DATA PROTECTION POLICY
VERSION: 4.0

Version	By Author	Reason	Reviewed Date	Date Ratified
2.6	HB/TS	Add legislation/further info section	January 2017	April 2017
3.0	HB/TS	Updated to meet new GDPR requirements	January 2018	March 2018
4.0	HB/TS	• Add additional GDPR information • Add linked Policies section • Clarity re team roles • Update to retention schedule	January 2019	March 2019

This policy applies to all members of the Make Some Noise (MSN) team including Trustees, staff, volunteers, freelance workers, the carer of a beneficiary / or a beneficiary of Make Some Noise services.

Introduction

Make Some Noise is fully committed to compliance with the requirements of the Data Protection Act 1998 ("the Act"), which came into force on the 1st March 2000 and General Data Processing Regulations (GDPR) which came into force on 28 May 2018. Make Some Noise will therefore follow procedures that aim to ensure that all employees, trustees, sub-contractors, agents, consultants, partners or other servants of Make Some Noise who have access to any personal data held by or on behalf of Make Some Noise, are fully aware of and abide by their duties and responsibilities under the Act and GDPR.

Statement of Policy

In order to operate efficiently and to comply with funding requirements, Make Some Noise has to collect and use information about people with whom it works. These may include children, members of the public, current, past and prospective employees, clients and customers, and suppliers. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means, and there are safeguards within the current legislation to ensure this.

Make Some Noise regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between Make Some Noise and those with whom it carries out its activities. Make Some Noise will ensure that it treats personal information lawfully and correctly.

To this end Make Some Noise fully endorses and adheres to the Principles of Data Protection as set out in the Data Protection Act 1998 and GDPR.

Implementation
The CEO of Make Some Noise will be responsible for ensuring that the Policy is implemented with responsibility for:

- The provision of cascade data protection training
- For the development of best practice guidelines
- For carrying out compliance checks to ensure adherence with the Data Protection Act.

Data controller and data processor
There is a distinction under the GDPR between a 'data controller' and a 'data processor'. This is because different organisations involved in processing personal data have varying degrees of responsibility. An organisation must choose whether it is a data controller, or a data processor as regards a particular activity and cannot be both. As a Data Controller Make Some Noise is responsible for ensuring that all potential data subjects have sight of this notice prior to the collection and/or processing of their personal data by Make Some Noise.

Responsibilities
This policy does not form part of the formal contract of employment, however it is a condition of employment that team members will abide by the rules and policies made by Make Some Noise. Any failures to follow the policy can therefore result in disciplinary proceedings.

Anyone who considers that the policy has not been followed in respect of personal data should raise the matter with Make Some Noise Data Protection Co-ordinator (the Chief Executive Officer).

Team members should also ensure that any information they supply to Make Some Noise is accurate and up to date. Make Some Noise cannot be held accountable for errors arising from changes about which it has not been informed.

Privacy Impact Assessment
Make Some Noise's data processing activities will undergo an initial Privacy Impact Assessment ("PIA") and subsequent PIAs throughout its lifecycle.

A subsequent PIA may be carried out in the following circumstances:
- When setting up a new IT system;

- When new legislation, policies or related matters affecting privacy, are developed;
- When launching a data sharing initiative; and/or
- When personal data is used for new purposes.

The CEO, acting as the Data Protection Officer (DPO), is responsible for determining whether a full PIA is required.

- The CEO shall reach this decision based on a PIA questionnaire, which must be undertaken for the purposes of making such a determination
- All completed PIAs will be signed off by the Board of Trustees
- The CEO shall at all times conduct PIAs by direct reference to the Information Commissioner's Office ("ICO") Code of Practice
- The CEO may seek specialist advice regarding privacy, should he or she feel it is required
- The CEO shall record all outcomes, including whether or not a PIA is required, in the ICO Code of Practice Annexes
- The DPO shall record in all change control processes that a PIA has been considered.

The principles of Data Protection

GDPR requires that personal data shall meet the following legally enforceable principles:

Article 5 of the GDPR requires that personal data shall be:

(a) Processed lawfully, fairly and in a transparent manner in relation to individuals
(b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes
(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
(d) Accurate, and where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
(e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals
(f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measure.

Article 5(2) requires that "the controller shall be responsible for, and be able to demonstrate, compliance with the principles".

