requirement, for example requests from All3Media HQ. Transfers of data between members of the All3Media Group are governed by the terms of the All3Media intra-group transfer agreement.

Transfers to third parties inside the EEA

It may from time to time be necessary to transfer Personal Data to third parties contracted by or on behalf of an Operating Company, for example for the processing of payroll. Where such a transfer is necessary, Operating Companies must ensure that they have written agreements in place ensuring that the third party complies will all applicable Data Protection Legislation including having contractual provisions that as a minimum reflect those in Third Party Contracts Guidance.

Transfers to third parties outside of the EEA

Personal Data must never be transferred to third parties outside of the EEA without the prior written consent of the data subject. Where Personal Data is to be transferred outside of the EEA, this should be subject to an agreement containing the relevant model clauses relating to data transfers outside of the EEA. Links to the model clauses are included in the Third Party Contracts Guidance.

8. Information retention

The final signed and dated versions of new agreements entered into should be scanned and saved electronically.

Data should only be kept for so long as is necessary to keep it and where such retention can be justified (either as a result of an applicable legal obligation or genuine business requirement) and, in any event, should not be kept longer than the maximum retention period as set out in the table below. Notwithstanding the table below, documents may be destroyed at an earlier date where they are no longer required.

The table below applies to both paper copy and digital documents.

Non-Production Information	Retention period
HR information relating to current and former employees (including contracts, payslips, disciplinary files, leave records, freelancer agreements)	7 years post engagement
HR information relating to prospective employees	12 months from decision not to proceed with application
Company information (including articles, board minutes, certificates of incorporation, statutory registers)	Life of company plus 2 years
Third party contracts/agreements (including fixer agreements, supplier agreements, location agreements)	7 years after expiry
Finance and tax related documents	7 years
Property – deeds of title	Permanent or until delivered to purchaser

Other property related documents (including leases, agreements with architects/builders)	12 years after expiry of lease and any terminal queries have been settled (e.g. dilapidations)
Insurance – Public & Employers Liability, E&O	Indefinitely
Insurance certificates and policies (all others)	7 years after expiry
Health and safety records	7 years post engagement
Other documents not being production information and not otherwise covered by this section 8	7 years

Production Information (not covered by the above)	**Retention period**
Agreements under which there may be residual payments due or under which intellectual property rights are held (for example, broadcaster/commissioning agreements, production, distribution and financing agreements, writer and cast agreements, clearances)	Indefinitely
Production budgets	7 years after delivery of the programme
Contributor forms and releases	Life of operating company plus 2 years
Health information (other than statement of health forms)	7 years post engagement
Statement of health forms	As soon as no longer required
Records of contributors, cast or crew not engaged in a production should be destroyed once the show has delivered unless consent has been given to your retaining that information for the stated purposes.	

9. Disposal of information

Operating Companies should not keep information for any longer period than is necessary and should securely dispose of or destroy any such information as soon as possible after the end of the relevant period set out in section 8 or, if earlier, as soon as it is no longer required for a legitimate business need.

Operating Companies should check their records annually to ensure that they are not keep information and data for longer than permitted and dispose of or destroy any information that has reached the end of its retention period.

Policy version:	v.2
Last Updated:	July 2020

Data Breach Protocol

1. Purpose and Scope

The purpose of this protocol is to ensure that all members of the All3Media Group and all Staff and Freelancers understand their responsibilities in the event of a suspected or actual data breach and ensure that any actual or potential breach is notified to the relevant persons in accordance with this protocol.

2. What is a data breach?

A data breach arises if there is:

(a) accidental or unlawful destruction, loss or alteration of data; or

(b) unauthorised disclosure of or access to data.

Examples of when data breaches (including breaches of personal data) may arise include:

(a) loss or theft of equipment such as laptops, mobile phones and memory sticks or of the data (including rushes) stored on the equipment and documents;

(b) loss of company documents or other commercially sensitive information;

(c) loss of paper files such as call sheets, contributor forms , talent details;

(d) inappropriate access to our systems controls allowing unauthorised use of personal data;

(e) human error – for example sending an email containing personal data to the wrong recipient;

(f) hacking attacks; and

(g) phishing attacks where information is obtained by deception.

3. Should you report the breach?

If you become aware of a potential or actual data breach, you must immediately (and, in any event, in less than 24 hours) notify, your Operating Company's Head of Legal & Business Affairs (or if your operating company doesn't have one, your Head of Production) and your Information Officer.

Your Information Officer is responsible for notifying the All3Media Group General Counsel (with a copy to compliance@all3media.com) and must provide a completed copy of the Data Breach Notification Form (attached at the appendix to this protocol) at the same time. All notifications to All3Media HQ must take place within 24 hours of you becoming aware of an actual or potential data breach.

4. Managing our response to a data breach

The Operating Company Information Officer together with All3Media HQ will be responsible for managing any response to a data breach. Once a breach has been notified in accordance with section 3 above, the Operating Company Information Officer should follow any guidance or instructions given by All3Media HQ.

Each Operating Company must keep a record of each actual or potential data breach, its effect and any remedial action taken to address the breach. All3Media may request copies of these records from time to time.

5. Notifying affected individuals

Any individual whose data is the subject of the actual or potential data breach must be notified of the actual or potential breach without delay unless:

(a) the individual's data was encrypted or other measures had been taken to make it unintelligible to an unauthorised person; or

(b) the relevant Operating Company has been able to take measures after becoming aware of the data breach which means that there is no longer a high risk to the privacy or other rights and freedoms of any individual affected.

It is the responsibility of the Information Officer to notify any affected individuals of a data breach (if required). When notifying the affected Individual, the Operating Company/Information Officer must provide:

(a) explain the breach;

(b) provide contact details of a person within the Operating Company with whom the affected individual can raise any concerns;

(c) an explanation of the likely consequences of the data breach;

(d) details of the measures that taken or proposed to be taken to address the data breach including any damage limitation measures.

6. Notifying the regulator

If it is determined that the regulator must be notified of a data breach, then All3Media HQ will be responsible for notifying the Regulator and for managing any response to queries raised by the Regulator. If a notification is required, then the regulator must be notified within 72 hours of when we first become aware of the breach.

All data breaches must be notified to the regulator unless

(a) the breach is unlikely to result in a risk to individual's personal data, rights or freedoms; and

(b) it can be demonstrated that there is no likely risk.

7. Monitoring compliance

All Staff and Freelancers must comply with all applicable policies regardless of which country they work in and/or any local laws that provide for a less stringent level of protection. You must also comply with any local legislation which requires a more stringent level of protection. Your compliance with this protocol will be subject to periodic checks by the All3Media Group including the provision of records relating to the managing of our Operating Company's response to any actual or potential breach.

8. Consequences of non-compliance

Breaches of data protection legislation can result in fines up to a maximum of the greater of €20million or 4% of worldwide turnover of the All3Media Group depending on the circumstances of the breach as well as significant harm to the reputation of All3Media and any Operating Company involved as well as the individual whose data has been mismanaged.

Any failure by Staff and/or Freelancers to comply with this protocol may result in disciplinary action in line with their employment or engagement agreements and All3Media Group policy.

9. Questions

Staff and Freelancers should contact their Operating Company's Information Officer in the first instance. If they are not able to help then please contact compliance@all3media.com.

Appendix I
Data Breach Notification form

Company Name:	
Author of the Form:	
Date of the actual incident:	
Date indecent discovered:	
Who reported the incident:	
Physical location of incident:	
Office(s) involved:	
Production(s) Involved:	
Broadcaster involved:	
Internal individual(s) involved (and role):	
External individual(s) involved (and role):	
Who, if anybody, has been notified:	
Description of incident (including the nature of the data the subject of the breach):	
Actions taken or proposed to be taken:	
Measures implemented or proposed to be implemented to prevent further incidents occurring in the future	
Other relevant information	

Data Breach Protocol – Guidance for Notification to the Information Commissioners' Office

1. Purpose and Scope

The purpose of this protocol is to provide guidance to All3Media HQ as to when an actual or potential data breach will be notifiable to the ICO and what information must be provided to the ICO in the event of notification.

2. Data breach risk assessment

In determining whether a breach should be notified, an assessment must be made of what has happened and the related risks including consideration of the type of data involved, circumstances surrounding the breach and reputational harm and whether external legal advice should be sought.

Records of the risk assessment should be maintained.

3. Notifying the regulator

The regulator must be notified of a data breach unless:

(c) the breach is unlikely to result in a risk to individual's personal data, rights or freedoms; and

(d) it can be demonstrated that there is no likely risk to the individual's personal data, rights or freedoms.

The regulator must be notified with 72 hours of the relevant Staff/Freelancer/Operating Company first becoming aware of a breach: Any notification must include:

(e) an explanation of the nature of the breach, including, if possible:

(f) the categories of data subjects and approximate numbers;

(g) the categories of personal data records and approximate numbers.

(h) details of the contact person at All3Media HQ;

(i) details of the likely consequences of the data breach;

(j) measures taken or proposed to be taken to address the data breach including any damage limitation measures.

It may not be possible to provide all of the information listed above within 72 hours. Where this is the case, the information available at the time of notification should be provided with the remaining and any further information to follow as soon as it is available.

All notifications to the regulator will be made by the All3Media Group General Counsel, Jamie McIntyre-Brown, with the prior consent of the All3Media Group Chief Operating Officer.

Complete records must be kept of any data breach and the response to it.

4. Records

Complete records of any data breach risk assessment, actions taken, notifications and responses will be maintained by All3Media HQ.

Release forms and filming notices guidance

1. Purpose and scope

The purpose of this guidance is to provide details around the updates to be made by Operating Companies to release forms.

2. Release forms- general

All release forms must contain a description of the relevant programme in sufficient detail so as to enable a contributor to understand the nature of the programme as well as the usual information regarding assignment of rights and waiver of moral rights. The release form should separate:

(i) the release to appear in the programme; and
(ii) data protection.

Generally, including from a GDPR compliance perspective, release forms do not need to include consent from the individual contributor to the processing of their data unless data collected includes health or other sensitive personal data. Instead, for non-special category programmes, the release form should contain the following wording:

"***By necessity we will process your personal data, including your image and voice, as part of producing the programme. We will do so in accordance with all relevant data protection law and you can find out more information about how we process your personal data [[here [insert link to contributor privacy notice]] OR [in the Contributor Privacy Notice attached to this form]] OR [please contact [•] for a copy of our Contributor Privacy Notice]***"

Where health or other special categories of data are being collected from an individual contributor, including checks made or health data requested or collected in relation to a health emergency (including Covid-19), explicit consent will be required for the processing of that contributor's Personal Data. Where this is the case, the procedure set out in paragraph 3. (Special category programmes) below should be followed and the additional explicit consent wording used.

The Contributor Privacy Notice can be made available in hardcopy (i.e. by appending it to the release form), by including a link in the release form to the Contributor Privacy Notice or by providing the contact details of an individual at your operating company from whom the contributor may obtain a copy of the privacy notice.

It is not necessary for a contributor to sign a document confirming they have read and understood the Contributor Privacy Notice however Operating Companies may elect to ask their contributors to do so should they choose.

3. Special category programmes

For special category programmes, being those programmes involving children or those focussing on health/medical issues (both physical and psychological), explicit consent will be required for the processing of that contributor's Personal Data. In addition, where health or other sensitive personal data is being collected or processed explicit consent will also be required form the contributor as set out in this paragraph 3..

In addition to including the wording detailed in section 2 above, release forms for special category programme should also include the following wording:

"***I explicitly consent to the processing of my personal data for the purposes of producing (including broadcasting) of [name of programme] as described in paragraph [•] of this form and I understand that such data will be processed in accordance with the privacy notice [found at [•]] OR [appended to this notice]***"

As consent needs to be informed consent, release forms relating to special category programmes must either include a link to where the privacy notice may be found or, ideally, append the privacy notice to the release form. Operating Companies should also explain to the contributor what the release form covers and what types

of that contributor's Personal Data will be processed prior the contributor signing the release form. This will assist in ensuring that the consent given is informed consent.

When dealing with those under the age of 18, you should seek guidance from the relevant broadcaster as to who needs to signs the relevant forms. We suggest that the fall-back position be that for those under the age of 16, a parent or guardian sign the relevant forms, for those between the ages of 16 and 18, the forms are co-signed by a parent or guardian and the relevant individual and those over the age of 18 sign themselves unless you are aware of a reason by the forms should be signed by another person.

4. Filming notices

When filming in public areas with heavy footfall, filming notices used by Operating Companies should include:

(i) a description of the programme which contains sufficient detail so as to enable individuals to understand the nature of the programme;

(ii) information as to why the crew is there, what they are filming and for which broadcaster; and

(iii) a statement that limited personal data may be processed as part of the filming and either a web link to where the Contributor Privacy Notice may be found or contact details of where it can be made available.

Workplace privacy notice

1. Purpose and Scope

Like most businesses, we hold and process a wide range of information, some of which relates to individuals who work for us. This Privacy Notice explains the type of information we process, why we are processing it and how that processing may affect you and focusses on employees as well as former employees.

This Privacy Notice is set out in this document (the Core Notice) and the Supplementary Information in the annex to this document on our intranet. In the Supplementary Information, we explain what we mean by "personal data", "processing", "sensitive personal data" and other terms used in the notice.

2. Personal data- what we hold and why we process it

We process data for the purposes of our business including management, administrative, employment and legal purposes. The Supplementary Information provides more specific information on these purposes, on the type of data that may be processed and on the grounds on which we process data. See *Processing gateways – the legal basis for processing* and *Further information on the data we process and our purposes.*

3. Where the data comes from and who gets to see it?

Some of the personal data that we process about you comes from you. For example, you tell us your contact and banking details. Other personal data about you is generated in the course of your work, for example, from your managers, colleagues and customers or others outside our organisation with whom you deal.

Your personal data will be seen internally by managers, HR and, in some circumstances, colleagues. We may also pass your data outside the organisation, for example to payroll agencies. Further information on this is provided in the Supplementary Information. See *Where the data comes from* and *Who gets to see your data?*

4. How long do we keep your personal data?

We do not keep your personal data for any specific period but will not keep it for longer than is necessary for our purposes. In general, we will keep your personal data for the duration of your employment and for a period afterwards. See *Retaining your personal data – more information* in the Supplementary Information.

5. Transfers of personal data outside the EEA

We may transfer your personal data outside the EEA to other members of the All3Media Group.

Further information on these transfers and the measures taken to safeguard your data are set out in the Supplementary Information under *Transfers of personal data outside the EEA – more information.*

6. Your data rights

You have a right to make a subject access request to receive information about the data that we process about you. Further information on this and on other rights is in the Supplementary Information under *Access to your personal data and other rights.* We also explain how to make a complaint about our processing of your data.

7. Contact details

In processing your personal data, we act as a data controller. Our contact details are as follows: [*Name and contact details*][1].

[1] Each Operating Company to insert name of appropriate contact within their business.

8. Status of this policy

This notice does not form part of your contract of employment and does not create contractual rights or obligations. It may be amended by us at any time.

Workplace privacy notice- supplementary information

1. What is Personal Data and Processing

"**Personal data**" is information relating to you (or from which you may be identified) which is processed by automatic means or which is (or is intended to be) part of a structured manual filing system. It includes not only facts about you, but also intentions and opinions about you.

Data "**processed automatically**" includes information held on, or relating to use of, a computer, laptop, mobile phone or similar device. It covers data derived from equipment such as access passes within a building, data on use of vehicles and sound and image data such as CCTV or photographs.

"**Processing**" means doing anything with the data. For example, it includes collecting it, holding it, disclosing it and deleting it.

Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, health, sexual orientation, sex life, trade union membership and genetic and biometric data are subject to special protection and considered by EU privacy law to be "**sensitive personal data**".

