Data Protection Policy

12/03/2020
Version 0.1
Draft

HybridTheory

Contents

Change History

Version	Status	Issue Date	Author	Comments
V0.1	Draft	12/03/2020	Kaveh Cope-Lahooti	Draft

Document Controls

Reviewer	Role	Responsibility	Date

01. Introduction

Hybrid Theory is committed to conducting its business in accordance with all applicable Data Protection laws and regulations and in line with the highest standards of ethical conduct.

This policy details expected behaviours of Hybrid Theory 's Employees and Data Processors in relation to the collection, use, retention, transfer, disclosure and destruction of any Personal Data belonging to a Hybrid Theory customers, staff and other relevant Data Subjects and irrespective of the media used to store the information.

An organisation that handles personal data and makes decisions about its use is known under the GDPR as a Data Controller. Hybrid Theory, as a Data Controller, is responsible for ensuring compliance with the Data Protection requirements outlined in this policy. Typically, this will involve online identifiers that we process in relation to online advertising services we provide, in addition to data about our clients' and suppliers' staff, our own employees and other people the organisation has a relationship with or may need to contact.

Non-compliance with this policy, and wider data protection law, may expose Hybrid Theory to complaints, regulatory action, fines and/or reputational damage. This policy helps to protect Hybrid Theory from some very real data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.
- Reputational damage. For instance, the company could suffer if hackers success fully gained access to sensitive data.

Any breach of this policy will be taken seriously and may result in disciplinary action or business sanction.

02. Scope

1.1
This policy applies to all Hybrid Theory's employees in the EU, UK, USA and globally. The GDPR applies to all of Hybrid Theory's operations that involve collecting Personal Data from the EU or of EU citizens, and the UK implementation of the GDPR, achieved through the Data Protection Act 2018, brings into law the provisions of the GDPR and applies to all of our operations in the UK. The CCPA applies to all of our operations that target or collect the personal data of California residents. However, the CCPA will not apply with respect to employees' rights until 1st January 2021. Additionally, where other legislation applies, such as in Singapore, Hong Kong and Australia, this policy should also be followed as a baseline standard.

1.2
This policy applies to Hybrid Theory employees and contractors, suppliers and other Data Processors acting on behalf of Hybrid Theory where a Data Subject's personal data is processed. Employees should only have access to Hybrid Theory Personal Data during the course of, and for the performance of, their employment duties. This policy shall apply:

1.2.1
In the context of the business activities of Hybrid Theory, which includes business between Hybrid Theory and its suppliers;

1.2.2
For employment purposes, and;

1.2.3
Both in relation to services provided to clients and for its own purposes, where Hybrid Theory is involved in online behavioural monitoring and/or advertising.

1.3
This policy has been designed to establish a baseline standard for the processing and protection of personal data by all Hybrid Theory employees. Where national law imposes a requirement that is stricter than, that imposed by, or otherwise not addressed by, this policy, the requirements in national law must be followed.

1.4
This policy applies where Personal Data is processed by Hybrid Theory. Under Article 4(1) of the GDPR, Personal Data means any information relating to an identified or identifiable natural person ("Data Subject"); an identifiable person is one who can be identified, directly or indirectly. Similarly, the CCPA applies to information that is means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.

1.5
Both definitions include reference to an identifier such as a name, identification number, location, online identifier or to one or more factors specific to the physical, physiological, genetic, biometric, mental, economic, cultural or social identity of that natural person.

1.6
Under both laws, unique identifiers that "enable Data Subjects to be 'singled out' for the purpose of tracking online website user behaviour while browsing on different websites" are Personal Data. In certain circumstances, IP addresses, Cookie IDs and mobile device IDs may also be classed as personal data.

1.7
Additionally, any information linked to these IDs is likely to come within the scope of the GDPR and the CCPA. This included Inferred Data, i.e. whereby we assign characteristics such as related to a Data Subject (such as a website user's), gender, lifestyle or interests that we ascribe to them by nature of their viewing history.

1.8
The DPO is responsible for overseeing this Privacy Standard and, as applicable, developing Related Policies and Privacy Guidelines. The DPO is within our company is Gemserv Ltd., who can be contacted at privacy@hybridtheory.com.

