eStage.

GDPR compliance.

v2 - 9th april 2020

introduction.

eStage Group Ltd (eStage) collects personal data across the business to assist in its efficient day to day running. This document covers the polices that eStage has in place to ensure it is processing this data responsibly and in compliance with the GDPR.

contents.

what is GDPR?

GDPR aims to give people greater control over their personal data and to simplify the regulatory environment for international businesses. It replaced the 1995 Data Protection Directive (Directive 95/46/EC).

It applies when any data is received from customers that are located within Europe. Unlike a directive, it does not require national governments to pass any enabling legislation and so it is directly binding and applicable to businesses all over the world.

protected data.

The data that is protected under GDPR is data concerning individuals (not companies). *Personal Data* extends to any information pertaining to an individual, whether it relates to their private, professional or public life. It can be anything from a name, to a home address, photo, email address, bank account details, posts on social networking websites, medical information, a computer's IP address and more.

data we collect.

eStage collects personal data from customers and the freelancers we work with, this varies between business areas.

In production we collect personal data specifically on the freelancers and clients we work with, which is held in a central database, and also to process payment invoices and for contracting.

eStage Digital collects data from Cookies & Data Sent from Browsers/Devices and Data provided by the customer when ordering services or entering into a contract, therefore, several new features and functionalities have been introduced into eStage Digital's Systems that are designed to assist with compliance.

lawful basis.

Data can be processed under a number of lawful basis under GDPR. Below we outline the data we hold under each of these.

legal obligations.

Invoicing and payments: eStage holds the personal information of clients, suppliers, and customers for invoicing purposes on FreeAgent. We also process payments through Stripe and GoCardless. As we are obligated to produce taxation reporting and keep financial records we need to keep this data to allow us to fulfil these obligations.

legitimate interests.

ePM: eStage manages a custom built database on Ninox called ePM, this is used by our freelancers to help make production management easier. On this database it stores contact information for a number of freelancers, staff from venues and production companies in the industry who we have worked with, and suppliers. We hold this information beyond the run of the production that relates to them. This data is held beyond our contractual obligations, so we can contact these freelancers in the future regarding new work. For production companies and venues it is held to save double data entry. We may on occasion pass the data to other clients strictly for the purposes of providing additional work to these data subject. To meet the standards required for this justification eStage notes that:

- **For freelance individuals:**
    - **Purpose of holding the data:** This data is held as it allows eStage to contact individuals with new work opportunities they would not otherwise have access to. Freelancers would expect data to be held for this purpose.
    - **Necessity for holding data**: Without this data eStage would not be able to offer these opportunities. The data held is limited to name, email address, and phone number. Additional data is held on roles undertaken and projects they have worked on with us, which is not considered personal information.
    - **Balancing test:** eStage would not be able to contact these individuals without holding this data, and offer them new work. This new work will benefit the individual financially and the amount of data held is limited to that which is strictly necessary to undertake this function.
- **For production company and venue staff:**
    - **Purpose of holding the data:** This data is held as it allows eStage to build a contact database of staff at venues or production companies, this can be shared between our freelance production managers to ensure they can contact the best people. It also allows us to have on-going discussions with our client base about our services where it is relevant to them, such as providing advice in extreme situations, sharing knowledge on where we can help them deliver productions more efficiently.
    - **Necessity for holding data**: Without this data eStage would not be able to manage it's client database effectively and efficiently, as without holding it then the data would need to be re-entered on every contract signing and could remain incomplete. The data held is limited to name, company email address, and company phone number.
    - **Balancing test:** Much of this data is available publicly on venue or company websites and communications are strictly limited, communications that use this data are

exclusively to save both eStage and the Venue or Production company time or cost. It is expected in this business that we would retain this data on file for this purpose.

- **For supplier staff:**
    - **Purpose of holding the data:** This data is held as it allows eStage to build a contact database of staff at suppliers across the industry, this can be shared between our freelance production managers to ensure they can contact the best people in each business.
    - **Necessity for holding data**: Without this data eStage would not be able to manage it's supplier database effectively and efficiently, as without holding it then the data would need to be re-entered on every supply agreement signing, and new supplier contacts would need to be sourced for each production. The data held is limited to name, company email address, and company phone number.
    - **Balancing test:** Much of this data is available publicly on supplier websites and communications are purely to discuss the further supply of goods from the supplier, benefiting them financially. It is expected in the industry that we would retain this data on file for this purpose.

contracts.

ePM: eStage holds personal data for those working on its productions on ePM, including freelancers, venues and production company staff, and suppliers, for the period of time that they are contracted to provide production management services to the production as they are required to contact those people throughout that period.