References in the Privacy Notice to employment, work (and similar expressions) include any arrangement we may have under which an individual provides us with work or services. By way of example, when we mention an "**employment contract**" that includes a contract under which you provide us with services; when we refer to ending your employment, that includes terminating a contract for services. We use the word "**you**" to refer to anyone within the scope of the notice.

2. Legal ground for processing personal data

Under applicable data protection law, there are various grounds on which we can rely when processing your personal data. In some contexts more than one ground applies. We have summarised these grounds as Contract, Legal obligation, Legitimate Interests and Consent and outline what those terms mean in the following table.

Term	***Ground for processing***	***Explanation***
Contract	Processing necessary for performance of a contract with you or to take steps at your request to enter a contract	This covers carrying out our contractual duties and exercising our contractual rights.
Legal obligation	Processing necessary to comply with our legal obligations	Ensuring we perform our legal and regulatory obligations. For example, providing a safe place of work and avoiding unlawful discrimination
Legitimate Interests	Processing necessary for our or a third party's legitimate interests	We or a third party have legitimate interests in carrying on, managing and administering our respective businesses effectively and properly and in connection with those interests processing your data. Your data will not be processed on this basis if our or a third party's interests are overridden by your own interests, rights and freedoms.

Consent	You have given specific consent to processing your data	In general processing of your data in connection with employment is not conditional on your consent. But there may be occasions where we do specific things such as provide a reference, deduct union dues or obtain medical reports and rely on your consent to our doing so.

3. Processing Sensitive Personal Data

If we process sensitive personal data about you, as well as ensuring that one of the grounds for processing mentioned above applies, we will make sure that one or more of the grounds for processing sensitive personal data applies. In outline, these include:

- processing being necessary for the purposes of your or our obligations and rights in relation to employment in so far as it is authorised by law or collective agreement;
- processing relating to data about you that you have made public (e.g. if you tell colleagues that you are ill);
- processing being necessary for the purpose of establishing, making or defending legal claims;
- processing being necessary for provision of health care or treatment, medical diagnosis, and assessment of your working capacity (including (but not limited to) for infectious disease control and / or health emergencies such as Covid-19 or any other pandemic / epidemic); and
- processing for equality and diversity purposes to the extent permitted by law.

4. Further information on the data we process and our purposes

The Core Notice outlines the purposes for which we process your personal data. More specific information on these, examples of the data and the grounds on which we process data are in the table below.

The examples in the table cannot, of course, be exhaustive. For example, although the table does not mention data relating to criminal offences, if we were to find out that someone working for us was suspected of committing a criminal offence, we might process that information if relevant for our purposes.

Purpose	***Examples of personal data that may be processed***	***Grounds for processing***
Recruitment	Information concerning your application and our assessment of it, your references, any checks we may make to verify information provided or background checks and any information connected with your right to work in the UK. If relevant, we may also process information concerning your health, any disability and in connection with any adjustments to working arrangements.	Contract Legal obligation Legitimate interests
Your employment contract including entering it, performing it and changing it.	Information on your terms of employment from time to time including your pay and benefits, such as your participation in pension arrangements, life and medical insurance; and any bonus or share schemes.	Contract Legal obligation Legitimate interests

Purpose	*Examples of personal data that may be processed*	*Grounds for processing*
Contacting you or others on your behalf	Your address and phone number, emergency contact information and information on your next of kin	Contract Legitimate interests
Payroll administration	Information on your bank account, pension contributions and on tax and national insurance Information on attendance, holiday and other leave and sickness absence	Contract Legal obligation Legitimate interests
Supporting and managing your work and performance and any health concerns	Information connected with your work, anything you do at work and your performance including records of documents and emails created by or relating to you and information on your use of our systems including computers, laptops or other device. Management information regarding you including notes of meetings and appraisal records. Information relating to your compliance with our policies. Information concerning disciplinary allegations, investigations and processes and relating to grievances in which you are or may be directly or indirectly involved. Information concerning your health, including self-certification forms, fit notes and medial and occupational health reports.	Contract Legal obligation Legitimate interests
Health and safety of the workforce and assessment of your working capacity	Information concerning your health, including self-certification forms, temperature checks (both self-certified and / or checked by us at your place of work), antibody or disease testing / results, and sharing results of any tests or checks carried out with third parties where it is necessary to do so (on an anonymous basis unless reason requires more specific information to be included).	Consent Legitimate interests Legal obligation Necessary for assessment of working capacity
Changing or ending your working arrangements	Information connected with anything that may affect your continuing employment or the terms on which you work including any proposal to promote you, to change your pay or benefits, to change your working arrangements or to end your employment	Contract Legitimate interests
Physical and system security	CCTV images Records of use of swipe and similar entry cards Records of your use of our systems including computers, phones and other devices and passwords.	Legal obligation Legitimate interests

Purpose	*Examples of personal data that may be processed*	*Grounds for processing*
Providing references in connection with your finding new employment	Information on your working for us and on your performance.	Consent Legitimate interests
Providing information to third parties in connection with transactions that we contemplate or carry out	Information on your contract and other employment data that may be required by a party to a transaction such as a prospective purchaser, seller or outsourcer	Legitimate interests
Monitoring of diversity and equal opportunities	Information on your nationality, racial and ethnic origin, gender, sexual orientation, religion, disability and age	Legitimate interests
Monitoring and investigating compliance with policies and rules – both generally and specifically	We expect our employees to comply with our policies and rules and may monitor our systems to check compliance (.e.g. rules on accessing pornography at work). We may also have specific concerns about compliance and check system and other data to look into those concerns (e.g. log in records, records of usage and emails and documents, CCTV images).	Legitimate interests
Disputes and legal proceedings	Any information relevant or potentially relevant to a dispute or legal proceeding affecting us.	Legitimate interests Legal obligation
Trade union check off arrangements	Details of trade union membership and deductions of contributions made at source	Contract
Day to day business operations including marketing and customer/client relations	Information relating to the work you do for us, your role and contact details including relations with current or potential customers or clients. This may include a picture of you for internal or external use.	Legitimate interests
Maintaining appropriate business records during and after your employment	Information relating to your work, anything you do at work and your performance relevant to such records.	Contract Legal obligation Legitimate interests

Please note that owing to the fact that you are appearing in one of programmes, on some occasions we or third parties will rely upon exemptions to data protection rules in relation to journalistic freedom, the right to artistic expression or more generally, the right to freedom of expression (as mentioned in article 85 of the General Data Protection Regulation and in various jurisdictions' data protection rules, for example in the UK's Data Protection Bill section on the exemption for '*journalistic, academic, artistic or literary purposes*'.

5. Where the data comes from

When you start employment with us, the initial data about you that we process is likely to come from you: for example, contact details, bank details and information on your immigration status and whether you can lawfully

work. We may also require references and information to carry out background checks. In the course of employment, you may be required to provide us with information for other purposes such as sick pay (and SSP) and family rights (e.g. maternity and paternity leave and pay). If you do not provide information that you are required by statute or contract to give us, you may lose benefits or we may decide not to employ you or to end your contract. If you have concerns about this in a particular context, you should speak to HR.

In the course of your work, we may receive personal data relating to you from others. Internally, personal data may be derived from your managers and other colleagues or our IT systems; externally, it may be derived from those with whom you communicate by email or other systems.

In relation to infectious disease control and national health emergencies, including but not limited to Covid-19 and / or other pandemics or epidemics, you may be required to provide us with information or a self-certification which includes sensitive personal data relating to your health and fitness to work on a regular basis as requested by us. In addition, we may require you to undertake testing such as temperature checks and / or antibody or disease tests either at work or any other place we designate during or outside working hours. We shall either receive the results directly or require you to inform us of the results, and shall treat and process the information as sensitive personal data.

6. Who gets to see your data?

Internal use: Your personal data may be disclosed to your managers, HR and administrators for employment, administrative and management purposes as mentioned in this document. We may also disclose this to other members of the All3Media Group including in response to infectious disease prevention and / or health emergencies (including, but not limited to Covid-19) where your personal data and / or test results may need to be disclosed in specific circumstances for the health and safety of the wider workforce and the group as a whole.

External use: *We will only disclose your personal data outside the group if disclosure is consistent with a ground for processing on which we rely and doing so is lawful and fair to you. We may disclose your data if it is necessary for our legitimate interests as an organisation or the interests of a third party (but we will not do this if these interests are over-ridden by your interests and rights in particular to privacy). We may also disclose your personal data if you consent, where we are required to do so by law and in connection with criminal or regulatory investigations or where it is mandated by government regulation or legislation in response to infectious disease control and / or a public health emergency (including, but not limited to, Covid-19).*

Specific circumstances in which your personal data may be disclosed include:

- disclosure to organisations that process data on our behalf such as our payroll service, insurers and other benefit providers, our bank and organisations that host our IT systems and data;
- disclosure to external recipients of electronic communications (such as emails) which contain your personal data.

7. Retaining your Personal Data- more information

Although there is no specific period for which we will keep your personal data, we will not keep it for longer than is necessary for our purposes. In general, we will keep your personal data for the duration of your employment and for a period afterwards. In considering how long to keep it, we will take into account its relevance to our business and your employment either as a record or in the event of a legal claim.

If your data is only useful for a short period (for example, CCTV or a record of a holiday request), we may delete it.

Personal Data relating to job applicants (other than the person who is successful) will normally be deleted after 12 months.

8. Transfers of Personal Data outside the EEA- more information

In connection with our business and for production, broadcasting, distribution, administrative, management, marketing and legal purposes, we may transfer your personal data outside the EEA to members of our group and data processors in other jurisdictions in which we are established. Some of our systems are hosted outside of the EEA. We will ensure that any transfer is lawful and that there are appropriate security arrangements.

9. Access to your personal data and other rights

We try to be as open as we reasonably can about personal data that we process. If you would like specific information, just ask us. You also have a legal right to make a "subject access request". If you exercise this right and we hold personal data about you, we are required to provide you with information on it, including:

- giving you a description and copy of the Personal Data;
- telling you why we are processing it.

If you make a subject access request and there is any question about who you are, we may require you to provide information from which we can satisfy ourselves as to your identity.

As well as your subject access right, you may have a legal right to have your personal data rectified or erased, to object to its processing or to have its processing restricted. If you have provided us with data about yourself (for example your address or bank details), you have the right to be given the data in machine readable format for transmitting to another data controller. This only applies if the ground for processing is Consent or Contract.

If we have relied on consent as a ground for processing, you may withdraw consent at any time – though if you do so that will not affect the lawfulness of what we have done before you withdraw consent.

10. Complaints

If you have complaints relating to our processing of your personal data, you should raise these with HR in the first instance or with your Information Officer. You may also raise complaints with the Information Commissioner who is the statutory regulator. For contact and other details ask HR or see: https://ico.org.uk/ICO.

11. Status of this notice

This notice does not form part of your contract of employment and does not create contractual rights or obligations. It may be amended by us at any time.

Cast, Crew and Talent Privacy Notice

1. Scope

Like most businesses, we hold and process a wide range of information, some of which relates to individuals who we engage to work on our productions. This Privacy Notice explains the type of information we process, why we are processing it and how that processing may affect you.

The notice focuses on individuals who we contract to work on our productions. This includes those in production roles, such as designers, production assistants, camera crew etc. and also those working on-screen be it as extras or featured performers, as well as our voiceover artists. It also covers information on those who have carried out these roles previously.

This Privacy Notice is set out in this document (the Core Notice) and the Supplementary Information in the Annex to this document. In the Supplementary Information, we explain what we mean by "personal data", "processing", "sensitive personal data" and other terms used in the notice.

2. Personal Data- what we hold and why we process it

We process data for the purposes of our business including for production, broadcasting, distribution, marketing, management, administrative and legal purposes. The Supplementary Information provides more specific information on these purposes, on the type of data that may be processed and on the grounds on which we process data. See *Legal grounds for processing personal data* and f*urther information on the data we process and our purposes.*

3. Where the data comes from and who gets to see it

Some of the personal data that we process about you comes from you. For example, if we pay you directly into a bank account, you tell us your contact and banking details. Other personal data about you is generated in the course of your work, for example from other contractors working on your production, or from our employees.

Your personal data may be seen internally by the relevant mangers for that production, our finance teams, in some circumstances, other employees of ours. We may also pass your data outside the organisation, for example to people you are dealing with and payroll agencies or (where applicable) for distribution and marketing purposes.

Further information on this is provided in the Supplementary Information. See *Where the data comes from* and *Who gets to see your data?*

4. How long do we keep Personal Data

We do not keep your personal data for any specific period but will not keep it for longer than is necessary for our purposes. In general, we will keep your personal data for the duration of your engagement and for a period afterwards.

See *Retaining your personal data – more information* in the Supplementary Information.

5. Transfers of Personal Data outside the EEA

We may transfer your personal data outside the EEA to members of our group and processors in the US or, on rarer occasions, other jurisdictions in which we are established. If you featured in a production, the data constituting your performance may be transferred out of the EEA for distribution and marketing purposes. Further information on these transfers and the measures taken to safeguard your data are set out in the Supplementary Information under *Transfers of personal data outside the EEA – more information.*

6. Your data rights

You have a right to make a subject access request to receive information about the data that we process about you. Further information on this and on other rights is in the Supplementary Information under *Access to your personal data and other rights.* We also explain how to make a complaint about our processing of your data.

7. Contact details

In processing your personal data, we act as a data controller. Our contact details are as follows: [*Name and other details*][2].

8. Status of this notice

This notice does not form part of your contract and does not create contractual rights or obligations. It may be amended by us at any time.

[2] Each Operating Company to insert name of appropriate contact within their business

Cast, Crew and Talent Privacy Notice- Supplementary Information

1. What is "Personal Data" and "Processing"

"**Personal data**" is information relating to you (or from which you may be identified) which is processed by automatic means or which is (or is intended to be) part of a structured manual filing system. It includes not only facts about you, but also intentions and opinions about you**.**

Data "**processed automatically**" includes information held on, or relating to use of, a computer, laptop, mobile phone or similar device. It covers data derived from equipment such as access passes within a building, data on use of vehicles and sound and image data such as CCTV. It also covers video, audio and images captured as part of a production.

"**Processing**" means doing anything with the data, for example, it includes collecting it, holding it, disclosing it and deleting it.

Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, health, sexual orientation, sex life, trade union membership and genetic and biometric data are subject to special protection and considered by EU privacy law to be "**sensitive personal data**".

References in the Cast, Crew and Talent Privacy Notice to work or services (and similar expressions) include any arrangement we may have under which an individual provides us services in relation to a production. We use the word "**you**" to refer to anyone within the scope of the notice.

2. Legal grounds for processing Personal Data

Under data protection law, there are various grounds on which we can rely when processing your personal data. In some contexts more than one ground applies. We have summarised these grounds as Contract, Legal obligation, Legitimate Interests and Consent and outline what those terms mean in the following table.

Term	***Ground for processing***	***Explanation***
Contract	Processing necessary for performance of a contract with you or to take steps at your request to enter a contract	This covers carrying out our contractual duties and exercising our contractual rights.
Legal obligation	Processing necessary to comply with our legal obligations	Ensuring we perform our legal and regulatory obligations. For example, providing a safe place of work and avoiding unlawful discrimination.
Legitimate Interests	Processing necessary for our or a third party's legitimate interests	We or a third party have legitimate interests in carrying on, managing and administering our respective businesses effectively and properly and in connection with those interests processing your data. Your data will not be processed on this basis if our or a third party's interests are overridden by your own interests, rights and freedoms.
Consent	You have given specific consent to processing your data	In general processing of your data in connection with the services you provide is not conditional on your consent, although there may be general exceptions to this.

