Data Protection / Privacy Policy – May 2018

Policy information	
Organisation	Rea Sound (NI) Ltd / Rea Sound (Pro Audio) Ltd / Rea Sound Partnership
Scope of policy	This policy covers the offices / warehouses of the above-named companies across Northern Ireland and Ireland.
Policy operational date	This policy is adopted May 2018
Policy prepared by	Roger McMullan - Advisor
Date approved by Board/ Management Committee	The Directors / Partners have read and approved this policy
Policy review date	April 2021

Introduction	
Purpose of policy	This document is written to comply with the GDPR (EU General Data Protection Regulation) coming into force on 25th May 2018. This document sets out clearly our commitment to follow good practice, to enable protection of data held on clients, staff and other individuals (potential clients). This document helps to protect all involved within the organisation going forward.
Types of data & Why we process data	We hold on our accounting systems the following information: • Name • Addresses • Delivery Addresses • Contact Telephones • Contact Mobiles • Contact Emails This information is part of our contract with the individual to provide financial records, as we are legally obliged to do. For payment by credit cards we process your details, we do not keep your card details, if written down these are immediately shredded / permanently destroyed. Our representatives, who visit and or meet with potential clients will also take record of the following information for the purposes of providing quotations and additional information required by the client. This information may be written in a diary / notebook and will only ever contain: Name Address Contact Telephones Contact Mobiles Contact Emails General Requirements Referrals from online companies maybe passed to us, as per your request. We hold the data you have submitted. For Marketing purposes, we have a separate database for the use of marketing contact. This database is only accessible by Directors or senior members / representatives of the companies. We will also seek your permission before you are added to this database. Employees – we hold: Name Address Contact Telephone Date of Birth Bank Account Details NI Number Email address (if provided) Information provided by HMRC / Pension provider • *Please see separate data statement*

Policy statement	Our Group of Companies are committed to complying with both the law and good practice in protecting and respecting your privacy. When you purchase from us we need to hold the above-mentioned information in order that we can process your transaction. We respect individuals' rights and only hold data that is shown above on our accounting software. Hard copies of printed invoices, statements or financial reports may be printed for the use of staff / directors of the company. All emails, correspondence and communications to and from the company can be accessed by senior management and directors. Names and telephone numbers are taken down within a notebook / diary for message purposes and passed on. The original record of the call is kept for reference. CCTV – across our sites we operate a CCTV system for the purposes of security, health and safety and monitoring purposes. External suppliers – Access from time to time may be required from our external suppliers for maintenance purposes. The supplier will only have access to a limited part of the computer systems and all personal data will not be made or allowed access to. Passwords – All computer equipment which has access to data may have is passworded. These passwords are to be changed regularly. Payments - For payment by credit cards we process your details, we do not keep your card details, if written down these are immediately shredded / permanently destroyed. The merchant copy is maintained for financial / accounting records in a lockable drawer. These are kept for a period of 6 months following your transaction then permanently stored in line with accounting requirements. In the event of a data processing error we will notify the Information Commissioner voluntarily, even if this is not required.
Key risks	When processing data we aim to do so securely, efficiently and minimise any risk involved. All data is processed in a separate area, with computer screens and desk not readily available to being overlooked. The area is a restricted area. When we make client visits, our representatives do gather information as listed above to enable them to provide the information they request. This information can be gathered in two ways, directly onto our Accounting program by way of Iphone / Ipad App or manually in a note book / Diary. We do not use loose paper to make notes. These books are then securely stored for a maximum of 5 years.

Responsibilities	
The Board / Company Directors	They have overall responsibility for ensuring that the organisation complies with its legal obligations.
Employees & Volunteers	All staff and volunteers have read, understand and accept these policies and procedures that relate to the personal data they may handle in the course of their work. (From now on, where 'employees' is used, this includes both paid employees, representatives and volunteers.)
Enforcement	Our key staff have received one on one training to help cover the processing of the data they need.