Digital services: In most cases, users register an account or have one registered as part of the process of submitting an order for services. In doing so, end users are entering a contract with us and our Service Providers for us and the Service Providers to provide services. In a scenario such as this it may mean asking users for consent is not required, however we will often have a GDPR Acceptance section within the order form which requires the customer to acknowledge and henceforth consent that we collect and process their personal data.

consent.

For all of these the terms of each are outlined in our **privacy policy** on our website.

Email marketing: These give the individual flexibility and control over how our users opt into marketing emails which can be used for newsletters and similar products. Users are asked to confirm and agree to our privacy policy when signing up.

Production Freelancer sign up form: We ask freelancers to provide us their information even if we haven't worked with them using our freelancer sign up form. This data is voluntarily given for the use to contact them about future work opportunities and stored on our database for that purpose.

Digital services: When providing any digital services, a positive opt-in is given separate to other terms and conditions, and we do not bundle several uses under one consent. We specify clearly how we intend to use the data in our privacy policy and obtain the consent for each specific use when we attempt to obtain such consent. We also have simple ways for people to withdraw consent. WHMCS

has a consent log that records each time the consent setting is changed. For each change, WHMCS will record the date/time of that change, who it was initiated by and the IP address of the user.

Digital Analytics: Cookies and usage data is collected on our website for various forms of analytics and spam protection, this allows us to understand how people are moving around our website and how they are accessing us. This is only collected if the data holder agrees to our privacy policy on the handling of this data.

individual rights and how we comply.

For anyone we hold data on eStage provides a single email address for contacting us on data enquiries, **data@eStage.net**. Any enquiry across the business will be managed through this email address.

We will consider each such request in accordance with all applicable data protection laws and regulations. No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature. It should be noted that situations may arise where providing the information requested by a data subject would disclose personal data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that person's rights.

the right to be informed.

The right to be informed covers some of the key transparency requirements of GDPR. It is about providing individuals with clear and concise information about what you do with their personal data. This document and our **privacy policy** are the first steps in this.

All emails from eStage accounts contain links to inform clients and customers of our privacy policy and how we handle their data.

For digital services, customers are required to agree to our Terms of Service in order to register an account and complete checkout. A user account cannot be created, and an order cannot be placed, without the user checking a box to confirm their agreement to our Terms of Service. That Terms of Service also includes a link to our Privacy Policy and any other important terms and service agreements that are necessary to complete an all-inclusive agreement.

Such policies are also available on all pages of the eStage website in the footer menu area, in relevant emails sent to customers and available to access directly with a link.

the right of access/right to rectification.

For the wider business we can be contacted by anyone to access and modify the data we hold on them through **data@eStage.net**.

For digital services we provide a self-service client portal that gives our customers access to login and view their personal information (profile data). The client portals also provide our customers with access to update their personal information including name, email address, postal address and phone number and most other data collected that is not required for historical/legal/systematic reasons (e.g. when an order was placed, or when acceptance was given for agreements). We do not charge an administration fee for this service.

the right to erasure ('right to be forgotten').

If we receive a request for erasure, we can perform a deletion of the records from our individual systems using built-in functionality. Using this feature removes all data relating to a given customer

including, but not limited to, personal information in the user's profile, service and invoice history, activity log entries, support ticket and email history.

For Digital, we automate the enforcement of any data retention policies we have using WHMCS that allows us to define a period of time for which client records should be kept. We will a perform a right to erasure for any customer records that aren't required to complete a contract/agreement.

the right to data portability.

Data portability means the right to receive personal data in a machine-readable format and to request for such data to be transferred directly from one controller to another. This will be offered for all services when any individual gets in contact with us. WHMCS allows us to generate a customizable export of data relating to a given client. This allows us to generate an export in JSON format containing the data entity types from a list of options.

the right to restrict processing.

The user may ask us to restrict processing by making a written request to us. In addition we ask website users to opt in to processing done from cookies and usage data.

the right to object.

Objections should be sent in a written request to us. We have provided full information about how we process data in this document, and our privacy policy.

rights in relation to automated decision making and profiling.

No personal data eStage processes is not used for profiling or automated decision making.

governance.

data controller.

The assigned Data Controller for eStage is **Ian Taylor (ian.taylor@estage.net)**.

The Data Controller's responsibilities include:

- Being accountable for Lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation and integrity and confidentiality of data.
- Ensuring Lawful Processing of Data.
- Making reasonable efforts to verify parental consent (concerning children aged 13-16) where necessary.
- Stopping unlawful processing of data collected
- Implementing suitable measures to safeguard the data subject's rights and freedoms and legitimate interests where automated decision making is necessary for the performance of a contract
- Implementing appropriate technical and organisational measures and demonstrate compliance (such as pseudonymisation/encryption, maintaining confidentiality, restoration of access following technical incidents and regular testing of measures)
- Implementing data protection policies as appropriate
- Co-operating with Supervisory Authorities
- Ensuring any natural person acting under their authority does not process data except on the controller's instructions
- Informing supervisory bodies within 72hrs of becoming aware of any personal data breach, its effects and remedial action taken
- Communicating personal data breach to data subjects without undue delay where breach is likely to result in a high risk to the rights/freedoms of persons
- Completing a DPIA (Data Protection Impact Assessment) before carrying out potentially high risk processing.
- Consulting supervisory authorities prior to processing data that a DPIA has indicated high risk in the absence of measures taken by the controller to mitigate the risk and provide the authority with the information specified in Article 36(3) of the DPA/GDPR.