3. Processing Sensitive Personal Data

If we process sensitive personal data about you, as well as ensuring that one of the grounds for processing mentioned above applies, we will make sure that one or more of the grounds for processing sensitive personal data applies. In outline, these include:

- processing being necessary for the purposes of your or our obligations and rights in relation to your engagement in so far as it is authorised by law or collective agreement;
- processing relating to data about you that you have made public (e.g. if you tell us you are ill);
- processing being necessary for the purpose of establishing, making or defending legal claims;
- processing being necessary for provision of health care or treatment, medical diagnosis, and assessment of your working capacity (including (but not limited to) for infectious disease control and / or health emergencies such as Covid-19 or any other pandemic / epidemic); and
- processing for equality and diversity purposes to the extent permitted by law.

4. Further information on the data we process and purposes

The Core Notice outlines the purposes for which we process your personal data. More specific information on these, examples of the data and the grounds on which we process data are in the table below.

The examples in the table cannot, of course, be exhaustive. For example, although the table does not mention data relating to criminal offences, if we were to find out that someone working for us was suspected of committing a criminal offence, we might process that information if relevant for our purposes. We may also require criminal background checks for certain roles – for example those working with minors.

Purpose	***Examples of personal data that may be processed***	***Grounds for processing***
Engagement	Information concerning your application to work on our productions and our assessment of it, your references, any checks we may make to verify information provided or background checks and any information connected with your right to work. If relevant, we may also process information concerning your health, any disability and in connection with any adjustments to working arrangements.	Contract Legal obligation Legitimate interests
Your contract including entering it, performing it and changing it	Information on your terms of engagement from time to time including your role, the duration of your contract and your remuneration.	Contract Legal obligation Legitimate interests
Contacting you or others on your behalf	Your address and phone number, emergency contact information and information on your next of kin.	Contract Legitimate interests
Payroll administration	Information on your bank account, pension contributions and on tax and national insurance (if applicable). Information on attendance and absences.	Contract Legal obligation Legitimate interests

Purpose	*Examples of personal data that may be processed*	*Grounds for processing*
Financial planning and budgeting	Information relating to your remuneration.	Legitimate interests
Enabling the creation, sale and distribution / broadcast of a production you are working on	Information connected with your role including (if applicable) records of documents and emails created by or relating to you and information on your use of our systems including computers, laptops or other device. If you have an on-screen or voiceover role this will likely involve processing images / video / audio of you. Information relating to your compliance with our policies.	Contract Legal obligation Legitimate interests
Health and safety of the workforce and assessment of your working capacity	Information concerning your health, including self-certification forms, temperature checks (both self-certified and / or checked by us at your place of work), antibody or disease testing / results, and sharing results of any test or checks carried out with third parties where it is necessary to do so (on an anonymous basis unless reason requires more specific information to be included).	Consent Legitimate interests Legal obligation Necessary for assessment of working capacity
Changing or ending your working arrangements	Information connected with anything that may affect your continuing engagement or the terms on which you are engaged including any proposal to change the scope of your role, to change your remuneration or to end your contract.	Contract Legitimate interests
Physical and system security	CCTV images. Records of use of swipe and similar entry cards. Records of your use of our systems including computers, phones and other devices and passwords (if applicable).	Legal obligation Legitimate interests
Providing references in connection with your seeking new work on other productions	Information on your working for us and on your performance.	Consent Legitimate interests
Providing information to third parties in connection with transactions that we contemplate or carry out	Information on your contract and remuneration in relation to a given production may be required by a party to a transaction such as a prospective purchaser, seller or outsourcer.	Legitimate interests

Purpose	*Examples of personal data that may be processed*	*Grounds for processing*
Monitoring of diversity and equal opportunities	Information on your nationality, racial and ethnic origin, gender, sexual orientation, religion, disability and age as part of diversity monitoring initiatives. Such data will be aggregated and used for equality of opportunity monitoring purposes. Please note we may share aggregated and anonymised diversity statistics with regulators if formally required / requested.	Legitimate interests
Monitoring and investigating compliance with policies and rules – both generally and specifically	We expect our persons whom we engage to comply with our policies and rules and may monitor our systems to check compliance (.e.g. rules on accessing pornography in work or on set). We may also have specific concerns about compliance and check system and other data to look into those concerns (e.g. log in records, records of usage and emails and documents, CCTV images).	Legitimate interests
Disputes and legal proceedings	Any information relevant or potentially relevant to a dispute or legal proceeding affecting us.	Legitimate interests Legal obligation
Day to day business operations including marketing and travel on our behalf	Information relating to the work you do for us and your role on a production. This may include a picture or profile of you. Information regarding your travel arrangements and location.	Legitimate interests
Maintaining appropriate business records during and after your contract with us ends	Information relating to your contract and anything you do whilst engaged by us.	Contract Legal obligation Legitimate interests

Please note that owing to the fact that you are appearing in one of programmes, on some occasions we or third parties will rely upon exemptions to data protection rules in relation to journalistic freedom, the right to artistic expression or more generally, the right to freedom of expression (as mentioned in article 85 of the General Data Protection Regulation and in various jurisdictions' data protection rules, for example in the UK's Data Protection Bill section on the exemption for '*journalistic, academic, artistic or literary purposes*'.

5. Where data comes from

When you start working on one of our productions, the initial data about you that we process is likely to come from you: for example, contact details, bank details and information on your immigration status and whether you can lawfully work. We may also require references and information to carry out background checks (see above).

In the course of your engagement, we may receive personal data relating to you from others. For example, personal data may be derived from managers and employees of ours (for example those involved in the production you are working on) or our IT systems.

In relation to infectious disease control and national health emergencies, including but not limited to Covid-19 and / or other pandemics or epidemics, you may be required to provide us with information or a self-certification which includes sensitive personal data relating to your health and fitness to work on a regular basis as requested by us. In addition, we may require you to undertake testing such as temperature checks and / or antibody or disease tests either at work or any other place we designate during or outside working hours. We shall either receive the results directly or require you to inform us of the results, and shall treat and process the information as sensitive personal data.

6. Who gets to see your data?

Internal use: Your personal data may be disclosed to our employees working on your production, as well as to our managers and administrators for production, broadcasting, distribution, marketing, administrative and management purposes as mentioned in this document. We may also disclose this to other members of our group including in response to infectious disease prevention and / or health emergencies (including, but not limited to Covid-19) where your personal data and / or test results may need to be disclosed in specific circumstances for the health and safety of the wider workforce and the group as a whole.

External use: We will only disclose your personal data outside the group if disclosure is consistent with a ground for processing on which we rely and doing so is lawful and fair to you. We may disclose your data if it is necessary for our legitimate interests as an organisation or the interests of a third party (but we will not do this if these interests are over-ridden by your interests and rights in particular to privacy). We may also disclose your personal data if you consent, where we are required to do so by law and in connection with criminal or regulatory investigations or where it is mandated by government regulation or legislation in response to infectious disease control and / or public health emergency (including, but not limited to, Covid-19).

Specific circumstances in which your personal data may be disclosed include:

- disclosure to organisations that process data on our behalf such as our payroll service, insurers, our bank and organisations that host our IT systems and data;
- disclosure to external recipients of electronic communications (such as emails) which contain your personal data;
- disclosure of aggregated and anonymised diversity data to relevant regulators as part of a formal request;
- if you have an on-screen role, disclosure of footage, images, or audio recordings of you as part of the broadcasting, distribution and marketing of the production. Or, whether you have an on-screen or off-screen role, to allow us to credit your role.

7. Retaining your Personal Data- more information

Although there is no specific period for which we will keep your personal data, we will not keep it for longer than is necessary for our purposes. In general, we will keep your personal data for the duration of your contract and for a period afterwards. In considering how long to keep it, we will take into account its relevance to our business and your engagement either as a record or in the event of a legal claim.

If your data is only useful for a short period (for example, CCTV), we may delete it. Personal data relating to job applicants (other than the person who is successful) will normally be deleted after 12 months.

Some data, such as production footage itself and credit information, will be kept indefinitely as we have an ongoing legitimate interest in retaining the product.

8. Transfers of Personal Data outside of the EEA- more information

In connection with our business and for production, broadcasting, distribution, administrative, management, marketing and legal purposes, we may transfer your personal data outside the EEA to members of our group

and data processors in other jurisdictions in which we are established. Some of our systems are hosted outside of the EEA. We will ensure that any transfer is lawful and that there are appropriate security arrangements.

9. Access to your Personal Data and other rights

We try to be as open as we reasonably can about personal data that we process. If you would like specific information, just ask us.

You also have a legal right to make a "subject access request". If you exercise this right and we hold personal data about you, we are required to provide you with information on it, including:

- giving you a description and copy of the personal data; and
- telling you why we are processing it

If you make a subject access request and there is any question about who you are, we may require you to provide information from which we can satisfy ourselves as to your identity.

As well as your subject access right, you may have a legal right to have your personal data rectified or erased, to object to its processing or to have its processing restricted. If you have provided us with data about yourself (for example your address or bank details), you have the right to be given the data in machine readable format for transmitting to another data controller. This only applies if the ground for processing is Consent or Contract.

If we have relied on consent as a ground for processing, you may withdraw consent at any time – though if you do so that will not affect the lawfulness of what we have done before you withdraw consent

10. Complaints

If you have complaints relating to our processing of your personal data, you should raise these with your key contact at the production in the first instance or with the Information Officer. You may also raise complaints with your statutory regulator. For contact and other details ask your key contact at the production.

11. Status of this notice

This notice does not form part of your contract and does not create contractual rights or obligations. It may be amended by us at any time.

Contributor Privacy Notice

1. Scope

Like most businesses, we hold and process a wide range of information, some of which relates to individuals who we engage to take part in our productions. This Privacy Notice explains the type of information we process, why we are processing it and how that processing may affect you.

The notice focuses on individuals who take part in our productions. And also covers information on those who have previously taken part in our productions.

This Privacy Notice is set out in this document (the Core Notice) and the Supplementary Information in the Annex to this document. In the Supplementary Information, we explain what we mean by "personal data", "processing", "sensitive personal data" and other terms used in the notice.

2. Personal Data- what we hold and why we process it

We process data for the purposes of our business including for production, broadcasting, distribution and marketing,. The Supplementary Information provides more specific information on these purposes, on the type of data that may be processed and on the grounds on which we process data. See *Legal grounds for processing personal data* and f*urther information on the data we process and our purposes.*

3. Where the data comes from and who gets to see it

Some of the personal data that we process about you comes from you. For example, your name, age and email address. Other personal data about you is generated in the course of you taking part in the production.

Your personal data may be seen internally by relevant people working on the production. We may also pass your data outside the organisation, for example for distribution and marketing purposes. Further information on this is provided in the Supplementary Information. See *Where the data comes from* and *Who gets to see your data?*

4. How long do we keep Personal Data

We do not keep your personal data for any specific period but will not keep it for longer than is necessary for our purposes. In general, we will keep your personal data for so long as you take part in a production and for a period afterwards. See *Retaining your personal data – more information* in the Supplementary Information.

5. Transfers of Personal Data outside the EEA

We may transfer your personal data outside the EEA to members of our group and processors in the US or, on rarer occasions, other jurisdictions in which we are established. If you featured in a production, the data constituting your performance may be transferred out of the EEA for distribution and marketing purposes. Further information on these transfers and the measures taken to safeguard your data are set out in the Supplementary Information under *Transfers of personal data outside the EEA – more information.*

6. Your data rights

You have a right to make a subject access request to receive information about the data that we process about you. Further information on this and on other rights is in the Supplementary Information under *Access to your personal data and other rights.* We also explain how to make a complaint about our processing of your data.

7. Contact details

In processing your personal data, we act as a data controller. Our contact details are as follows: [*Name and other contact details, website and email for contact if wished]*[3].

[3] Each Operating Company to insert name of appropriate contact within their business.

8. Status of this notice

This notice does not form part of your contract and does not create contractual rights or obligations. It may be amended by us at any time.

Contributor Privacy Notice- Supplementary Information

1. What is "Personal Data" and "Processing"

"**Personal data**" is information relating to you (or from which you may be identified) which is processed by automatic means or which is (or is intended to be) part of a structured manual filing system. It includes not only facts about you, but also intentions and opinions about you**.**

Data "**processed automatically**" includes information held on, or relating to use of, a computer, laptop, mobile phone or similar device. It covers data derived from equipment such as access passes within a building, data on use of vehicles and sound and image data such as CCTV. It also covers video, audio and images captured as part of a production.

"**Processing**" means doing anything with the data, for example, it includes collecting it, holding it, disclosing it and deleting it.

Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, health, sexual orientation, sex life, trade union membership and genetic and biometric data are subject to special protection and considered by EU privacy law to be "**sensitive personal data**".

References in the Contributor Privacy Notice to work or services (and similar expressions) include any arrangement we may have under which an individual provides us services in relation to a production. We use the word "**you**" to refer to anyone within the scope of the notice.

2. Legal grounds for processing Personal Data

Under data protection law, there are various grounds on which we can rely when processing your personal data. In some contexts more than one ground applies. We have summarised these grounds as Legal obligation, Legitimate Interests and Consent and outline what those terms mean in the following table.

Term	***Ground for processing***	***Explanation***
Legal obligation	Processing necessary to comply with our legal obligations	Ensuring we perform our legal and regulatory obligations. For example, avoiding unlawful discrimination.
Legitimate Interests	Processing necessary for our or a third party's legitimate interests	We or a third party have legitimate interests in carrying on, managing and administering our respective businesses effectively and properly and in connection with those interests processing your data. Your data will not be processed on this basis if our or a third party's interests are overridden by your own interests, rights and freedoms.
Consent	You have given specific consent to processing your data	In general processing of your data in connection with the services you provide is not conditional on your consent, although there may be general exceptions to this.

3. Processing Sensitive Personal Data

If we process sensitive personal data about you, as well as ensuring that one of the grounds for processing mentioned above applies, we will make sure that one or more of the grounds for processing sensitive personal data applies. In outline, these include:

- Processing being necessary for the purposes of your or our obligations and rights in relation to your engagement in so far as it is authorised by law or collective agreement;
- Processing relating to data about you that you have made public (e.g. if you tell us you are ill);
- Processing being necessary for the purpose of establishing, making or defending legal claims;
- Processing being necessary for provision of health care or treatment, medical diagnosis, and assessment of your working capacity (including (but not limited to) for infectious disease control and / or health emergencies such as Covid-19 or any other pandemic / epidemic);
- Processing for equality and diversity purposes to the extent permitted by law.

4. Further information on the data we process and purposes

The Core Notice outlines the purposes for which we process your personal data. More specific information on these, examples of the data and the grounds on which we process data are in the table below.

The examples in the table cannot, of course, be exhaustive. For example, although the table does not mention data relating to criminal offences, if we were to find out that someone working for us was suspected of committing a criminal offence, we might process that information if relevant for our purposes. We may also require criminal background checks for certain roles – for example those working with minors.

Purpose	***Examples of personal data that may be processed***	***Grounds for processing***
Engagement	Information concerning your taking part in our productions and our assessment of it, your references, any checks we may make to verify information provided or background checks. If relevant, we may also process information concerning your health, any disability and in connection with any adjustments to filming arrangements.	Legal obligation Legitimate interests
Contacting you or others on your behalf	Your address and phone number, emergency contact information and information on your next of kin.	Legitimate interests
Enabling the creation, sale and distribution / broadcast of a production you are taking part in	Information connected with your participation including, the processing of images/ video/ audio of you.	Legal obligation Legitimate interests
Health and safety of you and the workforce and assessment of your capacity to contribute	Information concerning your health, including self-certification forms, temperature checks (both self-certified and / or checked by us when you are at any location specific or controlled by us, antibody or disease testing / results, and sharing results of any tests or checks carried out with third parties where it is necessary to do so (on an	Consent Legitimate interests Legal obligation

Purpose	*Examples of personal data that may be processed*	*Grounds for processing*
	anonymous basis unless reason requires more specific information to be included).	
Physical and system security	CCTV images. Records of use of swipe and similar entry cards.	Legal obligation Legitimate interests
Providing details in connection with your seeking to participate on other production	Information on your taking part in one of our productions.	Consent Legitimate interests
Monitoring of diversity and equal opportunities	Information on your nationality, racial and ethnic origin, gender, sexual orientation, religion, disability and age as part of diversity monitoring initiatives. Such data will be aggregated and used for equality of opportunity monitoring purposes. Please note we may share aggregated and anonymised diversity statistics with regulators if formally required / requested.	Legitimate interests
Disputes and legal proceedings	Any information relevant or potentially relevant to a dispute or legal proceeding affecting us.	Legitimate interests Legal obligation
Day to day business operations including marketing and travel on our behalf	Information relating to your participation in a programme. This may include a picture or profile of you. Information regarding your travel arrangements and location.	Legitimate interests
Maintaining appropriate business records during and after your participation in a programme	Information relating to your participation in one of our productions.	Legal obligation Legitimate interests

Please note that owing to the fact that you are appearing in one of programmes, on some occasions we or third parties will rely upon exemptions to data protection rules in relation to journalistic freedom, the right to artistic expression or more generally, the right to freedom of expression (as mentioned in article 85 of the General Data Protection Regulation and in various jurisdictions' data protection rules, for example in the UK's Data Protection Bill section on the exemption for '*journalistic, academic, artistic or literary purposes*'.