The Act and GDPR provide conditions for the processing of any personal data. It also makes a distinction between **personal data and special categories of data**.

Personal data
The GDPR applies to "personal data" meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – eg key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Special Category Data
The GDPR refers to sensitive personal data as "special categories of personal data".

GDPR Article 9 states that "*Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation* ***shall be prohibited***."

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing. GDPR Article 10 states that "Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority. "

NB: It is important to note that, where the ability to identify an individual depends partly on the data held and partly on other information (not necessarily data), the data held will still be "personal and/or special category data".

NB: The presumption is that, because information about these matters could be used in a discriminatory way, and is likely to be of a private nature, it needs to be treated with greater care than other personal data. In particular, if you are processing special category personal data you must satisfy one or more of the conditions for processing which apply specifically to such data, as well as one of the general conditions which apply in every case. The nature of the data is also a factor in deciding what security is appropriate.

Data Protection Training
Make Some Noise is responsible for ensuring that those who are responsible, on a day-to-day basis, for compliance with the General Data Protection Regulation ("GDPR") and relevant good

practice, can exhibit competency in their understanding of the GDPR, good practice and the implementation thereof by Make Some Noise.

Make Some Noise is responsible for ensuring that all the team should be aware of their personal responsibilities in relation to personal data, ensuring that it is properly protected at all times and is only processed in line with organisational procedures.

Make Some Noise shall ensure that all the team are given appropriate and relevant training. It shall be the duty of Make Some Noise to organise both specific training for GDPR responsible persons as well as general training, appropriate for all staff and to maintain records of attendance.

Handling of personal/special category data
Make Some Noise will, through appropriate management and the use of strict criteria and controls:-

Observe fully conditions regarding the fair collection and use of personal information:

- Meet its legal obligations to specify the purpose for which information is used
- Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements
- Ensure the quality of information used
- Apply strict checks to determine the length of time information is held (please see Appendix 1)
- Take appropriate technical and organisational security measures to safeguard personal information
- Ensure that personal information is not transferred abroad without suitable safeguards
- Ensure that the rights of people about whom the information is held can be fully exercised under the Act and GDPR.

  These include:
  - The right to be informed that processing is being undertaken
  - The right of access to one's personal information within the statutory 40 days
  - The right to prevent processing in certain circumstances
  - The right to correct, rectify, block or erase information regarded as incorrect.

In addition, Make Some Noise will ensure that:

- There is someone with specific responsibility for data protection in the organisation (the Chief Executive Officer)
- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice
- Everyone managing and handling personal information is appropriately trained to do so
- Everyone managing and handling personal information is appropriately supervised
- Anyone wanting to make enquiries about handling personal information, whether a member of the team or a member of the public, knows what to do
- Queries about handling personal information are promptly and courteously dealt with

- Methods of handling personal information are regularly assessed and evaluated
- Performance with handling personal information is regularly assessed and evaluated
- Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures (please see Appendix 1)
- All Trustees are to be made fully aware of this policy and of their duties and responsibilities under the Act and GDPR.

The team will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

- Paper files and other records or documents containing personal/special category data are kept in a secure environment
- Personal data held on computers and computer systems is protected by the use of secure passwords, which where possible have forced changes periodically
- Individual passwords should be such that they are not easily compromised.

All sub-contractors, consultants, partners or other servants or agents of Make Some Noise must:

- Ensure that they and all those who have access to personal data held or processed for or on behalf of Make Some Noise, are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the Act. Any breach of any provision of the Act will be deemed as being a breach of any contract between Make Some Noise and that individual, company, partner or firm (see Appendix 1)
- Allow data protection audits by Make Some Noise of data held on its behalf (if requested)
- Indemnify Make Some Noise against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

All sub-contractors who are users of personal information supplied by Make Some Noise will be required to confirm that they will abide by the requirements of the Act with regard to information supplied by Make Some Noise.

Data Subject Consent
Consent is defined as any indication on the part of the data subject that he or she agrees that their personal data may be processed. Consent must be given freely, without any duress, it must be specific, informed and without ambiguity and shall be granted by the data subject either by way of a statement or through clear, affirmative action on his or her part.

Responsibilities
As a data controller, Make Some Noise is responsible for obtaining the consent of the data subject, under the oversight of the CEO.