Continuity / Risks	
Business continuity	We use a cloud-based accounting / CRM system, which allows for safe and secure off site data holding. This enables safe continuity if required going forward.
Specific risks	Our key employees can meet with you in your chosen location and your data can be accessed there, subject to mobile internet access. They can also work on your data remotely at home, at any of our offices or locations with internet access. Every effort will be made to do this privately and they will never make available in public spaces. Each user has a dedicated login which is logged each and every time something is undertaken or the system is logged in or out of. Our employees will not provide your information over the telephone. Emailed invoices / statement / quotations and financial reports will be made available by email to you. We can send these to you as required.

Data recording and storage	
Accuracy	We obtain our data directly from our clients / potential clients. Where contact details are requested from you we will usually ask you to check we have it right. If it is not, we will amend within 8 working hours of notice.
Updating / Retention	We need to keep data and information in line with legal requirements. We retain data on the following basis: Employee Records – 6 years after date of termination Pension Records – 6 years after date of termination Photos / Videos – indefinitely CCTV – each machine is on a 30-45 day loop. Downloaded material required as part of an investigation will be kept for a period of up to 3 years after the incident Insurance Records – indefinitely Safeguarding matters – indefinitely or until advised by authorised authority Accident books - 3 years from the date of the last entry (or, if the accident involves a child/ young adult, then until that person reaches the age of 21) Customer Records – reviewed every 3 years Marketing Records – reviewed every 3 years Access Request Letters – Held for a maximum of 1 year following completion of request Sales leads - indefinitely
Storage	We aim to hold all information digitally, in our Accounts and CRM software including MS Outlook. Employee data is held on MS One drive and online payroll software with limited access by only those who require it. Pension information is also held online and limited access is given
Retention periods	Please see above
Archiving	In the event we have printed personal information, this will be stored only for a limited time until the purpose of this print has been addressed and completed. Once completed the printed material is then destroyed securely.

Right of Access	
Responsibility	Should you require access to the information we hold please make contact as stated below.
Procedure for making request	Right of access requests must be in writing. This should be addressed to the Managing Director and provide the following: - Your Name Your Address Your Contact Number Your Email address Your request We suggest that your letter is sent by recorded delivery if by post. Post address: Rea Sound – 57 Drum Road, Cookstown, BT80 8QS Email address: accounts@reasound.com
Provision for verifying identity	Where the person managing the access procedure does not know the individual personally we will make contact with you to verify you to the best of our ability.
Charging	We hold very limited data on you, this is detailed above. We may charge £10 to process and supply your data as requested.
Procedure for granting access	If the request is made electronically, we wil provide the information in a commonly used electronic format. If your request is in writing please confirm in what way you would like your information to be provided back to you.

Transparency	
Commitment	Our goal is to explain the type and how we use your data. This core document provides this information to you and includes • for what purpose it is being processed • what types of disclosure are likely, and • how to exercise their rights in relation to the data
Procedure	We aim to cover this as below: New Clients – Briefly covered by our representatives during the initial meeting Current Clients – Data Protection Policy made available to all openly – Link on website, mentioned on the email footers Employees – Verbally during training and conformation by letter.
Responsibility	Our key employees form part of this transparency and responsibility lies with the Directors to maintain and review in line with this policy

Lawful Basis	
Opting out	For employees, clients and potential clients we only hold information which is required to complete our contracts with you and do so as required by law. For Marketing purposes you can opt out at any time from our online database. Every email we send will allow you to easily and quickly opt out.
Withdrawing consent	We acknowledge that, once given, consent can be withdrawn, but not retrospectively. There may be occasions where the organisation has no choice but to retain data for a certain length of time, even though consent for using it has been withdrawn

Employee training & Acceptance of responsibilities	
Induction	All employees who have access to any kind of personal data should have had their responsibilities outlined during their induction procedures
Continuing training	There are opportunities to raise Data Protection issues during employee training, team meetings, supervisions, etc. this is encouraged.
Procedure for staff signifying acceptance of policy	Each staff member has signed for a copy of this document and our Data Privacy Statement, acknowledging receipt and understanding.

Policy review	
Responsibility	The Directors and senior team members will review this policy as stated.
Procedure	A complete review of the policy is undertaken during the period specified, consulting and change in the law, systems, stake holders and good practice.
Timing	The review will start in April 2021 and be completed by May 2021.