5. Where data comes from

When you participate in one of our productions, the initial data about you that we process is likely to come from you: for example, contact details.

In relation to infectious disease control and national health emergencies, including but not limited to Covid-19 and / or other pandemics or epidemics, you may be required to provide us with information or a self-certification which includes sensitive personal data relating to your health and fitness to contribute on a regular basis as requested by us. In addition, we may require you to undertake testing such as temperature checks and / or antibody or disease tests either on location or any other place we designate during or outside working hours. We shall either receive the results directly or require you to inform us of the results, and shall treat and process the information as sensitive personal data.

6. Who gets to see your data?

Internal use: Your personal data may be disclosed within the [Operating Company] group to our employees working on your production. In response to infectious disease prevention and / or health emergencies (including, but not limited to Covid-19) we may also disclose personal data to other members of the All3Media group where your personal data and / or test results may need to be disclosed in specific circumstances for the health and safety of the wider workforce and the group as a whole.

External use: We will only disclose your personal data outside the [Operating Company] group if disclosure is consistent with a ground for processing on which we rely and doing so is lawful and fair to you. We may disclose your data if it is necessary for our legitimate interests as an organisation or the interests of a third party (but we will not do this if these interests are over-ridden by your interests and rights in particular to privacy). We may also disclose your personal data where it is mandated by government regulation or legislation in response to infectious disease control and / or a public health emergency (including, but not limited to, Covid-19).

Specific circumstances in which your personal data may be disclosed include:

- Disclosure to external recipients of electronic communications (such as emails) which contain your personal data;
- Disclosure of aggregated and anonymised diversity data to relevant regulators as part of a formal request;
- If you have an on-screen role, disclosure of footage, images, or audio recordings of you as part of the broadcasting, distribution and marketing of the production. Or, whether you have an on-screen or off-screen role, to allow us to credit your role.

7. Retaining your Personal Data- more information

Although there is no specific period for which we will keep your personal data, we will not keep it for longer than is necessary for our purposes. In general, we will keep your personal data until the show has been produced and for a period afterwards. In considering how long to keep it, we will take into account its relevance to our business and your participation either as a record or in the event of a legal claim.

If your data is only useful for a short period (for example, CCTV), we may delete it. Some data, such as production footage itself and credit information, will be kept indefinitely as we have an ongoing legitimate interest in retaining the product.

8. Transfers of Personal Data outside of the EEA- more information

In connection with our business and for production, broadcasting, distribution, administrative, management, marketing and legal purposes, we may transfer your personal data outside the EEA to members of our group and data processors in the US and on occasion other jurisdictions in which we are established. Some of our systems are hosted outside of the EEA. We will ensure that any transfer is lawful and that there are appropriate security arrangements.

9. Access to your Personal Data and other rights

We try to be as open as we reasonably can about personal data that we process. If you would like specific information, just ask us.

You also have a legal right to make a "subject access request". If you exercise this right and we hold personal data about you, we are required to provide you with information on it, including:

- Giving you a description and copy of the personal data
- Telling you why we are processing it

If you make a subject access request and there is any question about who you are, we may require you to provide information from which we can satisfy ourselves as to your identity.

As well as your subject access right, you may have a legal right to have your personal data rectified or erased, to object to its processing or to have its processing restricted. If you have provided us with data about yourself, for example your address, you have the right to be given the data in machine readable format for transmitting to another data controller. This only applies if the ground for processing is Consent.

If we have relied on consent as a ground for processing, you may withdraw consent at any time – though if you do so that will not affect the lawfulness of what we have done before you withdraw consent

10. Complaints

If you have complaints relating to our processing of your personal data, you should raise these with your key contact at the production in the first instance. You may also raise complaints with your statutory regulator. For contact and other details ask your key contact at the production.

11. Status of this notice

This notice does not form part of your contract and does not create contractual rights or obligations. It may be amended by us at any time.

Recruitment privacy notice

1. Purpose and Scope

Like most businesses, we hold and process a wide range of information, some of which relates to individuals who we may seek to recruit. This Recruitment Privacy Notice explains the type of information we process, why we are processing it and how that processing may affect you.

2. Personal data- what is Personal Data and Processing

"**Personal data**" is information relating to you (or from which you may be identified) which is processed by automatic means or which is (or is intended to be) part of a structured manual filing system. It includes not only facts about you, but also intentions and opinions about you.

"**Processing**" means doing anything with the data. For example, it includes collecting it, holding it, disclosing it and deleting it.

Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, health, sexual orientation, sex life, trade union membership and genetic and biometric data are subject to special protection and considered by EU privacy law to be "sensitive personal data".

3. Personal data- what we hold and why we process it

We process your data for the purposes of fulfilling our recruitment practices. Some of the personal data that we process about you comes from you. For example, you tell us your contact details. Other personal data about you is generated from references and third party companies such as recruitment agencies. Your personal data will be seen internally by managers, administrators and HR.

4. How long do we keep your Personal Data?

If you are successful in your application your data will be kept on your personnel file. If you are unsuccessful, your data will normally be destroyed twelve months after you have been informed that you were unsuccessful. Irrelevant data such as CCTV images may be deleted after a short period.

5. Transfers of personal data outside the EEA

We may transfer your personal data outside the EEA to members of our group. Where necessary these transfers are covered by the intra-group transfer agreement and model clauses.

6. Contact details

In processing your personal data, we act as a data controller. Our contact details are as follows: [*Name and contact details*][4].

7. Legal grounds for processing your data

What are the grounds for processing?

Under data protection law, there are various grounds on which we can rely when processing your personal data. In some contexts more than one ground applies. We have summarised certain grounds as Legal obligation and Legitimate Interests and outline what those terms mean below.

Term	*Ground for processing*	*Explanation*

[4] Each Operating Company to insert name of appropriate contact within their business

Contract	Processing necessary for performance of a contract with you or to take steps at your request to enter a contract	This covers carrying out our contractual duties and exercising our contractual rights.
Legal obligation	Processing necessary to comply with our legal obligations	Ensuring we perform our legal and regulatory obligations. For example, providing a safe place of work and avoiding unlawful discrimination
Legitimate Interests	Processing necessary for our or a third party's legitimate interests	We or a third party have legitimate interests in carrying on, managing and administering our respective businesses effectively and properly and in connection with those interests processing your data. Your data will not be processed on this basis if our or a third party's interests are overridden by your own interests, rights and freedoms.

Processing sensitive personal data

If we process sensitive personal data about you, as well as ensuring that one of the grounds for processing mentioned above applies, we will make sure that one or more of the grounds for processing sensitive personal data applies (see below), including that the processing is for equality and diversity purposes to the extent permitted by law.

In outline, these include:

- processing being necessary for the purposes of your or our obligations and rights in relation to employment in so far as it is authorised by law or collective agreement;
- processing relating to data about you that you have made public (e.g. if you tell colleagues that you are ill);
- processing being necessary for the purpose of establishing, making or defending legal claims;
- processing being necessary for provision of health care or treatment, medical diagnosis, and assessment of your working capacity (including (but not limited to) for infectious disease control and / or health emergencies such as Covid-19 or any other pandemic / epidemic); and
- processing for equality and diversity purposes to the extent permitted by law.

Further information on the data we process and our purposes

Examples of the data and the grounds on which we process data are in the table below. The examples in the table cannot, of course, be exhaustive.

Purpose	***Examples of personal data that may be processed***	***Grounds for processing***
Recruitment	Information concerning your application and our assessment of it, your references, any checks we may make to verify information provided or background checks and any information connected with your right to work in the UK. If relevant, we may also process information concerning your health, any disability and in connection with any adjustments to working arrangements.	Contract Legal obligation Legitimate interests
Contacting you or others	Your address and phone number, emergency contact information and information on your next of kin	Contract

Purpose	*Examples of personal data that may be processed*	*Grounds for processing*
on your behalf		Legitimate interests
Health and safety of the workforce and assessment of your working capacity	Information concerning your health, including self-certification forms, temperature checks (both self-certified and / or checked by us at our offices), antibody or disease testing / results, and sharing results of any test or checks carried out with third parties where it is necessary to do so (on an anonymous basis unless reason requires more specific information to be included).	Consent Legitimate interests Legal obligation
Security	CCTV images	Legitimate interests
Monitoring of diversity and equal opportunities	Information on your nationality, racial and ethnic origin, gender, sexual orientation, religion, disability and age	Legitimate interests

In relation to infectious disease control and national health emergencies, including but not limited to Covid-19 and / or other pandemics or epidemics, you may be required to provide us with information or a self-certification which includes sensitive personal data relating to your health as requested by us. In addition, we may require you to undertake testing such as temperature checks. We shall either receive the results directly or require you to inform us of the results, and shall treat and process the information as sensitive personal data.

Who gets to see your data?

Your personal data may be disclosed to managers, HR and administrators for employment, administrative and management purposes as mentioned in this document. We may also disclose this to other members of our group including in response to infectious disease prevention and / or health emergencies (including, but not limited to Covid-19) where your personal data and / or test results may need to be disclosed in specific circumstances for the health and safety of the wider workforce and the group as a whole.

We may also disclose your personal data where it is mandated by government regulation or legislation in response to infectious disease control and / or a public health emergency (including, but not limited to, Covid-19).

Access to your personal data and other rights

We try to be as open as we reasonably can about personal data that we process. If you would like specific information, just ask us.

You also have a legal right to make a "subject access request". If you exercise this right and we hold personal data about you, we are required to provide you with information, including a description of the personal data, and an explanation of why we are processing it.

If you make a subject access request and there is any question about who you are, we may require you to provide information from which we can satisfy ourselves as to your identity.

As well as your subject access right, you may have a legal right to have your personal data rectified or erased, to object to its processing or to have its processing restricted.

If we have relied on consent as a ground for processing, you may withdraw consent at any time – though if you do so that will not affect the lawfulness of what we have done before you withdraw consent.

Complaints

If you have complaints relating to our processing of your personal data, you should raise these with HR in the first instance. You may also raise complaints with the Information Commissioner who is the statutory regulator. For contact and other details ask HR or see: https://ico.org.uk/ICO.

Scope

This notice does not form part of any contractual relationship between us and a job applicant. This notice can be changed at any time.

Prospective Cast, Crew and Talent Privacy Notice

1. Scope

Like most businesses, we hold and process a wide range of information, some of which relates to individuals who we seek to engage on our productions. This Privacy Notice explains the type of information we process, why we are processing it and how that processing may affect you.

The notice focuses on individuals who we are speaking to about potentially taking part in or working on one of our productions. This Privacy Notice is set out in this document (the Core Notice) and the Supplementary Information in the Annex to this document. In the Supplementary Information, we explain what we mean by "personal data", "processing", "sensitive personal data" and other terms used in the notice.

2. Personal Data- what we hold and why we process it

We process data for the purposes of our business including for our productions. The Supplementary Information provides more specific information on this purpose, the type(s) of data that may be processed and on the grounds on which we process data. See *Legal grounds for processing personal data* and f*urther information on the data we process and our purposes.*

3. Where the data comes from and who gets to see it

Some of the personal data that we process about you comes from you, for example your mobile number, name, age and email address

Your personal data may be seen internally by relevant people working on a production. Further information on this is provided in the Supplementary Information. See *Where the data comes from* and *Who gets to see your data?*

4. How long do we keep Personal Data

We do not keep your personal data for any specific period but will not keep it for longer than is necessary for our purposes. If you are chosen to work on a production, we will, in general, keep your personal data for the duration of your engagement and for a period afterwards. Otherwise we will only retain for your personal data for a short period of time after our discussions have ended. See *Retaining your personal data – more information* in the Supplementary Information.

5. Your data rights

You have a right to make a subject access request to receive information about the data that we process about you. Further information on this and on other rights is in the Supplementary Information under *Access to your personal data and other rights.* We also explain how to make a complaint about our processing of your data.

6. Contact details

In processing your personal data, we act as a data controller. Our contact details are as follows: [*Name and contact details*][5].

7. Status of this notice

This notice is for information purposes only and does not mean or imply that you will be chosen to work on one of our productions.

[5] Each Operating Company to insert name of appropriate contact within their business

Prospective Cast, Crew and Talent Privacy Notice- Supplementary Information

1. What is "Personal Data" and "Processing"

"**Personal data**" is information relating to you (or from which you may be identified) which is processed by automatic means or which is (or is intended to be) part of a structured manual filing system. It includes not only facts about you, but also intentions and opinions about you**.**

Data "**processed automatically**" includes information held on, or relating to use of, a computer, laptop, mobile phone or similar device. It covers data derived from equipment such as access passes within a building, data on use of vehicles and sound and image data such as CCTV. It also covers video, audio and images captured as part of a production.

"**Processing**" means doing anything with the data, for example, it includes collecting it, holding it, disclosing it and deleting it.

Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, health, sexual orientation, sex life, trade union membership and genetic and biometric data are subject to special protection and considered by EU privacy law to be "**sensitive personal data**".

References in the privacy notice for prospective Cast, Crew and Talent to work or services (and similar expressions) include any arrangement we may have under which an individual provides us services in relation to a production. We use the word "**you**" to refer to anyone within the scope of the notice.

2. Legal grounds for processing Personal Data

Under data protection law, there are various grounds on which we can rely when processing your personal data. In some contexts more than one ground applies. We have summarised these grounds as Contract, Legal obligation, Legitimate Interests and Consent and outline what those terms mean in the following table.

Term	***Ground for processing***	***Explanation***
Contract	Processing necessary for performance of a contract with you or to take steps at your request to enter a contract	This covers carrying out our contractual duties and exercising our contractual rights.
Legal obligation	Processing necessary to comply with our legal obligations	Ensuring we perform our legal and regulatory obligations. For example, providing a safe place of work and avoiding unlawful discrimination.
Legitimate Interests	Processing necessary for our or a third party's legitimate interests	We or a third party have legitimate interests in carrying on, managing and administering our respective businesses effectively and properly and in connection with those interests processing your data. Your data will not be processed on this basis if our or a third party's interests are overridden by your own interests, rights and freedoms.
Consent	You have given specific consent to processing your data	In general processing of your data in connection with the services you provide is not conditional on your consent, although there may be general exceptions to this.

3. Processing Sensitive Personal Data

If we process sensitive personal data about you, as well as ensuring that one of the grounds for processing mentioned above applies, we will make sure that one or more of the grounds for processing sensitive personal data applies. In outline, these include:

- Processing being necessary for the purposes of your or our obligations and rights in relation to your engagement in so far as it is authorised by law or collective agreement;
- Processing relating to data about you that you have made public (e.g. if you tell us you are ill);
- Processing being necessary for the purpose of establishing, making or defending legal claims;
- Processing being necessary for provision of health care or treatment, medical diagnosis, and assessment of your working capacity (including (but not limited to) for infectious disease control and / or health emergencies such as Covid-19 or any other pandemic / epidemic);
- Processing for equality and diversity purposes to the extent permitted by law.