Consent procedure
Make Some Noise must demonstrate that explicit consent has been given for the processing of a data subject's personal data. This is done using the relevant Make Some Noise registration form.

The specific purpose or purposes of the processing must be set out in the Data Subject Consent Form and the data subject must expressly consent to this.

Make Some Noise must be able to demonstrate the following:

- That the consent of the data subject is easily distinguishable from all other data held on the data subject (i.e. it is easy to locate and identify)
- That the consent of the data subject is made in an intelligible manner, using clear and plain language
- That prior to giving consent the data subject has been informed of his or her rights to withdraw consent, as per the Right to Withdraw Consent Procedure, and
- That the processing of personal data can only take place pursuant to the agreement between make Some Noise and the data subject, whereby the data subject provides his or her explicit consent.

Child consent procedure
In relation to the processing of personal data of children under the age of 16, Make Some Noise requires additional consent from the person who has parental responsibility over the child and Make Some Noise must be able to demonstrate that this additional consent has been provided, using the relevant form and that it has taken reasonable efforts to ensure that the claim of parental responsibility is authentic and true, including the use of available technology.

Right of access
Everyone has the right to access personal data held about them by Make Some Noise, whether in manual or electronic format.

Any individual wishing to exercise this right should apply in writing to the CEO using the Data Subject Request Form. Evidence of ID must be provided when submitting the completed Form, and further clarification will be requested if necessary. Make Some Noise has **one month** from the point they have the necessary information to provide the data subject the personal data requested.

The CEO will carry out a check for all data (electronic and hard-copy databases, including manual files, backup and archived files as well as email folders and archives).

The CEO is responsible for ensuring that a record of all Subject Access Requests is kept – including date received and for reviewing all documents provided to a data subject to check for the mention of any third parties and if a third party is mentioned, to prevent the disclosure of the identity of the third party to the data subject, or to seek written consent from the third party as to the disclosure of their identity.

Right to Withdraw Consent/ Right to Withdraw Parental Consent
Data Subjects have the right to withdraw consent to processing of data.

Those indicating they wish to withdraw consent (either Data Subject or Parental Consent) should complete the Withdrawal of Consent Form and Make Some Noise must be able to demonstrate that the data subject has withdrawn consent, by producing the completed form, if required.

If Make Some Noise was processing the data for multiple purposes, Make Some Noise must be able to show that consent has been withdrawn for all purposes.

- Make Some Noise is required by law to retain information relating to some activities (e.g. reporting to HMRC, Health and Safety) and in these instances it may not be possible to withdraw consent
- Withdrawal of consent by the data subject covers all processing activities carried out for a specific purpose or purposes, for which that data subject provided consent in the first place
- Withdrawal of consent shall not make unlawful any processing of personal data engaged in by Make Some Noise prior to the withdrawal of consent
- Make Some Noise is responsible for administering the withdrawal of consent on the part of the data subject, under the oversight of the CEO
- Make Some Noise must be able to demonstrate that it has taken reasonable efforts to ensure that the claim of parental responsibility is authentic and true, when consent is withdrawn for a child data subject, including the use of available technology.

Personal Data Breach
In the event of a data breach Make Some Noise may be required to make a report to the relevant bodies and/or the data subject.
All users, including Trustees, staff, freelance contractors, volunteers and temporary employees of Make Some Noise and third parties, and Make Some Noise must be aware of this procedure and are required to follow it should a personal data breach incident occur.

See Appendix 3 for further information about this process.

Personal Data Transfer Outside of the EU
Make Some Noise is required to have additional safeguards in place when it intends to engage in the transfer of personal data to countries or to international organisations outside of the EU for processing. See Appendix 4

Monitoring, reporting and review
The Chief Executive Officer will ensure that Make Some Noise monitors the effectiveness of this policy through the collection and analysis of monitoring data using the tools featured in the following appendices. This data shall provide the basis of scheduled Data Protection reports to the Board of Trustees and subsequent reviews of this policy.

