Introduction

As part of our everyday business activity Headers and Volleys Entertainment (H&VE) processes large amounts of personal data.

In doing this H&VE respects the privacy of our viewers, customers, contractors, talent and colleagues and seeks to protect their personal data , by complying with the applicable laws and regulations and fully cooperating with the relevant regulatory authorities.

This policy sets out how H&VE collects, stores, analyses, uses or does absolutely anything else with personal data. It is supplemented by (and should be read alongside) the more detailed processes and policies listed at the end of this document.

Why are you reading this policy?

Compliance with the applicable privacy and data protection laws and regulations is mandatory for everyone. Failure to do so may subject us to civil and/or criminal liability and may result in disciplinary action, including dismissal. We are all responsible for the personal data we process, so we must
make sure we can demonstrate compliance (including by maintaining adequate and up-to-date documentation).

The General Data Protection Regulation (GDPR) applies to the processing of personal data of individuals, replacing many local or national laws. Global data protection and data privacy laws, including the GDPR, take a stringent position regarding how businesses like ours handle and process data. GDPR protects the rights and freedoms of living individuals (data subjects) in relation to their personal data. It imposes obligations, restrictions and controls over the way organizations collect, process, transfer and store this information.

What is personal data?

Personal data is very broadly defined and includes any offline or online data that makes a person identifiable. It does not have to be particularly "personal" or "private" in nature and includes information, facts or opinions about living individuals by reference to:

- an identifier such as name, identification number, location data, online identifier (e.g. IP address); OR
- one of more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

How do we handle sensitive personal data?

Additional restrictions apply to the processing of special categories of sensitive personal data such as:

- racial or ethnic origin;
- political opinions;

- religious or philosophical beliefs, or trade union membership;
- data concerning health or a person's sex life or sexual orientation;
- genetic / biometric data for the purpose of uniquely identifying a person;
- data relating to criminal convictions and offences.

We must take particular care in the processing of personal data in these special categories as the law requires us to take further steps to safeguard this sensitive and special category information.

It is H&VE's policy that personal data must be:

- Collected and processed in a lawful, fair and transparent manner;
- collected for a specified, explicit and legitimate purpose;
- minimised (to limit use of personal data to what is adequate and relevant, in relation to the specified purpose);
- accurate and where necessary kept up to date;
- kept no longer than is necessary to fulfil the specified purpose.
  and
- kept secure - by using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and accidental loss, destruction or damage.

If you need more information, guidance or have any questions please contact info@have.team

Collecting and Processing Data

When collecting personal data from an individual, we must ensure there is a lawful basis and provide that person with transparent information about the processing of their data (this is usually done via a privacy notice).

Where the lawful processing is based on consent from the individual, this must be freely given, unambiguous, separate from other matters using clear and plain language. It should be as easy to withdraw consent as to give it. Where the data subject is a child below the age of consent in the relevant country, processing is only lawful with parental consent. Please note that although GDPR requires parental consent where the child is below 16 years old, it allows national law to lower this as long as it is not below 13 years - for guidance, please check with your Privacy Champion.

There are strict conditions around processing the special categories of sensitive personal data and that relating to criminal convictions and offences (see above).

Please complete a Data Protection Impact Assessment where necessary (see below).

International Data Transfers

When transferring data outside the European Economic Area (EEA) or the UK (after it has left the EU), we must ensure that prior to the transfer:

- the individual has been informed about this and has explicitly consented to it; Or
- the transfer is to a country or territory which has been assessed by the European Commission (or equivalent UK body) as having adequate protection for data in place, as exists within the EEA.

If you are contemplating any other data transfers, you must contact info@have.team prior to the transfer to ensure that appropriate safeguards are in place.

Transferring Data to Third Parties

When transferring personal data to, or outsourcing processing activities to a third party, please make sure that:

- the third party will handle the data in compliance with the relevant legislation and regulations,
- the processing is governed by a contract or legal processing agreement.

In addition, H&VE's *Third Party Security Policy* must be followed which includes the third party completing the H&VE cyber security assessment. Please contact info@have.team for guidance.

Requests from individuals

In addition to the information that must be provided to individuals before processing, data subjects have numerous other rights over their personal data, such as:

- Right of access (also called a 'Subject Access Request')
- Right to rectification
- Right to request erasure (also known as 'right to be forgotten')
- Right to restriction of processing
- Right to be notified and informed
- Right to data portability
- Right to object
- Right against automated decision making (including profiling)
- Right to complain to the relevant supervisory authority (e.g. the Information Commissioner's Office in the UK).

Each business area is responsible for handling these requests by following the relevant process. An important part of each process is to log the request centrally on our compliance portal so that its progress can be monitored and all communication with the data subject

recorded. For further guidance please contact your *Data Protection Manager.*

Records of Processing / Retention

Each business area is responsible for maintaining an up-to-date inventory of all the personal data it processes. It is H&VE's group policy that these records are held centrally in our compliance portal.

We must not process more personal data than we need to. Our policy is to delete or anonymise personal data when no longer needed.

While records containing personal data are retained in accordance with our *Record Retention Policy*, we must all regularly review and delete personal data which is no longer required.

Data Protection by design and by default

When a new process or system involving the processing of personal data is designed, there must be by default, technical and organisational measures implemented to process personal data to comply with the data protection principles and protect the rights and freedoms of data subjects.

Data Protection Impact Assessment (DPIA)

Where processing is likely to result in high risk to the privacy of data subjects, a DPIA must be completed prior to commencement of the processing. This includes new system implementation or changes to existing data processing. Please contact your Privacy Champion/DPO and consult the *Guidelines on Data Protection Impact Assessment*.

Data Breaches

Personal data breaches can result in a risk to the rights and freedoms of the individuals, as well reputational damage for the H&VE brand and substantial fines based on our global revenue. If you become aware of a personal data breach, you must immediately inform your line manager.