4. Further information on the data we process and purposes

The Core Notice outlines the purposes for which we process your personal data. More specific information on these, examples of the data and the grounds on which we process data are in the table below.

The examples in the table cannot, of course, be exhaustive. For example, although the table does not mention data relating to criminal offences, if we were to find out that someone working for us was suspected of committing a criminal offence, we might process that information if relevant for our purposes. We may also require criminal background checks for certain roles – for example those working with minors.

Purpose	***Examples of personal data that may be processed***	***Grounds for processing***
Engagement	Information concerning your application to work on our productions and our assessment of it, your references, any checks we may make to verify information provided or background checks and any information connected with your right to work. If relevant, we may also process information concerning your health, any disability and in connection with any adjustments to working arrangements.	Contract Legal obligation Legitimate interests
Your contract including entering it, performing it and changing it	Information on your terms of engagement from time to time including your role, the duration of your contract and your remuneration.	Contract Legal obligation Legitimate interests
Contacting you or others on your behalf	Your address and phone number, emergency contact information and information on your next of kin.	Contract Legitimate interests
Payroll administration	Information on your bank account, pension contributions and on tax and national insurance (if applicable). Information on attendance and absences.	Contract Legal obligation Legitimate interests
Financial planning and budgeting	Information relating to your remuneration.	Legitimate interests

Purpose	*Examples of personal data that may be processed*	*Grounds for processing*
Enabling the creation, sale and distribution / broadcast of a production you are working on	Information connected with your role including (if applicable) records of documents and emails created by or relating to you and information on your use of our systems including computers, laptops or other device. If you have an on-screen or voiceover role this will likely involve processing images / video / audio of you. Information relating to your compliance with our policies.	Contract Legal obligation Legitimate interests
Health and safety of the workforce and assessment of your working capacity	Information concerning your health, including self-certification forms, temperature checks (both self-certified and / or checked by us at your place of work), antibody or disease testing / results, and sharing results of any tests or checks carried out with third parties where it is necessary to do so (on an anonymous basis unless reason requires more specific information to be included).	Consent Legitimate interests Legal obligation Necessary for assessment of working capacity
Changing or ending your working arrangements	Information connected with anything that may affect your continuing engagement or the terms on which you are engaged including any proposal to change the scope of your role, to change your remuneration or to end your contract.	Contract Legitimate interests
Physical and system security	CCTV images. Records of use of swipe and similar entry cards. Records of your use of our systems including computers, phones and other devices and passwords (if applicable).	Legal obligation Legitimate interests
Providing references in connection with your seeking new work on other productions	Information on your working for us and on your performance.	Consent Legitimate interests
Providing information to third parties in connection with transactions that we contemplate or carry out	Information on your contract and remuneration in relation to a given production may be required by a party to a transaction such as a prospective purchaser, seller or outsourcer.	Legitimate interests
Monitoring of diversity and equal opportunities	Information on your nationality, racial and ethnic origin, gender, sexual orientation, religion, disability and age as part of diversity monitoring initiatives. Such data will be aggregated and used for equality of opportunity monitoring purposes. Please note we may share aggregated and anonymised diversity statistics with regulators if formally required / requested.	Legitimate interests

Purpose	*Examples of personal data that may be processed*	*Grounds for processing*
Monitoring and investigating compliance with policies and rules – both generally and specifically	We expect our persons whom we engage to comply with our policies and rules and may monitor our systems to check compliance (.e.g. rules on accessing pornography in work or on set). We may also have specific concerns about compliance and check system and other data to look into those concerns (e.g. log in records, records of usage and emails and documents, CCTV images).	Legitimate interests
Disputes and legal proceedings	Any information relevant or potentially relevant to a dispute or legal proceeding affecting us.	Legitimate interests Legal obligation
Day to day business operations including marketing and travel on our behalf	Information relating to the work you do for us and your role on a production. This may include a picture or profile of you. Information regarding your travel arrangements and location.	Legitimate interests
Maintaining appropriate business records during and after your contract with us ends	Information relating to your contract and anything you do whilst engaged by us.	Contract Legal obligation Legitimate interests

Please note that owing to the fact that you are appearing in one of programmes, on some occasions we or third parties will rely upon exemptions to data protection rules in relation to journalistic freedom, the right to artistic expression or more generally, the right to freedom of expression (as mentioned in article 85 of the General Data Protection Regulation and in various jurisdictions' data protection rules, for example in the UK's Data Protection Bill section on the exemption for '*journalistic, academic, artistic or literary purposes*'.

5. Where data comes from

When you start working on one of our productions, the initial data about you that we process is likely to come from you: for example, contact details, bank details and information on your immigration status and whether you can lawfully work. We may also require references and information to carry out background checks (see above).

In the course of your engagement, we may receive personal data relating to you from others. For example, personal data may be derived from managers and employees of ours (for example those involved in the production you are working on) or our IT systems.

In relation to infectious disease control and national health emergencies, including but not limited to Covid-19 and / or other pandemics or epidemics, you may be required to provide us with information or a self-certification which includes sensitive personal data relating to your health and fitness to work on a regular basis as requested by us. In addition, we may require you to undertake testing such as temperature checks and / or antibody or disease tests either at work or any other place we designate during or outside working hours. We shall either receive the results directly or require you to inform us of the results, and shall treat and process the information as sensitive personal data.

6. Who gets to see your data?

Internal use: Your personal data may be disclosed to our employees working on your production, as well as to our managers and administrators for production, broadcasting, distribution, marketing, administrative and management purposes as mentioned in this document. We may also disclose this to other members of our group including in response to infectious disease prevention and / or health emergencies (including, but not limited to Covid-19) where your personal data and / or test results may need to be disclosed in specific circumstances for the health and safety of the wider workforce and the group as a whole.

External use: We will only disclose your personal data outside the group if disclosure is consistent with a ground for processing on which we rely and doing so is lawful and fair to you. We may disclose your data if it is necessary for our legitimate interests as an organisation or the interests of a third party (but we will not do this if these interests are over-ridden by your interests and rights in particular to privacy). We may also disclose your personal data if you consent, where we are required to do so by law and in connection with criminal or regulatory investigations or where it is mandated by government regulation or legislation in response to infectious disease control and / or a public health emergency (including, but not limited to, Covid-19).

Specific circumstances in which your personal data may be disclosed include:

- disclosure to organisations that process data on our behalf such as our payroll service, insurers, our bank and organisations that host our IT systems and data;
- disclosure to external recipients of electronic communications (such as emails) which contain your personal data;
- disclosure on a confidential basis to a potential buyer of our business or company for the purposes of evaluation – but only if we were to contemplate selling;
- disclosure of aggregated and anonymised diversity data to relevant regulators as part of a formal request;
- if you have an on-screen role, disclosure of footage, images, or audio recordings of you as part of the broadcasting, distribution and marketing of the production. Or, whether you have an on-screen or off-screen role, to allow us to credit your role.

7. Retaining your Personal Data- more information

Although there is no specific period for which we will keep your personal data, we will not keep it for longer than is necessary for our purposes. In general, we will keep your personal data for the duration of your contract and for a period afterwards. In considering how long to keep it, we will take into account its relevance to our business and your engagement either as a record or in the event of a legal claim.

If your data is only useful for a short period (for example, CCTV or a record of a holiday request), we may delete it. Personal data relating to job applicants (other than the person who is successful) will normally be deleted after 12 months.

Some data, such as production footage itself and credit information, will be kept indefinitely as we have an ongoing legitimate interest in retaining the product.

8. Transfers of Personal Data outside of the EEA- more information

In connection with our business and for production, broadcasting, distribution, administrative, management, marketing and legal purposes, we may transfer your personal data outside the EEA to members of our group and data processors other jurisdictions in which we are established. Some of our systems are hosted in the US. We will ensure that any transfer is lawful and that there are appropriate security arrangements.

9. Access to your Personal Data and other rights

We try to be as open as we reasonably can about personal data that we process. If you would like specific information, just ask us.

You also have a legal right to make a "subject access request". If you exercise this right and we hold personal data about you, we are required to provide you with information on it, including:

- giving you a description and copy of the personal data
- telling you why we are processing it

If you make a subject access request and there is any question about who you are, we may require you to provide information from which we can satisfy ourselves as to your identity.

As well as your subject access right, you may have a legal right to have your personal data rectified or erased, to object to its processing or to have its processing restricted. If you have provided us with data about yourself (for example your address or bank details), you have the right to be given the data in machine readable format for transmitting to another data controller. This only applies if the ground for processing is Consent or Contract.

If we have relied on consent as a ground for processing, you may withdraw consent at any time – though if you do so that will not affect the lawfulness of what we have done before you withdraw consent

10. Complaints

If you have complaints relating to our processing of your personal data, you should raise these with your key contact at the production in the first instance or with our Information Officer. You may also raise complaints with your statutory regulator. For contact and other details ask your key contact at the production.

11. Status of this notice

This notice is for information purposes only and does not mean or imply that you will be chosen to work on one of our productions.

Prospective Contributor Privacy Notice

1. Scope

Like most businesses, we hold and process a wide range of information, some of which relates to individuals who we seek to engage on our productions. This Privacy Notice explains the type of information we process, why we are processing it and how that processing may affect you.

The notice focuses on individuals who we are speaking to about potentially taking part one of our productions. This Privacy Notice is set out in this document (the Core Notice) and the Supplementary Information in the Annex to this document. In the Supplementary Information, we explain what we mean by "personal data", "processing", "sensitive personal data" and other terms used in the notice.

2. Personal Data- what we hold and why we process it

We process data for the purposes of our business including for our productions. The Supplementary Information provides more specific information on this purpose, the type(s) of data that may be processed and on the grounds on which we process data. See *Legal grounds for processing personal data* and f*urther information on the data we process and our purposes***.**

3. Where the data comes from and who gets to see it

Some of the personal data that we process about you comes from you, for example your mobile number, name, age and email address

Your personal data may be seen internally by relevant people working on a production. Further information on this is provided in the Supplementary Information. See *Where the data comes from* and *Who gets to see your data?*

4. How long do we keep Personal Data

We do not keep your personal data for any specific period but will not keep it for longer than is necessary for our purposes. If you are chosen to work on a production, we will, in general, keep your personal data for the duration of your engagement and for a period afterwards. Otherwise we will only retain for your personal data for a short period of time after our discussions have ended. See *Retaining your personal data – more information* in the Supplementary Information.

5. Your data rights

You have a right to make a subject access request to receive information about the data that we process about you. Further information on this and on other rights is in the Supplementary Information under *Access to your personal data and other rights.* We also explain how to make a complaint about our processing of your data.

6. Contact details

In processing your personal data, we act as a data controller. Our contact details are as follows: [*Name and contact details*][6]

7. Status of this notice

This notice is for information purposes only and does not mean or imply that you will be chosen to work on one of our productions.

[6] Each Operating Company to insert name of appropriate contact within their business

Prospective Contributor Privacy Notice- Supplementary Information

1. What is "Personal Data" and "Processing"

"**Personal data**" is information relating to you (or from which you may be identified) which is processed by automatic means or which is (or is intended to be) part of a structured manual filing system. It includes not only facts about you, but also intentions and opinions about you**.**

Data "**processed automatically**" includes information held on, or relating to use of, a computer, laptop, mobile phone or similar device. It covers data derived from equipment such as access passes within a building, data on use of vehicles and sound and image data such as CCTV. It also covers video, audio and images captured as part of a production.

"**Processing**" means doing anything with the data, for example, it includes collecting it, holding it, disclosing it and deleting it.

Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, health, sexual orientation, sex life, trade union membership and genetic and biometric data are subject to special protection and considered by EU privacy law to be "**sensitive personal data**".

References in the privacy notice for prospective contributors to work or services (and similar expressions) include any arrangement we may have under which an individual provides us services in relation to a production. We use the word "**you**" to refer to anyone within the scope of the notice.

2. Legal grounds for processing Personal Data

Under data protection law, there are various grounds on which we can rely when processing your personal data. In some contexts more than one ground applies. We have summarised these grounds as, Legal obligation, Legitimate Interests and Consent and outline what those terms mean in the following table.

Term	***Ground for processing***	***Explanation***
Legal obligation	Processing necessary to comply with our legal obligations	Ensuring we perform our legal and regulatory obligations.
Legitimate Interests	Processing necessary for our or a third party's legitimate interests	We or a third party have legitimate interests in carrying on, managing and administering our respective businesses effectively and properly and in connection with those interests processing your data. Your data will not be processed on this basis if our or a third party's interests are overridden by your own interests, rights and freedoms.
Consent	You have given specific consent to processing your data	In general processing of your data in connection with the services you provide is not conditional on your consent, although there may be general exceptions to this.

3. Processing Sensitive Personal Data

If we process sensitive personal data about you, as well as ensuring that one of the grounds for processing mentioned above applies, we will make sure that one or more of the grounds for processing sensitive personal data applies. In outline, these include:

- Processing being necessary for the purposes of your or our obligations and rights in relation to your engagement in so far as it is authorised by law or collective agreement;

- Processing relating to data about you that you have made public (e.g. if you tell us you are ill);
- Processing being necessary for the purpose of establishing, making or defending legal claims;
- Processing being necessary for provision of health care or treatment, medical diagnosis, and assessment of your working capacity (including (but not limited to) for infectious disease control and / or health emergencies such as Covid-19 or any other pandemic / epidemic);
- Processing for equality and diversity purposes to the extent permitted by law.

4. Further information on the data we process and purposes

The Core Notice outlines the purposes for which we process your personal data. More specific information on these, examples of the data and the grounds on which we process data are in the table below. The examples in the table cannot, of course, be exhaustive. For example, although the table does not mention data relating to criminal offences, if we were to find out that someone working for us was suspected of committing a criminal offence, we might process that information if relevant for our purposes. We may also require criminal background checks for certain roles – for example those working with minors.

Purpose	***Examples of personal data that may be processed***	***Grounds for processing***
Potential Engagement	Information concerning your application to work on our productions and our assessment of it, your references, any checks we may make to verify information provided or background checks and any information connected with your right to work. If relevant, we may also process information concerning your health, any disability and in connection with any adjustments to filming arrangements.	Legal obligation Legitimate interests
Evaluating your potential role on a production to enable its creation, broadcast, sale and distribution	Information connected with our potential role including, if you are in consideration for an on-screen or voiceover role, the processing images / video / audio of you.	Legal obligation Legitimate interests
Providing details in connection with our seeking new engagements on other productions	Information relating to your potential role with us	Legitimate interests
Health and safety of the workforce and assessment of your working capacity	Information concerning your health, including self-certification forms, temperature checks (both self-certified and / or checked by us in connection with your potential role), antibody or disease testing / results, and sharing results of any tests or checks carried out with third parties where it is necessary to do so (on an anonymous basis unless reason requires more specific information to be included).	Consent Legitimate interests Legal obligation
Physical and system security	CCTV images. Records of use of swipe and similar entry cards.	Legal obligation Legitimate interests

Purpose	*Examples of personal data that may be processed*	*Grounds for processing*
Monitoring of diversity and equal opportunities	Information on your nationality, racial and ethnic origin, gender, sexual orientation, religion, disability and age as part of diversity monitoring initiatives. Such data will be aggregated and used for equality of opportunity monitoring purposes. Please note we may share aggregated and anonymised diversity statistics with regulators if formally required / requested.	Legitimate interests
Disputes and legal proceedings	Any information relevant or potentially relevant to a dispute or legal proceeding affecting us.	Legitimate interests Legal obligation

Please note that owing to the fact that you are appearing in one of programmes, on some occasions we or third parties will rely upon exemptions to data protection rules in relation to journalistic freedom, the right to artistic expression or more generally, the right to freedom of expression (as mentioned in article 85 of the General Data Protection Regulation and in various jurisdictions' data protection rules, for example in the UK's Data Protection Bill section on the exemption for '*journalistic, academic, artistic or literary purposes*'

5. Where data comes from

When you apply to be in one of our productions, the initial data about you that we process is likely to come from you, for example, contact details. We may also require references and information to carry out background checks (see above).