RELEVANT LEGISLATION

- Data Protection Act 1988
- General Data Protection Regulations (GDPR) May 2018
- Privacy and Electronic Communications Regulations (PECR)

FORMS REFERRED TO IN THIS POLICY

- Right to Withdraw Consent/ Right to Withdraw Parental Consent
- Registration Form
- Data Subject Consent Form
- Internal Personal Data Breach Register
- Data Subject Request Form
- Privacy Notice
- Data Protection Impact Assessment (DPIA)
- Disposal Log for Removal Storage Media

LINKED POLICIES

- IT & Internet
- Safeguarding

FURTHER INFORMATION

- Information Commissioner's Office (www.ico.org.uk)
- The Law Society (www.law society.org.uk)
- www.acas.org.uk
- www.gov.uk

Appendix 1

ABRIDGED PRIVACY NOTICE

Our full Privacy Notice, Safeguarding and Data Protection Policies are available online (http://www.make-some-noise.com/make-some-noise-policies/) or by contacting the office.

1 The EU's General Data Protection Regulation ("GDPR") sets out the rights of individuals in relation to their personal data and how this can be processed and requires us to identify a Lawful Basis/Condition for processing your personal data.

We process your personal information as this is necessary to meet our **Legal and Contractual Obligations** (eg safeguarding, health and safety and reporting to the funders and other relevant authorities such as National Foundation for Youth Music, BBC Children in Need, local authorities etc)

2 GDPR classifies certain data as "special category", including Ethnicity, Race and Health which we request, and we are required to have an additional condition to allow us to process "Special Category Data".

We require your **Consent** to retain your special category data. Most of our funding is received to pay for work with a specific demographic (eg Mental/Physical Health, Young Parents, Military families). We must report on our projects and events to our funders (eg National Foundation for Youth Music, BBC Children in Need, local authorities etc).

This funding ensures that our sessions are free to participants or charges are kept as low as possible.

Only statistical information is shared unless we have your consent to use your name for a specific and identified reason

3 We collect data to safeguard all participants, record attendance at workshops and to help us communicate about opportunities and projects

4 Your details will be entered into our databases/filing systems. This data is held securely and can only be accessed by members of the Make Some Noise team for whom it is necessary and relevant for them to do their role. Personal and Special Category Data will be stored in the Substance Views database whose servers are all based in the UK. Google Drive will be used to maintain a session register but only names will be entered, and records will be deleted once inputted on to our database

5 Data will be retained in line with our Data Protection Policy and will be securely destroyed after this time

6 **Your Rights under GDPR**

Under data protection legislation you have the following rights:

- The right to be informed how your personal data is processed
- The right of access to your personal data
- The right to rectification
- The right to erase
- The right to restrict processing
- The right to data portability

- The right to object
- Rights in relation to automated decision making and profiling
- The right to lodge a complaint with a supervisory authority

7 PHOTO, VIDEO AND AUDIO RECORDING

Photos, videos are classed as personal information. Make Some Noise will from time to time photograph/film/record projects– including workshops, performances and/or events/training to use as evidence to report to our funders and in our marketing. If the programme involves accreditation such as AQA Unit Awards Schemes or Arts Award then photos, video and/or audio recordings may be required as part of the qualification.

You will be informed in advance if photography and/or filming is to take place and will be asked to provide your written consent. We will always notify participants that a photographer or film maker will be at a session or event, and by bringing to our attention that you do not want to be photographed or filmed when this happens, we can ensure the photographer or film maker is aware of this at the time.

Photos, Videos and audio recording will be retained for up to 7 years from end of the programme. After this date we will delete copies from our records. You may still find images in circulation, but this is beyond our control.

If you see a photo or a film in the public domain in which you appear where you believe you have requested not to be included please inform us in writing by emailing info@make-some-noise.com with details of the photo/film/ recording, where seen and we will remove it as soon as possible or take measures to edit accordingly where possible.

Appendix 2

RETAINING INFORMATION GUIDANCE

HR RECORD - Staff

Type of Record	**Minimum Retention Period**	**Reason for Length of Period**
Application forms	Successful – duration of employment Unsuccessful – 6 months	Feedback to applicants and time limit on litigation
Interview notes	6 months	Feedback to applicants and time limit on litigation
Safeguarding record (A record of the dates of DBS and/or Update Service Checks and Disclosure numbers only)	25 years	Requirement of Insurers
Personnel Files	6 years from end of employment	Provision of references and potential litigation
Annual Leave records	2 years	Good practice
Appraisal/assessment records	5 years	Good practice
Summary of record of service	10 years from end of service	Provisions of references and requests for confirmation of employment
Records relating to accident or injury at work	3 years after the date of the last record (or if the accident involves a child/young adult, then until that person reaches the age of 21)	• Social Security (Claims and Payments) Regulations 1979; • RIDDOR 1995
Documentation relating to a grievance	2 years	Allows appropriate appeal mechanism and monitoring future grievances
Documentation relating to a disciplinary process	1 year for a verbal warning 1 year for first written warning 2 years for final written warning	In accordance with organisational policy & procedures