data protection officer.

eStage notes that whilst it is not required to appoint a Data Protection Office, it has appointed one to act as a single contact within the business and to provide advice and support to those employed on all data protection matters. The Data Protection Officer for eStage is **Dan Gosselin** (**dan.gosselin@estage.net**).

The data protection officer is responsible for:

- Informing and advising eStage, its employees, and freelancers, who carry out processing pursuant to data protection regulations, national law or European Union based data protection provisions;
- Ensuring the alignment of this policy with data protection regulations, national law or European Union based data protection provisions;

- Providing data subject with their personal data in a structured, commonly used, machine-readable format where processing is carried out by automated means upon request;
- Providing a copy of personal data undergoing processing on request by the data subject;
- Erasing personal data that isn't required without undue delay either when a data subject requests so or where obligatory or to cancel a contract in order to complete such an action upon the data subject's approval;
- Ensuring data is no longer processed once consent is removed;
- Communicating any rectification or erasure of personal data and any restriction of processing to each recipient that personal data has been sent to;
- Ensuring communications regarding data are concise, transparent, intelligible and easily accessible;
- Providing guidance with regards to carrying out Data Protection Impact Assessments (DPIAs);
- Acting as a point of contact for and cooperating with Data Protection Authorities (DPAs);
- Determining the need for notifications to one or more DPAs as a result of eStages current or intended personal data processing activities;
- Making and keeping current notifications to one or more DPAs as a result of eStages's current or intended personal data processing activities;
- Informing senior managers, officers, and directors of eStage of any potential corporate, civil and criminal penalties which may be levied against ADP Call Centres Limited and/or its employees for violation of applicable data protection laws.

data protection by design.

To ensure that all data protection requirements are identified and addressed when designing new systems or processes or when reviewing or expanding existing systems or processes, each of them must go through an approval process before continuing. This process should be conducted by the Data Protection Officer.

When required, eStage staff must ensure that a Data Protection Impact Assessment (DPIA) is conducted, in cooperation with the Data Protection Officer, for all new and/or revised systems or processes for which it has responsibility. The subsequent findings of the DPIA must then be submitted to the Managing Director for review and approval.

compliance monitoring.

eStage will review its data protection policies for compliance on a yearly basis and will ensure any new system involving personal data is compliant from the outset.

data protection.

eStage will adopt physical, technical, and organisational measures to ensure the security of personal data. This includes the prevention of loss or damage, unauthorised alteration, access or processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment. A summary of the personal data related security measures is provided below:

- Prevent unauthorised persons from gaining access to data processing systems in which personal data are processed.
- Prevent persons entitled to use a data processing system from accessing personal data beyond their needs and authorisations.
- Ensure that personal data in the course of electronic transmission during transport cannot be read, copied, modified or removed without authorisation.
- Ensure that access logs are in place to establish whether, and by whom, the personal data was entered into, modified on or removed from a data processing system.
- Ensure that in the case where processing is carried out by a Data Processor, the data can be processed only in accordance with the instructions of the Data Controller.
- Ensure that personal data is protected against undesired destruction or loss.
- Ensure that personal data collected for different purposes can and is processed separately.
- Ensure that personal data is not kept longer than necessary

children's data.

Children under the age of 14 are unable to consent to the processing of personal data for information society services (any service normally provided for payment, by electronic means and at the individual request of a recipient of services). Consent must be sought from the person who holds parental responsibility over the child. However, it should be noted that where processing is lawful under other grounds, consent need not be obtained from the child or the holder of parental responsibility.

transfers of data outside of the EU.

Individuals are entitled to learn about the legal basis of Data transfers to a country outside the European Union or to any international organization governed by public international law or set up by two or more countries, such as the UN, and about the security measures taken by the Owner to safeguard their Data. These are outlined below, and more specifically in our privacy policy.

In order to ensure the delivery of emails to customers, we use the Amazon Web Service Simple email Service to send emails from our support & billing system. Such emails are sent via SMTP and are encrypted using TLS but nevertheless, data is still transferred outside of the EU in this instance; the server endpoint is based in North Virginia, USA.

In order to ensure the upkeep of our online services, we split some of them over different servers and locations across the world. As mentioned above, some product-related emails are sent out via Amazon's Simple Email Service from North Virginia. In addition to the e-mail services provided by Amazon, we also use an e-mail service with servers based in Texas and Bulgaria for all of our staff

email accounts where data may be sent from time to time if it is sent in an -e-mail directly from a staff e-mail account.