In relation to infectious disease control and national health emergencies, including but not limited to Covid-19 and / or other pandemics or epidemics, you may be required to provide us with information or a self-certification which includes sensitive personal data relating to your health and fitness to work as requested by us. In addition, we may require you to undertake testing such as temperature checks and / or antibody or disease tests. We shall either receive the results directly or require you to inform us of the results, and shall treat and process the information as sensitive personal data.

6. Who gets to see your data?

Internal use: Your personal data may be disclosed within the [***name of operating company***] working on your production for the purposes of deciding whether to include you in a production. In response to infectious disease and / or health emergencies (including, but not limited to Covid-19) we may also disclose personal data to other members of the All3Media group where your personal data and / or test results may need to be disclosed in specific circumstances for the health and safety of the wider workforce and the group as a whole.

External use: We will only disclose your personal data outside the [***name of operating company***] if disclosure is consistent with a ground for processing on which we rely and doing so is lawful and fair to you. We may disclose your data if it is necessary for our legitimate interests as an organisation or the interests of a third party (but we will not do this if these interests are over-ridden by your interests and rights in particular to privacy). We may also disclose your personal data where it is mandated by government regulation or legislation in response to infectious disease control and / or a public health emergency (including, but not limited to, Covid-19).

Specific circumstances in which your personal data may be disclosed include:

- Disclosure to external recipients of electronic communications (such as emails) which contain your personal data;

- Disclosure of aggregated and anonymised diversity data to relevant regulators as part of a formal request.

7. Retaining your Personal Data- more information

Although there is no specific period for which we will keep your personal data, we will not keep it for longer than is necessary for our purposes. In general, we will keep your personal data until the show has been produced and for a period afterwards. In considering how long to keep it, we will take into account its relevance to our business and your engagement either as a record or in the event of a legal claim.

If your data is only useful for a short period (for example, CCTV, we may delete it. Personal data relating to contributor applications (other than the person who is successful) will normally be deleted after 12 months.

8. Transfers of Personal Data outside of the EEA- more information

In connection with our business and for production, broadcasting, distribution, administrative, management, marketing and legal purposes, we may transfer your personal data outside the EEA to members of our group and data processors in the US and on occasion other jurisdictions in which we are established. Some of our systems are hosted in the US. We will ensure that any transfer is lawful and that there are appropriate security arrangements.

9. Access to your Personal Data and other rights

We try to be as open as we reasonably can about personal data that we process. If you would like specific information, just ask us. You also have a legal right to make a "subject access request". If you exercise this right and we hold personal data about you, we are required to provide you with information on it, including:

- giving you a description and copy of the personal data; and
- telling you why we are processing it

If you make a subject access request and there is any question about who you are, we may require you to provide information from which we can satisfy ourselves as to your identity.

As well as your subject access right, you may have a legal right to have your personal data rectified or erased, to object to its processing or to have its processing restricted. If you have provided us with data about yourself (for example your address or bank details), you have the right to be given the data in machine readable format for transmitting to another data controller.

10. Complaints

If you have complaints relating to our processing of your personal data, you should raise these with your key contact at the production in the first instance. You may also raise complaints with your statutory regulator. For contact and other details ask your key contact at the production.

11. Status of this notice

This notice is for information purposes only and does not mean or imply that you will be chosen to work on one of our productions.

Arrangements with Staff and Freelancers

1. Purpose and scope

To comply with the provisions of GDPR, All3Media and all Operating Companies are required to ensure that all agreements entered into contain appropriate provisions regarding data protection. This guidance covers agreements and arrangements with Staff and Freelancers.

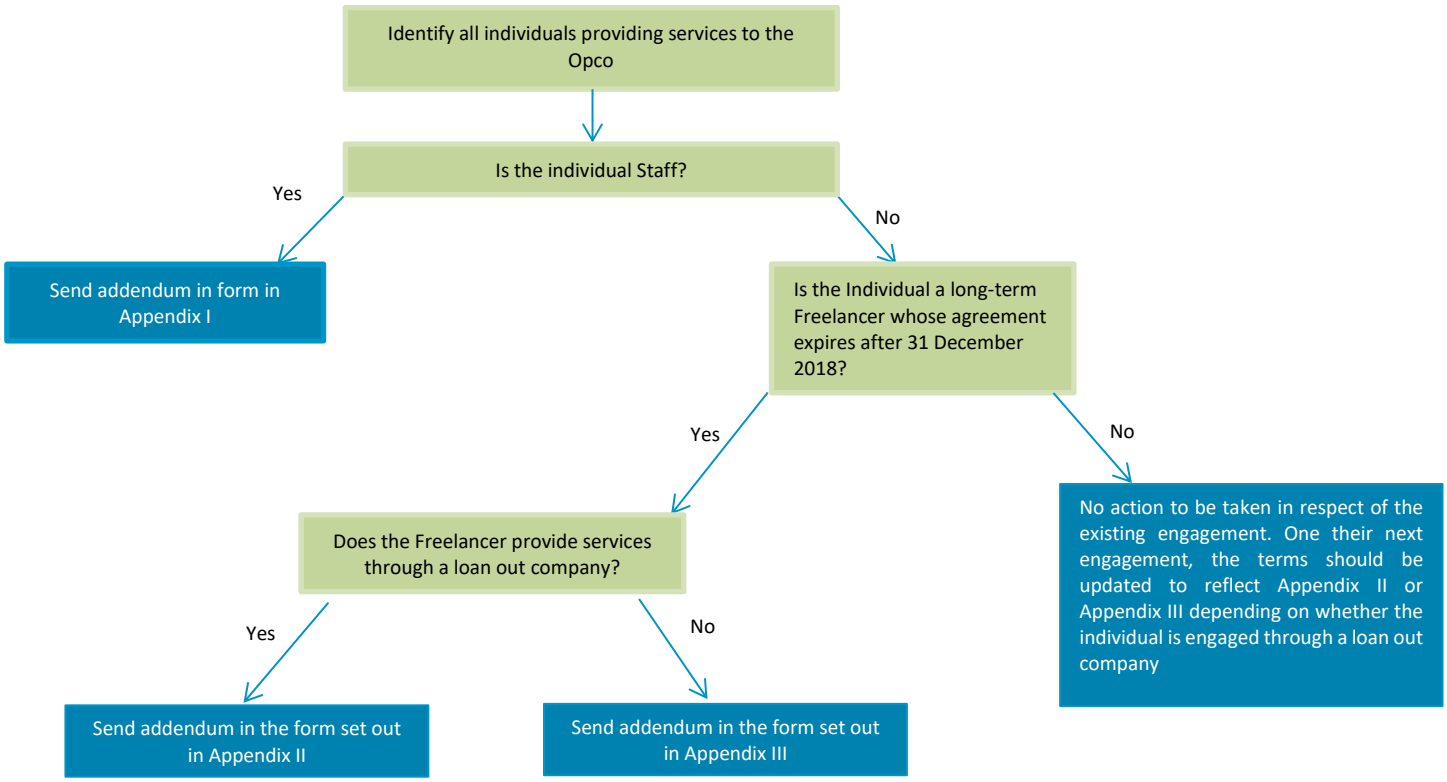
2. New agreements

All new agreements with employees should be entered into on the standard form employment agreements.

GDPR also requires that existing agreements with Staff and Freelancers are also updated. This section sets out the process to be followed when identifying and updating the relevant existing agreements that should be updated as part of the compliance process.

Identifying agreements to be updated

Each Operating Company should identify those agreements that require updating as per the chart below.



Updating agreements

Once the relevant employment related agreements have been identified, the applicable addendum should be circulated to the relevant individuals. This may be done by email. A suggested form of cover email is included at Appendix IV.

Generally, you will not need to ask for a response however you should check the employment agreements of your senior executives as the provisions of their contract may require their consent or acknowledgement to any changes to their agreement.

Appendix I

ADDENDUM TO AGREEMENTS WITH STAFF

This addendum applies to persons who are Staff of [NAME OF OPERATING COMPANY] and relates to our obligations to comply with the General Data Protection Regulation. For the purposes of this addendum, "Agreement" means your [employment agreement] [engagement agreement] you have with us.

This addendum is incorporated into your Agreement replaces any clauses in your Agreement so far as they deal with data protection. Specifically, but without limitation, it replaces any clause under which you have previously given your consent to process your personal data in a workplace context and, for the avoidance of doubt, we are not relying on any such clause.

In the event of conflict between the current terms of your Agreement and this addendum, the terms of this addendum shall prevail.

1 Personal data

1.1 In this clause:

'**Agreement**' means your agreement of employment or engagement with us.

'**We**' or '**Us**' refers to [***name of Operating Company***].

All definitions in this clause are intended to apply within this clause only and do not affect the definitions in your Agreement outside of this clause.

Processing of personal data and our policies

1.2 We hold and process a wide range of information including information relating to individuals or from which an individual may be identified, such information is "**personal data**".

1.3 In processing personal data, we are required to comply with the law on data protection. To help us achieve this, we have adopted policies including the Data Management Policy, the Data Security Policy and Data Breach Protocol (copies of which may be found on our intranet and are available from HR). You must read these and comply with them in carrying out your work. If you are unclear how the policies apply, you should speak to [***your Operating Company's Information Officer***][***HR***] in the first instance.

Data protection principles

1.4 In complying with the law on data protection, we are required to comply with what are known as data protection principles. These are summarised in the Data Management Policy. In performing your role and carrying out your responsibilities, you must do your best to ensure that we comply with these principles.

1.5 A key element of the data protection principles is the duty to ensure that data is processed securely and protected against unauthorised or unlawful processing or loss. The Data Security Policy sets out more detail. Key elements include the following:

(a) laptops, memory sticks, phones and other mobile devices must be password protected and, where possible encrypted. You must take care of them and keep them secure;

(b) you must either set or, where you have been provided a device with a pre-existing password, change your password so that it strings together three unrelated words or four letters or more with each word separated with a symbol. An example password is: table&hull%peachess. Passwords must be kept confidential and not shared; and

(c) you must only access the information you are authorised to for the purposes of your work.

Data breach – and urgent notification

1.6 If you discover a data breach, you **must** notify your line manager and your Operating Company's Information Officer immediately in line with the Data Breach Protocol. Depending on context, you may then need to provide further information on the circumstances of the breach.

A data breach occurs where there is destruction, loss, alteration or unauthorised disclosure of or access to personal data which is being held, stored, transmitted or processed in any way. For example, there is a data breach if our servers are hacked or if you lose a laptop or USB stick or send an email to the wrong person by mistake.

Failure to notify a breach or to provide information as set out above will be treated seriously and disciplinary action may be taken.

Further information regarding how we handle data breach is available on our intranet in our Data Breach Protocol.

Why we process personal data

1.7 For information on the nature of the data we process, why we process it, the legal basis for processing and related matters, please refer to our Workplace Privacy Notice which may be found on our intranet and is also available from HR. In summary:

(a) we process personal data relating to you for the purposes of our business including management, administrative, employment and legal purposes; and

(b) we monitor our premises and the use of our communication facilities, including monitoring compliance with our data and IT policies, and where non-compliance is suspected, looking in a more targeted way.

The summary above is for information only. We do not, in general, rely on your consent as a legal basis for processing. Agreeing the terms of this clause will not constitute your giving consent to our processing of your data.

1.8 We reserve the right to amend the policies referred to above from time to time.

Appendix II

ADDENDUM TO AGREEMENTS WITH FREELANCERS ENGAGED THROUGH A LOAN OUT COMPANY

This addendum applies to Freelancers and who provide services to Operating Company through a loan out company and relates to our obligations to comply with the General Data Protection Regulation. It does not apply to employees or workers. If you are a Freelancer but provide your services directly – i.e. not through a company, a different addendum applies to you and you should speak to [*name and contact details of appropriate contact*]. For the purposes of this addendum "Agreement" means the agreement for provision of services your personal service company has with us.

This addendum is incorporated into our agreement with your personal service company and replaces any clauses in the agreement to the extent they deal with data protection or data privacy. In the event of conflict between the current terms of the agreement and this addendum, the terms of this addendum shall prevail.

1 Personal data

1.1 In this clause:

"**Agreement**" means the agreement for provision of services you have with us.

"**consultant**" means any individual providing services under this agreement on your behalf.

"**data protection legislation**" means, the EU data protection directive 95/46/EC, the general data protection regulation or EC regulation 2016/679 ('GDPR') when in force, the privacy and electronic communications (EC Directive) Regulations 2003 and all applicable laws and regulations relating to the processing of personal data and privacy which may relate to you or the consultant, including where applicable, any guidance notes and codes of practice issued by the European commission and applicable national regulators (including where relevant the UK Information Commissioner);

"**GDPR**" means the general data protection regulation or EC regulation 2016/679.

"**group company**" means any holding company or subsidiary or otherwise of [*name of operating company*] from time to time and any other subsidiary of any holding company of [*name of operating company*] from time to time;

"**we**" or "**us**" means [*name of operating company*].

References to "data controller", data processor", "processing", "data protection officer" and "personal data" shall have the same meaning as defined in the data protection legislation.

All definitions in this clause are intended to apply within this clause only and do not affect the definitions in your agreement outside of this clause.

1.2 You agree that you shall be the "data controller" in respect of the personal data of the consultant and will share the personal data with us and any relevant group company as data controllers in common.

1.3 You agree that you shall comply with your own obligations under the data protection legislation.

1.4 You agree that you will provide services under this agreement in such a way as to ensure that we and any group company can comply with our obligations under the data protection legislation. In particular, you and the Consultant must follow our policies and procedures in respect of data protection (including the Data Management Policy and the Data Security Policy) and any other relevant policies which may be introduced from time to time. You must ensure that the consultant is provided with, reads, and follows these policies.

1.5 You shall also ensure that the Consultant is provided with and reads any policies and notices which provide information to data subjects about what personal data we process. This includes our Cast, Crew and Talent Privacy Notice. A copy of which is available from HR.

1.6 We reserve the right to amend the policy and protocol documents referred to above from time to time.

1.7 In addition to the above, for any personal data that we provide to you in relation to the services or your engagement, you are regarded as a data processor and the following conditions apply:

(a) you must processes the personal data only on documented instructions from us, including with regard to transfers of personal data to a third country or an international organisation;

(b) you must ensure that any persons authorised to process the personal data have committed themselves to confidentiality;

(c) you must comply with article 32 of the GDPR, including implementing appropriate technical and organisational measures to ensure the security of the personal data;

(d) you must not engage another processor ('sub-processor') in respect of personal data provided to you by us without prior written authorisation from us. If a sub-processor is engaged you will ensure that they enter into a binding agreement which meets the requirements of article 28 of the GDPR and you will remain liable for any breach of data protection legislation committed by that sub-processor;

(e) you must assist us, insofar as this is possible, with our obligations to respond to requests for exercising data subjects' rights;

(f) taking into account the nature of the processing and the information available to you, you must assist us in ensuring compliance with our data security obligations including the obligations pursuant to articles 32 to 36 of the GDPR;

(g) you must, at our election, delete or return all the personal data to us at the end of this agreement.

(h) you must make available to us all information necessary to demonstrate compliance with our obligations and allow for and contribute to audits or inspections conducted by us, or by another on our behalf; and

(i) you must immediately inform us if, in your opinion, an instruction infringes the data protection legislation.