HR Records - Freelancer

Type of Record	**Minimum Retention Period**	**Reason for Length of Period**
Safeguarding record (A record of the dates of DBS and/or Update Service Checks and Disclosure numbers only)	25 years	Requirement of Insurers
HR File (including all recruitment documentation, safeguarding checks and contracts	25 years	Safeguarding Practice (consistent with Insurance requirements)
Contract documentation (delivery)	25 years	Safeguarding Policy
Contract documentation (non-delivery)	6 years	

ACCOUNTING / FINANCE / MANAGEMENT RECORDS

Type of Record	Minimum Retention Period	Reason for Length of Period
Accounting Records	6 years	Section 221 of the Companies Act (1989 & 2006 modifications)
Income Tax and NI returns	6 years after end of financial year to which records relate	Income Tax (Employment) Regulations 1993
Wages and Salary records	6 years	Taxes Management Act 1970
Statutory Sick Pay records/calculations	6 years (as Income Tax)	Statutory Sick Pay (General) Regulations 1986
Statutory Maternity Pay records/calculations	6 years (as Income Tax)	Statutory Maternity pay (General) Regulations 1986
Board Papers	6 years	Companies House and Charities Commission guidance

PARTICIPANT / PROGRAMME DOCUMENTATION

Type of Record	**Minimum Retention Period**	**Reason for Length of Period**
Participant Data	7 years from last attendance	Safeguarding Policy
Registers	6 years from date of last session	Good Safeguarding Practice (Self-Imposed)

Photographs	7 years	Safeguarding Policy
Session Reports	6 years from date of last session	Good Safeguarding Practice (Self-Imposed)

Appendix 3

DATA BREACH PROCESS

Procedure – Breach Notification

Data processor to data controller

All personal data breaches by data processors for Make Some Noise must be notified to Make Some Noise CEO immediately. They must record the communication of the breach in the Data Breach Register stating how the notification was made (whether by email, telephone call etc.), to whom and how the confirmation of receipt was provided.

Data controller to supervisory authority

All personal data breaches by Make Some Noise must be notified to the appropriate supervisory authority immediately i.e. the ICO

Make Some Noise is required to carry out an assessment to determine whether the personal data breach is likely to cause a risk to the affected data subject's rights and freedoms under the GDPR.

If a risk is considered likely, Make Some Noise is required to report the personal data breach to the supervisory authority immediately and in any event, no later than 72 hours after the risk assessment. If the notification is made outside of the 72-hour window, Make Some Noise is required to provide reasons for the delay.

Pursuant to Data Breach Register, Make Some Noise is required to provide the following to the supervisory authority:

- A description of the nature of the personal data breach
- The categories of personal data that have been affected by the breach
- The number, which may be approximated if necessary, of data subjects affected by the breach
- The number, which may be approximated if necessary, of personal data records affected by the breach
- The name and contact details of the DPO
- The likely outcomes of the personal data breach
- Any measures taken by Make Some Noise to address and/or mitigate the breach; and
- All other information regarding the data breach.

The DPO must record the communication of the breach in the Internal Personal Data Breach Register, stating how the notification was made (whether by email, telephone call etc.), to whom and how the confirmation of receipt was provided.

Data controller to data subject

If it is likely that there will be a high risk to the affected data subject's rights and freedoms under the GDPR, Make Some Noise is required to provide immediate notification to the relevant data subjects.

The notification to the data subject must be made in clear and plain language and must include the following:

- A description of the nature of the personal data breach
- The categories of personal data that have been affected by the breach
- The number, which may be approximated if necessary, of data subjects affected by the breach
- The number, which may be approximated if necessary, of personal data records affected by the breach
- The name and contact details of the DPO
- The likely outcomes of the personal data breach
- Any measures taken by Make Some Noise to address and/or mitigate the breach; and
- All other information regarding the data breach.

Make Some Noise must use appropriate measures, such as encryption, to ensure that all personal data is secure and cannot be accessed by those without the requisite authority.