Personal data collected via our website for the Billing and Support area is saved on servers which are based in the UK only, but may be backed up externally (though securely) by our Service Providers.

If we take card payments over the internet via the WHMCS Client Portal, the payment will be processed via Stripe who have servers across the world. Since we do not save the customers full card details, Stripe keeps a log of all of the customers details for future convenience. Such data may be stored outside of the EU since but can be removed upon request to either party. More information regarding what data Stripe saves is available further down this document.

required data.

As already outlined in this document, we require some personal data in order to complete services, agreements or contracts. You are entitled to fulfil your right to erasure, but we are also entitled to keep certain data providing that it is kept within the boundaries set by the GDPR and the DPA 2018. If you do not provide certain data upon the creation/start of such services/agreements, the agreement may be lawfully terminated at any time by either party.

personal data held.

- **WHMCS**: WHMCS is our Billing & Support system for our Website Design Projects, Hosting & Domains.
    - Profile:
        - User ID
        - Unique User ID
        - First Name
        - Last Name
        - E-Mail Address
        - Full Address (Line 1 & 2, City, State, Postcode, Country)
        - Phone Number
        - Credit
        - Account Creation Date
        - Credit Card Details (Customer ID, Type & Last 4 Digits)
        - Last Login Date, Hostname & IP Address
    - Contacts
        - We keep data on any additional contacts/user accounts that are linked on your account. Such details include their address, contact information and access level to your account.
    - Services
        - Initial Order Number
        - Domain Names Linked
        - Username
        - Subscription/Promotion ID's
        - Suspension Reasons
        - Dedicated IP's and Assigned IP's
        - Nameservers
        - Storage Space Usage
        - Bandwidth Usage & Limits
        - Administrative/System Settings
            - Things like Suspension Overrides, Product & User Links, Creation Dates so that our system can work correctly.
    - Domain Names
        - Registration Date
        - Domain Name
        - Subscription/Promotion ID
        - Administrative/System Settings
            - Things like when payment reminders should occur, grace periods and fees and additional pricing information so that our system can work correctly.
    - Invoices
        - Invoice Number
        - Transaction ID's
        - Administrative/System Settings

            - Affiliation/Links between User, Products and Invoice Line Items so that our system can work properly.
    - Support Tickets
        - Ticket ID
        - Ticket Number
        - CC E-Mail Addresses
        - Security Number
        - Message
        - Replies
    - E-Mails
        - E-Mail ID
        - User ID
        - Message
        - To, CC, BCC
    - Activity Log
        - Entry Number
        - Date
        - Action Description
        - User
        - IP Address
- **eStage email marketing (Sendy)**
    - Email
    - Name
- **Google Analytics**
    - We use Google Analytics on our website to track the user flow of the website and demographics of users. Information regarding this is available in our Privacy Policy.
- **Stripe Payment Gateway**
    - Customer Creation Date & Time
    - Customer Name
    - Customer ID
    - E-Mail Address
    - Metadata
    - Card ID, Card Number, Card Fingerprint, Card Expiry Date, Card Type, Billing Address, CVC Check Status, Origin
    - Bank Accounts
    - Payment History, Transaction ID's, Payment Date & Time
    - Active Subscriptions
    - API Logs
    - Events
- **FreeAgent**
    - Client Name
    - Client Email
    - Client Address
    - Client Phone
- **ePM (Ninox)**
    - Freelancer/Staff Name
    - Freelancer/Staff Email
    - Freelancer/Staff Phone

additional policies.

Additional Policies that are directly and indirectly part of our overall GDPR compliance can be found at:

- TUCOWS Domain Name Agreement
  - domain name agreement
  - Contains 3 Acceptance Boxes for each Point of Consent

- Order Terms of Service & Acceptable Use Policy
  - website & digital terms
  - Also incorporates Privacy Policy, Exhibit A, OpenSRS UK Domain Policies and Nominet Regulations

- Privacy Policy
  - https://www.iubenda.com/privacy-policy/8106110/full-legal
  - Can also be found in the footer area of the website.

- Customer E-Mail Marketing System Policies
  - https://www.campaignmonitor.com/policies/

- Information Commissioner's Office Entry
  - https://ico.org.uk/ESDWebPages/Entry/ZA313531

enquiries and complaints.

Any enquiries relating to the data that we collect, or if you would like to submit a lawful request to us, you can do so by emailing data@estage.net or calling +44 (0) 207 1128 903. There is also at least one relevant support/contact medium in all of our client portals that you can contact us by if you have access to them.

If you have any concerns that you do not want to discuss with eStage, or our DPO or DC, you can complain to a supervisory authority.