1.8 You shall be responsible for the costs of ensuring your compliance with this clause.

Appendix III

ADDENDUM TO AGREEMENTS WITH FREELANCERS OTHER THAN THOSE ENGAGED THROUGH A LOAN OUT COMPANY

This addendum applies to persons who are Freelancers and who provide services to [*NAME OF OPERATING COMPANY*]. It does not apply to Staff or if you provide services through a loan out company. For the purposes of this addendum, "Agreement" means the agreement for provision of services you have with us.

This addendum is incorporated into your Agreement replaces any clauses in your Agreement so far as they deal with data protection. Specifically, but without limitation, it replaces any clause under which you have previously given your consent to process your personal data in a workplace context and, for the avoidance of doubt, we are not relying on any such clause.

In the event of conflict between the current terms of your Agreement and this addendum, the terms of this addendum shall prevail.

1 Personal Data

1.1 In this clause:

"**Agreement**" means the agreement for provision of services you have with us.

"**Data Protection Legislation**" means, the EU Data Protection Directive 95/46/EC, the General Data Protection Regulation or EC Regulation 2016/679 ('GDPR') when in force, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and all applicable laws and regulations relating to the processing of personal data and privacy which may relate to you or the Consultant, including where applicable, any guidance notes and codes of practice issued by the European Commission and applicable national regulators (including where relevant the UK Information Commissioner);

"**GDPR**" means the General Data Protection Regulation or EC Regulation 2016/679.

'**We**' or '**Us**' refers to [***name of operating company***].

References to "data controller", data processor", "processing", "data protection officer" and "personal data" shall have the same meaning as defined in the Data Protection Legislation.

All definitions in this clause are intended to apply within this clause only and do not affect the definitions in your Agreement outside of this clause.

Processing of personal data and our policies

1.2 We hold and process a wide range of information including information relating to individuals or from which an individual may be identified, such information is "**personal data**".

1.3 In processing personal data, we are required to comply with the law on data protection. To help us achieve this, we have adopted policies including the Data Management Policy, Data Security Policy and Data Breach Protocol. You must read these and comply with them when providing services. If you are unclear how the policies apply or, more generally, what you need to do to comply with the law on data protection, you should speak to your key contact at [***name of operating company***] in the first instance.

Data protection principles

1.4 In complying with the law on data protection, we are required to comply with what are known as data protection principles. These are summarised in the Data Management Policy and Data Security Policy. In performing the services you provide to us and carrying out your responsibilities, you must do your best to ensure that we comply with these principles.

1.5 A key element of the data protection principles is the duty to ensure that data is processed securely and protected against unauthorised or unlawful processing or loss. The Data Security Policy sets out more detail. Key elements include the following:

(a) laptops, memory sticks, phones and other mobile devices must be password protected and, where possible encrypted. You must take care of them and keep them secure;

(b) you must either set or, where you have been provided a device with a pre-existing password, change your password so that it strings together three unrelated words or four letters or more with each word separated with a symbol. An example password is: table&hull%peachess. Passwords must be kept confidential and not shared; and

(c) you must only access the information you are authorised to for the purposes of your work.

Data breach – and urgent notification

1.6 If you discover a data breach, you **must** notify your key contact at [***name of operating company***] immediately in line with the Data Breach Protocol. Depending on context, you may then need to provide further information on the circumstances of the breach.

A data breach occurs where there is destruction, loss, alteration or unauthorised disclosure of or access to personal data which is being held, stored, transmitted or processed in any way. For example, there is a data breach if our servers are hacked or if you lose a laptop or USB stick or send an email to the wrong person by mistake.

Failure to notify a breach or to provide information as set out above will be treated seriously and can constitute a breach of your Agreement.

Further information regarding how we handle data breach is included in the Data Breach Protocol.

Why we process personal data

1.7 For information on the nature of the data we process, why we process it, the legal basis for processing and related matters, please refer to our Workplace Privacy Notice which may be found on our intranet. In summary:

(a) we process personal data relating to you for the purposes of our business including management, administrative, employment and legal purposes; and

(b) we monitor our premises and the use of our communication facilities, including monitoring compliance with our data and IT policies, and where non-compliance is suspected, looking in a more targeted way.

The summary above is for information only. We do not, in general, rely on your consent as a legal basis for processing. Agreeing the terms of this clause will not constitute your giving consent to our processing of your data.

1.8 We reserve the right to amend the policy and protocol documents referred to above from time to time.

Data Processing

1.9 In addition to the above, for any personal data that we provide to you in relation to the services rendered under your Agreement you are regarded as a data processor and the following conditions apply:

(a) you must processes the personal data only on documented instructions from us, including with regard to transfers of personal data to a third country or an international organisation;

(b) you must ensure that any persons authorised to process the personal data have committed themselves to confidentiality;

(c) you must comply with Article 32 of the GDPR, including implementing appropriate technical and organisational measures to ensure the security of the personal data;

(d) you must not engage another processor ('Sub-Processor') in respect of personal data provided to you by us without prior written authorisation from us. If a Sub-Processor is engaged you will ensure that they enter into a binding agreement which meets the requirements of Article 28 of the GDPR and you will remain liable for any breach of Data Protection Legislation committed by that Sub-Processor;

(e) you must assist us, insofar as this is possible, with our obligations to respond to requests for exercising data subjects' rights;

(f) taking into account the nature of the processing and the information available to you, you must assist us in ensuring compliance with our data security obligations including the obligations pursuant to Articles 32 to 36 of the GDPR;

(g) you must, at our election, delete or return all the personal data to us at the end of this Agreement.

(h) you must make available to us all information necessary to demonstrate compliance with our obligations and allow for and contribute to audits or inspections conducted by us, or by another on our behalf; and

(i) you must immediately inform us if, in your opinion, an instruction infringes the Data Protection Legislation;

1.10 You shall be responsible for the costs of ensuring your compliance with this clause.

Appendix IV

FORM OF COVER EMAIL

Dear [•]

As you may be aware, the General Data Protection Regulations ("**GDPR**") come into force in May of this year. In order for us to comply with our obligations under GDPR, we are required to update the provisions relating to data protection contained in our [employment][freelancer] agreements, including yours.

The attached addendum sets out the new data protection provisions that apply to your [employment][engagement] with us and replace the existing ones in your agreement. Please contact [•] should you have any questions.

Many thanks
[•]

Third party contracts (Non- employment)

1. Purpose and scope

To comply the provisions of GDPR, All3Media and all Operating Companies are required to ensure that all agreements entered that contain appropriate provisions regarding data protection. This guidance covers agreements with third parties only. See the Arrangements with Permanent Staff and Freelancers Guidance for agreements with employees and freelancers (including Freelancers working through a loan out company). Transfers within the All3Media Group are covered by the All3Media intra-group transfer agreement.

2. New agreements

All new agreements entered into where Personal Data held by an Operating Company will be processed by the third party should include those clauses set out in part 1 of Appendix I. These clauses reflect the minimum standard required to comply with GDPR and assume that the Operating Company is the Data Controller and that such Personal Data will not be processed or transferred outside of the EEA.

Where your Operating Company is acting as Data Processor (i.e. processing personal data on behalf of a third party) the clauses set out in appendix II reflect the minimum standard required to comply with GDPR and assuming that the relevant data will not be processed or transferred outside of the EEA.

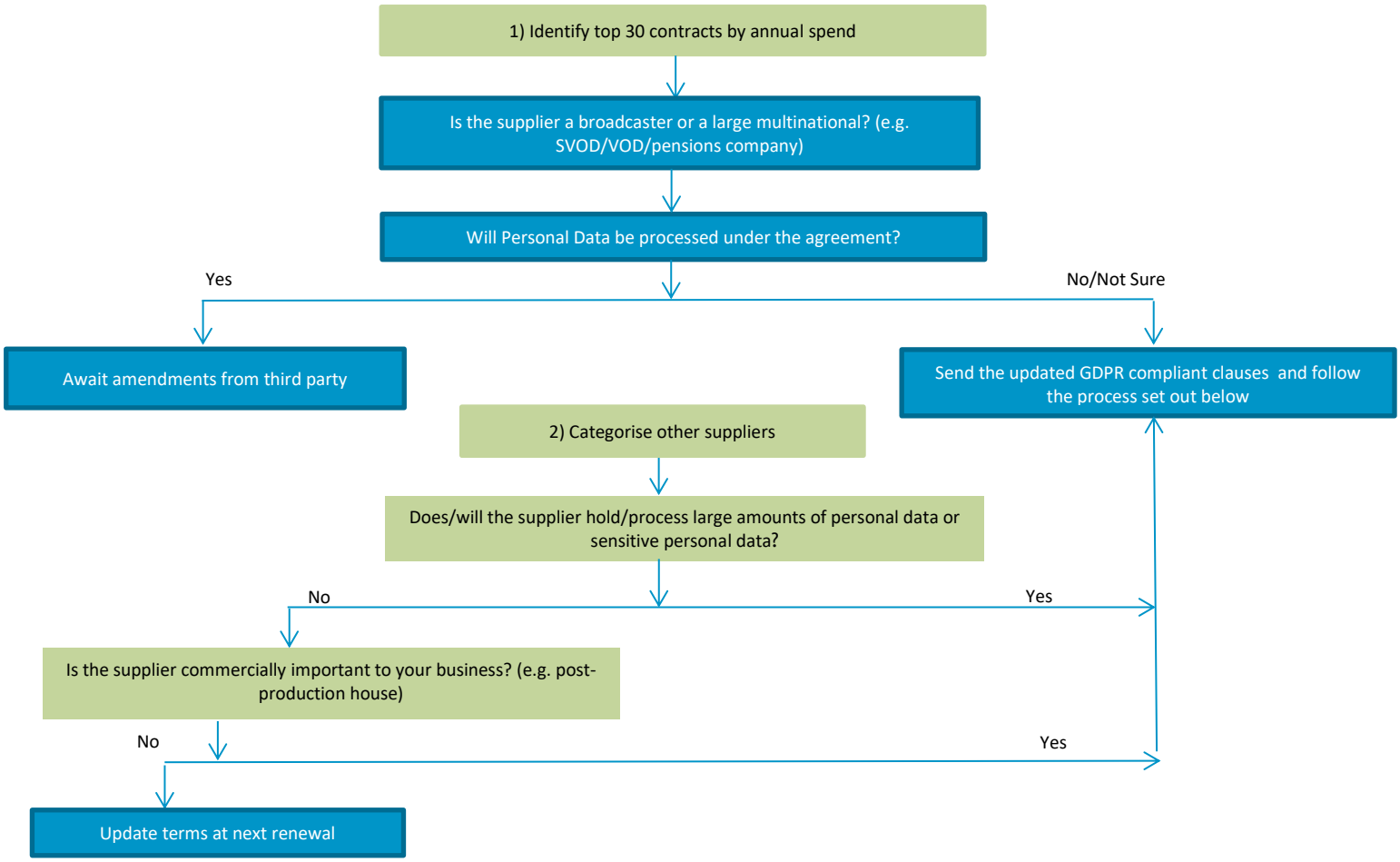
Where your Operating Company is acting as a Data Controller and the relevant data will be transferred to and processed outside of the EEA, the relevant agreement should include the relevant model clauses which may be found at https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en#international-data-transfers-using-model-contracts. The model clauses are standard clauses that have been issued by European Commission as standard contractual clauses that offer sufficient safeguards on data protection for the relevant data to be transferred outside of the EEA. Where these clauses are used, they must be used in their entirety and without amendment.

3. Existing agreements

GDPR also requires that existing agreements are also updated. This section sets out the process to be followed when identifying and updating the relevant existing agreements entered into by an Operating Company.

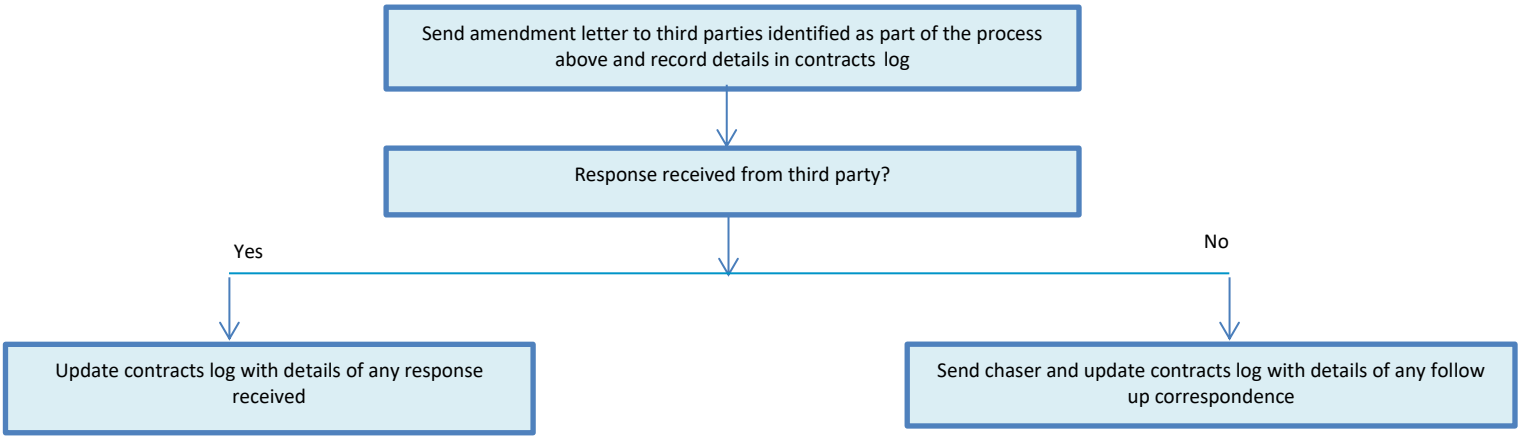
Reviewing and identifying existing third party contracts to be updated

Each Operating Company should identify those agreements that require updating as per the chart below and record them in their Third Party Contracts Log (the form of which is set out in part 2 of Appendix II).



Updating third party contracts

Once the third party contracts have been identified, you should follow the process below.



A deadline for responding should be included in any amendment letter sent and, where a response is not received within that time frame, at least one chaser should be sent.

Records of the amendment letters sent (including copies of the letters if sent by post), responses received and any chasers sent should be retained to demonstrate compliance with GDPR. The log included in part 2 pf Appendix I should be used for this purpose and copies of the log may be requested from time to time. These logs will not be shared within the All3Media Group but will instead be kept as a record of the actions taken by your Operating Company to comply with GDPR.

Group wide contracts

Group wide agreements such as EE, Virgin, Bupa will be reviewed at All3Media Group level.

Appendix I

PART 1- TEMPLATE CLAUSES- OPERATING COMPANY ACTING AS DATA CONTROLLER AND SERVICES ARE BEING PROVIDED TO OPERATING COMPANY

Definitions

"**Data Protection Legislation**" means Data Protection Act 1998, the EU Data Protection Directive 95/46/EC, the General Data Protection Regulations (being EC Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the movement of such data) (when in force), the Privacy and Electronic Communications (EC Directive) Regulations 2003 and all applicable laws and regulations relating to the processing of personal data and privacy, including where applicable, any guidance notes and codes of practice issued by the European Commission and applicable national regulators including the UK Information Commissioner.

Provisions to be included in front end of agreement

The parties acknowledge and agree that in order to provide the [Services], [the Service Provider] may process personal data. [•][7] sets out the subject matter and duration of the processing; nature and purpose of the processing; the type of personal data being processed; and the categories of data subject.

Each party acknowledges and agrees that each party has respective rights and obligations under applicable Data Protection Legislation. The Service Provider shall, and without prejudice to its other rights or obligations, in respect of its processing of such personal data comply with the provisions set out in schedule [A].