Make Some Noise must also take subsequent measures to ensure that the risk to the rights and freedoms of the data subject are no longer an issue.

If notification would require Make Some Noise to implement a disproportionate amount of effort, a public communication or other similar measure may suffice, so long as all data subject are effectively informed.

It is possible that the supervisory authority may require Make Some Noise to communicate the personal data breach to the data subject, should there be an element of high risk involved.

Appendix 4

Personal Data Transfer Outside of the EU

Make Some Noise is required to follow this procedure when it intends to engage in the transfer of personal data to countries or to international organisations outside of the EU for processing, as per the requirements of the GDPR, including the transfer of personal data from a country or an international organisation to another country or another international organisation. Make Some Noise must ensure that all the personal data of natural persons in its control is suitably protected, in line with the GDPR.

Transfer procedure

Make Some Noise as data controller or data processor, shall ensure that adequate protection is provided to the data subject whose personal data is being transferred to countries or to international organisations outside of the EU by ensuring the following:

1) That it has checked the *Official Journal of the European Union* and confirmed that the country of the recipient of the personal data is an approved country, as per the EU list of approved countries. This also applies to industry sectors within particular countries

2) That the country of the recipient of the personal data has adequate data protection systems and controls, whether by statute or self-regulation

3) That it has an agreement in place which the recipient of the personal data, incorporating existing and/or approved data protection clauses, ensuring the data subject is adequately protected

4) That it is transferring the personal data pursuant to approved binding corporate rules

5) That it is applying one of the exemptions set out at in the GDPR and Data Protection Act 2018, namely that:

    a. Explicit consent has been provided by a fully informed data subject, who has been made aware of all possible risks involved considering appropriate safeguards and an adequacy decision

    b. The personal data transfer is a prerequisite to the performance of a pre-existing contract between the data controller and the data subject or when the data subject requests that pre-contractual measures are implemented

    c. The personal data transfer is a prerequisite to the conclusion or performance of a pre-existing contract between the data controller and another person, whether natural or legal, if it is in the interest of the data subject

    d. The personal data transfer is in the public interest

e. The personal data transfer is required for the creation, exercise or defence of legal claims

f. The data subject is not capable of giving consent, whether due to physical or legal limitations or restrictions and the personal data transfer is necessary for the protection of the key interests of the data subject or of other persons, whether natural legal; and

g. The personal data transfer is made from an approved register, confirmed by EU or Member State law as having the intention of providing public information and which is open to consultation by the public or by an individual demonstrating a legitimate interest, but only so far as the legal requirements for consultation are fulfilled; and

h. That it is relying on approved certification mechanisms or codes of conduct alongside binding agreements in the country or international organisation outside of the EU that set out appropriate safeguards for the protection of the rights of personal data subjects.

Appendix 5

Third Party Access to Data

Make Some Noise is responsible for ensuring the security of its data processing facilities and other information assets in relation to third parties. This procedure applies to all situations where third parties require access to any of Make Some Noise's data, including all the following categories of external parties with whom Make Some Noise may have agreements in place:

- Service providers, including managed security service providers
- Clients and customers
- Outsourcing suppliers including: facilities, operations, IT systems, data collection and call centres
- Consultants
- Auditors
- Providers of IT systems and services;
- Providers of cleaning, catering and other outsourced support services; and
- Temporary staff, including placement and other short-term appointments.

Make Some Noise is responsible for assessing associated third-party risks according to the category and level of risk involved.

Responsibilities
Where there is a business requirement to work with third parties, Make Some Noise is required to enter into a formal agreement regarding information security with all third-party service providers.

The CEO and all third-party relationship owners responsible for the aforementioned service categories are required to ensure that formal external party contracts are entered into in line with this procedure. All contracts must implement adequate security controls, delivery levels and service definitions and the CEO and third-party relationship owners are responsible for ensuring that these are properly implemented and maintained by the third party, carrying out risk assessments as and when required by this procedure.

Throughout any transition periods Make Some Noise shall offer the same level of security.

Procedure
Make Some Noise shall only grant third parties access to organisational assets, including personal data and other information, once a risk assessment has been carried out and the appropriate systems and controls are implemented.