SCHEDULE [A]

1. The Service Provider shall comply with the following provisions in respect of the processing of personal data in the supply of the Services:

1.1 process the data only to the extent, and in such a manner, as is necessary to provide the Services and in accordance with the Company's written instructions from time to time and the Service Provider shall not process or permit the processing of the data for any other purpose. If the Service Provider is ever unsure as to the parameters of the instructions issued by the Company and/or believes that the Company's instructions may conflict with the requirements of Data Protection, the Service Provider shall immediately notify the Company for clarification and where requested provide reasonable details in support of any assertion that the Company's instructions may be unlawful;

1.2 shall ensure that any person authorised to process data in connection with this Agreement is subject to a duty of confidentiality;

1.3 having regard to the state of technological development and the cost of implementing any measures, take appropriate technical and organisational measures against the unauthorised or unlawful processing of data and against the accidental loss or destruction of, or damage to data, to ensure a level of security appropriate to: a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage of the data; and b) the nature of the data to be protected. Such measures shall be of at least the minimum standard required by Data Protection Legislation and be of a standard no less than the standards compliant with good industry practice for the protection of personal data;

[7] Note: description of data processing services to be provided or reference to schedule or scope of works that set out such services.

1.4 assist the Company by appropriate technical and organisational measures in responding to, and complying with, data subject requests;

1.5 provide the Company with full co-operation and assistance in relation to the Company's obligations and rights under Data Protection Legislation including providing the Company with all information and assistance necessary to investigate security breaches carry out privacy impact assessments or otherwise to assess or demonstrate compliance by the parties with Data Protection Legislation;

1.6 notify the Company in writing without undue delay and in any event with 24 hours of becoming aware becomes aware of any accidental or deliberate, unauthorised or unlawful acquisition, destruction, loss, alteration, corruption, access, use or disclosure of personal data under this Agreement or in breach of the Service Provider's security obligations under this Agreement;

1.7 not engage any third party to process data (or otherwise sub-contract or outsource the processing of any data to a third party) (a "**Sub processor**") without the prior written consent of the Company acting in its sole discretion. Where such consent is given, it is conditional on the Service Provider:

1.7.1 entering into a written contract with the Sub processor that:
1.7.2 is on terms that the same as those set out in this paragraph;
1.7.3 provides sufficient guarantees to implement appropriate technical and organisation measures in compliance with the Data Protection Legislation;
1.7.4 terminates automatically on termination or expiry of this Agreement for any reason; and
1.7.5 remaining liable for all acts or omissions of the Sub processors as if they were acts or omissions of the Service Provider;

1.8 return or destroy (as directed in writing by the [Operating Company]) all data it has in its possession and promptly delete existing copies unless applicable law requires storage of the personal data.

2. The Service Provider shall keep at its normal place of business a written record of data processing carried out in the course of the Services and in respect of the measures taken by the Service Provider under paragraph 1 of this Schedule, ("**Records**").

3. The Service Provider shall permit the Company, its third-party representatives or a regulator or its third party representatives, on reasonable notice during normal business hours, access to inspect, and take copies of, the Records and any other information held at the Service Provider's [and/or Sub processors' premises] or on the Service Provider's [and/or Sub processors'] systems relating to this Agreement, for the purpose of auditing the Service Provider's compliance with its obligations under this Schedule.

PART 2- THIRD PARTY CONTRACTS LOG

Details of third party contract	Details of amendment letter sent	Response	Follow-up

PART 3- FORM OF COVER LETTER TO THIRD PARTIES

[ON OPERATING COMPANY HEADED NOTEPAPER]

NAME AND ADDRESS OF THIRD PARTY
[By email: [•]]
Dear [•]

[**contract description**] (the "**Agreement**")

As you aware, the General Data Protection Regulations ("**GDPR**") come into force in May of this year. In order for us comply with our obligations under GDPR we are required to update the data protection provisions in all of our contracts with our suppliers including the Agreement.

We have attached to this letter:

(i) the clauses which replace and supersede clauses [•] of the Agreement; and
(ii) a new schedule [•] which replaces schedule [•][which sets out the types of data being processed and the reasons for the processing as required under GDPR,

(together the "**Amendments**").

Please sign and return a copy of this letter acknowledging receipt of this letter and your agreement to the Amendments and to those other terms of the Agreement that are deemed to be varied by reason of the Amendments by no later than [•] 2018[8].

For and on behalf of

……
[Operating Company]

Agreed and acknowledged

……..
[Name of third party]

[8] We suggest that each third party be given a period of 30 days to reply to the letter.

Appendix II

TEMPLATE CLAUSES WHERE OPERATING COMPANY IS ACTING AS PROCESSOR AND IS THE SERVICE PROVIDER

Definitions

"**Data Protection Legislation**" means Data Protection Act 1998, the EU Data Protection Directive 95/46/EC, the General Data Protection Regulations (being EC Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the movement of such data) (when in force), the Privacy and Electronic Communications (EC Directive) Regulations 2003 and all applicable laws and regulations relating to the processing of personal data and privacy, including where applicable, any guidance notes and codes of practice issued by the European Commission and applicable national regulators including the UK Information Commissioner (or similar or equivalent);

"**Security Breach**" means accidental or deliberate, unauthorised or unlawful acquisition, destruction, loss, alteration, corruption, access, use or disclosure of personal data processed under to this Agreement or breach of the Service Provider's security obligations under this Agreement.

Provisions to be included in front end of agreement

1.11 The parties acknowledge and agree that in order to provide the Services, the Service Provider may process personal data. [•][9] sets out the subject matter and duration of the processing; nature and purpose of the processing; the type of personal data being processed; and the categories of data subject.

1.12 Each party acknowledges and agrees that each party has respective rights and obligations under applicable Data Protection Legislation. The Service Provider shall, and without prejudice to its other rights or obligations, in respect of its processing of such personal data comply with the provisions set out in schedule [A].

SCHEDULE [A]

The Service Provider shall comply with the following provisions in respect of the processing of personal data in the supply of the Services:

(a) process the data only to the extent, and in such a manner, as is necessary for the purposes of this Agreement and in accordance with the Customer's lawful written instructions from time to time.;

(b) ensure that any person authorised to process data in connection with this Agreement is subject to a duty of confidentiality;

(c) take such measures as may be required in line with Article 32 of the GDPR (Security);

(d) assist the Customer by using appropriate technical and organisational measures in responding to, and complying with, data subject requests;

(e) provide the Customer with reasonable co-operation and assistance in relation to the Customer's obligations and rights under Data Protection Legislation, taking into account the nature of the processing and the information available to the processor, including providing the Customer and relevant Regulators (as applicable) with all information and assistance reasonably necessary to investigate security breaches, carry out privacy impact assessments or otherwise to demonstrate compliance by the parties with Data Protection Legislation;

[9] Note: description of data processing services to be provided or reference to schedule or scope of works that set out such services.

(f) without undue delay notify the Customer, and provide such co-operation, assistance and information as the Customer may reasonably require if the Service Provider becomes aware of any Security Breach;

(g) keep a written record of any processing of the data carried out in the course of the Services ("Records");

(h) permit no more than once per year the Customer, its third-party representatives (who is not a competitor of the Service Provider) or a regulator, on reasonable notice during normal business hours access to inspect, and take copies of, the Records for the purpose of auditing the Service Provider's compliance with its obligations under this clause;

(i) not engage any third party to process data (or otherwise sub-contract or outsource the processing of any data to a third party) (a "Sub processor"), provided that it:

(i) notifies the Customer of any new or replacement Sub processors. If the Customer objects to the appointment of a new or replacement Sub processor, it shall notify the Service Provider within five business days;

(ii) enters into a written contract with the Sub processor that:

(1) provides protections or guarantees that Sub processor considers necessary to implement appropriate technical and organisation measures in compliance with the Data Protection Legislation; and

(2) terminates automatically on termination or expiry of this Agreement for any reason; and

(iii) remains liable for all acts or omissions of the Sub processors as if they were acts or omissions of the Service Provider (except to the extent caused or exacerbated by the Customer);

(j) return or destroy (as directed in writing by the Customer) all personal data it has in its possession and delete existing copies unless applicable law requires storage of the personal data.

Website Privacy Policy

Last Updated [insert date]

We respect the privacy of every person who visits [Operating Company website] (the "**Site**") and we are committed to ensuring a safe online experience.

1 Purpose of this Policy

This privacy policy ("**Privacy Policy**") explains our approach to any personal information that we might collect from you or which we have obtained about you from a third party and the purposes for which we process your personal information and will inform you of the nature of the personal information about you that is processed by us and how you can request that we delete, update, transfer it and/or provide you with access to it.

This Privacy Policy is intended to assist you in making informed decisions when using the Site. Please take a moment to read and understand it. Please note that it should be read in conjunction with our Website Terms of Use[10].

Please also note that this Privacy Policy only applies to the use of your personal information obtained by us, it does not apply to your personal information collected during your communications with third parties.

2 Who are we and what do we do?

The Site is operated by [Operating Company], ("**we**", "**us**" or "**our**"). [Operating Company] is an English company with registered company number: **XXXXX** and whose registered office is at Berkshire House, 168-171 High Holborn, London WC1V 7AA.

3 What personal information do we collect and how do we use it?

Our primary goal in collecting personal information from you is to: (i) verify your identity; (ii) comply with any applicable law, court order, other judicial process, or the requirements of a regulator; (iii) use as otherwise required or permitted by law.

In particular, we use your personal information for business administration and legal compliance purposes including:

- to comply with our legal obligations;
- to enforce our legal rights;
- protect rights of third parties; and
- in connection with a business transition such as a merger, acquisition by another company, or sale of all or a portion of our assets.

Who do we share your personal information with for such purposes?

We will share your personal information with professional advisers such as lawyers and accountants and/or governmental or regulatory authorities.

What is our legal basis?

Where we use your personal information in connection with a business transition, enforce our legal rights, or to protect the rights of third parties it is in our legitimate interest to do so. For all other purposes described in this section, it is our legal obligation to use your personal information to comply with any legal obligations imposed upon us such as a court order.

Where we share your sensitive personal information, we shall obtain your consent to do so.

[10] Note: include link to website terms of use.

Any other purposes for which we wish to use your personal information that are not listed above, or any other changes we propose to make to the existing purposes will be notified to you using your contact details.

4 How do we obtain your consent?

Where our use of your personal information requires your consent, you can provide such consent:

- at the time we collect your personal information following the instructions provided; or
- by informing us by e-mail, post or phone using the contact details set out in this Privacy Policy.

5 [Our use of cookies and similar technologies

Our Sites use certain cookies of which you should be aware. **Please see our Cookie Policy** to find out more about the cookies we use and how to manage and delete cookies.][11]

6 Third Party Links and Services

Our Site contains links to third party websites and services. Please remember that when you use a link to go from our Site to another website or you request a service from a third party, this Privacy Policy no longer applies and your browsing and interaction on any other websites, or your dealings with any other third party service provider, is subject to that website's or third party service provider's own rules and policies.

We do not monitor, control, or endorse the privacy practices of any third parties and we therefore encourage you to become familiar with the privacy practices of every website you visit or third party service provider that you deal with and to contact them if you have any questions about their respective privacy policies and practices.

7 How long do we keep your personal information for?

We do not keep your data for any specific period but will not keep it for longer than is necessary for our purposes.

8 Confidentiality and security of your personal information

We are committed to keeping the personal information you provide to us secure and we will take reasonable precautions to protect your personal information from loss, misuse or alteration by implementing information security policies, rules and technical measures to protect the personal information that we have under our control from:

- unauthorised access;
- improper use or disclosure;
- unauthorised modification; and
- unlawful destruction or accidental loss.

All of our employees and data processors (i.e. those who process your personal information on our behalf, for the purposes listed above), who have access to, and are associated with the processing of personal information, are obliged to respect the confidentiality of the personal information of all users

9 Your rights

You have the right to apply for a copy of the information we hold about you. This is called a data subject access request and you can make a request in writing to us using the contact details below. We may require additional information about you, including to verify your identity, before disclosing any information to you. You also have the right to have any inaccurate information about you corrected. You may ask us to correct or delete any information you think is inaccurate or not up to date. Please contact us in writing using the contact details below if you could like any updates made to your personal information.

10 How to contact us?

[11] Note: to be included only where Operating Company website uses cookies.

If you have any questions about this Privacy Policy or want to exercise your rights set out in this Privacy Policy, please contact us by sending an email to [insert email address][12].

11 Changes to this Privacy Policy

To ensure that you are always aware of how we use your personal information we will update this Privacy Policy from time to time to reflect any changes to our use of your personal information and as required to comply with changes in applicable law or regulatory requirements. However, we encourage you to review this Privacy Policy periodically to be informed of how we use your personal information.

[12] Each Operating Company to insert relevant contact details.

Website Terms and Conditions

Use of this website

Use of the [All3Media][Operating Company] website (the "**Website**") is governed by these terms and conditions (the "**Terms**"). Please read these Terms carefully. By using the Website, you confirm that you accept these Terms and that you agree to comply with them. If you do not agree to these Terms, you must not use the Website.

Other policies that may apply

Please also refer to the [All3Media][Operating Company] Privacy Policy (the "**Privacy Policy**") [insert hyperlink or link] [and the [All3Media][Operating Company] Cookie Policy (the "**Cookie Policy**") [insert hyperlink or link]] [13] which also apply to your use of the Website.

Amendments to these Terms and other applicable policies

[All3Media][Operating Company] reserves the right to amend these Terms [,] [and/or] the Privacy Policy [and the Cookie Policy] from time to time without notice to you. By continuing to use the Website after the Terms [,][and/or] the Privacy Policy [and/or the Cookie Policy] have been amended, you will be deemed to have agreed to such amendments. You should therefore continue to check these Terms [,][and/or] the Privacy Policy [and the Cookie Policy] to understand the terms and conditions that apply at the time.

Availability of this Website

[All3Media][Operating Company] reserves the right to withdraw, suspend or restrict access to and the availability of the Website (or any part of it) without notice to you or to any other party.

Intellectual property rights

All copyright, trademarks and other intellectual property rights in materials on and in the Website are owned by or licensed to [All3Media][Operating Company]. All intellectual property rights are reserved. You may view, download and print pages from the Website for your own personal use provided that, in all cases, you acknowledge [All3Media][Operating Company] as the source of the material. Save as expressly provided in this paragraph, you may not copy, download, modify, reproduce, amend, distribute or delete or otherwise use for any purpose any material, content or part of the Website.

Third party websites

The Website may contain links to third party websites which are not controlled by [All3Media][Operating Company]. Should you use to access such websites, you do so at your own risk and you agree that [All3Media][Operating Company] has no liability towards you in respect of any loss or damage suffered by you resulting from or connected to your use of such third party websites.

Disclaimer

The Website and its content are provided on an 'as is' basis without any representation, warranty or guarantee (whether express or implied) including, without limitation, as to its accuracy, quality, completeness or fitness for purpose. [All3Media][Operating Company] does not warrant that the Website, its content or the server that makes it available are error free, virus free or free of other harmful elements or that your use of the Website will be uninterrupted.

[All3Media][Operating Company] will not be liable for any loss or damage (whether direct or indirect, including but not limited to, consequential loss, loss of profits, business interruption, loss of business opportunity, damage to goodwill or reputation) suffered arising out or in connection with your use of the Website or its content.

[13] Note: to be included only where website uses cookies.

Miscellaneous

If any of these Terms are found to be illegal, invalid or otherwise unenforceable by reason as a result of any applicable law or regulation, then to the extent permissible where the relevant law or regulation applies, such term shall be amended so as to make it legal, valid and enforceable. If such amendment is not possible, then the relevant term shall be deemed deleted from these Terms. The remaining Terms shall survive such amendment and shall remain in full force and effect.

These Terms are governed by and construed in accordance with the laws of England and Wales. Any disputes arising from or in connection with these Terms, use of the Website or its content shall be subject to the exclusive jurisdiction of the courts of England and Wales.

The Website is operated by [All3Media Limited, a company incorporated in England and Wales (company number 4781820) and whose registered office is at Berkshire House, 168-173 High Holborn, London WC1V 7AA. Our VAT number GB 820745736][Opco details].