Risk assessment - step by step

1. Make Some Noise carries out a risk assessment and identifies all risks pursuant to third party access to data

2. For each third party, the risk assessment shall identify the following:

    - The data and the processing facilities which the third party will have access to
    - The type of access the third party shall have, whether physical and/or logical, whether on or off-site
    - The exact location from which the third party will access the data
    - The value and specific classification of the information which the third party will access
    - The data to which the third party shall not be granted access, and which may need to be secured by additional means
    - A full list of the third party's personnel who will be or are likely to be involved in the access to data, including partners and external contractors
    - How the third party's personnel shall be authenticated
    - How the third party intends to store, process and communicate the data
    - The impact that inaccurate, incorrect or misleading data shared with the third party would have on the third party
    - The impact on the third party of a potential inability to access the data when required
    - How Make Some Noise's Security Incident Management Procedure applies and should be implemented if information security incidents take place, which involve the third party
    - Any legal or regulatory matters regarding the third party that are of note; and
    - How Make Some Noise's stakeholder interests may be affected by any of the decisions made in relation to the third-party relationship.

3. All systems and controls implemented by Make Some Noise pursuant to the risk assessment must be according to the GDPR and must be within the power of Make Some Noise.

4. Make Some Noise and the third party agree to implement appropriate controls and Make Some Noise shall draw up a contract, which the third party is required to sign. Amongst the third party's obligations is the requirement that all its personnel are aware of their obligations pursuant to the contract.

5. When drafting the contract, Make Some Noise are required to consider and include all the following information security matters and insofar as any matters are not included within the contract, must provide a documented reason why they were not included, as well as the requirement under which they were identified as part of the risk assessment:

    - A clear definition and/or description of the service or product provided by the third party and a description of the data and its classification
    - Training, education and awareness requirements for all third-party users
    - Any provisions for the transfer of personnel

- Responsibilities for the installation of software and hardware, as well as maintenance and destruction
- A robust and clearly defined process of reporting, including structural requirements, reporting formats and escalation protocols
- A requirement that the third party adequately resources reporting, monitoring and compliance activities
- A robust and clearly defined change management process
- An Access Control Procedure, refer to Security Access Procedure
- Physical controls, including secure areas
- Controls against malware
- Data security incident management
- Appropriate service and security levels, including what would amount to unacceptable service and security, as well as a clearly defined verifiable criteria of performance and security, monitoring and reporting
- The right for Make Some Noise to monitor and audit the performance of the third party, for which Make Some Noise may use external auditors, including the third party's processes for change management, identifying vulnerabilities and managing information security incidents, as well as Make Some Noise's right to revoke activities
- The requirements of service continuity
- Legal responsibilities and liabilities and how they shall be met
- Copyright and Intellectual Property Rights protection
- Systems and controls in relation to subcontractors; and
- Conditions for renegotiation and termination of agreements and contingency plans.

Information transfer agreements
When the contract between Make Some Noise and a third party is for the transfer of data or software, the following additional controls must be considered, pursuant to an individual risk assessment:

- How the management of both Make Some Noise and of the third party shall be responsible for notifying transmission, dispatch and receipt of data as well as any associated procedures and control
- Systems and procedures for ensuring the traceability and non-repudiation of data
- The means of data transmission
- Packaging of data
- Agreed system of labelling the data
- The selection of couriers and methods of identification
- The management of data security incidents
- Escrow agreements
- Copyright, data protection and software licensing
- Technical requirements for recording or reading data or software; and

- Any other systems and controls such the use of cryptography.

Managing changes to third party services

Make Some Noise may need to agree to variations to contracts with third parties, as a result of the following potential changes:

- The service it currently offers
- The implementation of new systems or applications
- Updates or modifications to its policies and procedures; and
- Updated systems and controls arising from new risk assessments or data security incidents.

A third party may require changes to its contract with Make Some Noise because of the following potential changes:

- New networks and infrastructure
- New technologies, products or new releases of current products
- New physical locations
- New physical services
- New tools or methodologies
- New service providers; and
- New suppliers of hardware or software.

If any changes arise, a new risk assessment and review of the selected controls must be carried out. Any changes to the contract based on the introduction of new controls, or the amendment of existing controls must be agreed with the third party and inserted into the contract via an agreed variation.

The CEO and relationship owners are responsible for ensuring that the new controls are implemented and incorporated into review and monitoring arrangements already in place.