1.9
Please contact the DPO with any questions about the operation of this policy, the GDPR or the CCPA or if you have any concerns that this Privacy Standard is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances:

1.9.1
if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by the Company);

1.9.2
if you need to rely on Consent and/or need to capture Explicit Consent

1.9.3
if you need to draft Privacy Notices or Fair Processing Notices;

1.9.4
if you are unsure about the retention period for the Personal Data being Processed;

1.9.5
if you are unsure about what security or other measures you need to implement to protect Personal Data;

1.9.6
if there has been a Personal Data Breach;

1.9.7
if you are unsure on what basis to transfer Personal Data outside the EEA or the USA;

1.9.8
if you need any assistance dealing with any rights invoked by a Data Subject;

1.9.9
whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA or plan to use Personal Data for Purposes others than what it was collected for;

1.9.10
if you plan to undertake any activities involving Automated Processing including profiling or Automated Decision Making;

1.9.11
if you need help complying with applicable law when carrying out direct marketing activities; or

1.9.12
if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors).

03. Definitions

Term	Definition
Anonymisation	Data amended in such a way that no individuals can be identified From the data (whether directly or indirectly) by any means or by any person.
Binding Corporate Rules	The Personal Data protection policies used for the transfer of Personal Data to one or more Third Countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.
Consent	Any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her.
Customer	Any past, current or prospective Hybrid Theory customer.
Data Controller	GDPR: A natural or legal person, Public Authority, Agency or other body which, alone or jointly with others, determines the Purposes and means of the Processing of Personal Data. CCPA: The CCPA applies to 'businesses', which have a similar role to Data Controllers.
Data Processors	GDPR A natural or legal person, Public Authority, Agency or other body which Processes Personal Data on behalf of a Data Controller. CCPA: A similar term, 'service providers' is used to describe an entity that acts on behalf of the Data Controller/Business.
Data Protection	The process of safeguarding Personal Data from unauthorised or unlawful disclosure, access, alteration, Processing, transfer or destruction.
Data Protection Officer (DPO)	The person required to be appointed in specific circumstances under the GDPR. For Hybrid Theory, the DPO is Gemserv Ltd., who can be contacted at privacy@hybridtheory.com

Data Subject	Anyone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
EEA	European Economic Area - the 28 countries in the EU, and Iceland, Liechtenstein and Norway.
Employee	An individual who works part-time or full-time for Hybrid Theory under a contract of employment, whether oral or written, express or implied, and has recognised rights and duties includes temporary employees and independent contractors.
Encryption	The process of encoding a message or information in such a way that only authorised parties can access it.
Inferred Data	Characteristics or traits assigned to a Data Subject, such as related to their lifestyle, that are ascribed to an individual by nature of observing their behaviour.
Information Commissioner's Office (ICO)	An independent Public Authority in the UK responsible for monitoring the application of the relevant Data Protection regulation set forth in national law.
Personal Data	Any information relating to an identified or identifiable natural person ("Data Subject"); an identifiable person is one who can be identified, directly or indirectly.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.
Process, Processed, Processing	Any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means. Operations performed may include collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling	Any form of automated processing of Personal Data, where Personal Data is used to evaluate specific or general characteristics relating to a data subject. In particular to analyse or predict certain aspects concerning that natural person's performance at work, economic situations, health, personal preferences, interests, reliability, behaviour, location or movement.
Pseudonymisation	Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) without a "key" that allows the data to be re-identified.
Special Categories of Data	Personal Data pertaining to or revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life and sexual orientation, genetic data or biometric data.

04. Policy

4.1 GOVERNANCE

4.1.1 POLICY DISSEMINATION AND ENFORCEMENT

The executive management team of Hybrid Theory must ensure that all Hybrid Theory Employees responsible for the Processing of Personal Data are aware of and comply with the contents of this policy. In addition, Hybrid Theory will make sure all Third Parties engaged to Process Personal Data on their behalf (as Data Processors) are aware of and comply with the contents of this policy. Assurance of such compliance must be obtained from all Third Parties, whether companies or individuals, prior to granting them access to Personal Data controlled by Hybrid Theory.

4.1.2 DATA PROTECTION BY DESIGN

4.1.2.1
To ensure that all Data Protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes, each of them must go through an approval process before continuing.

4.1.2.2
As required under the GDPR, Hybrid Theory must ensure that a Data Protection Impact Assessment (DPIA) is conducted, for all new and/or revised systems or processes for which it has responsibility.

4.1.2.3
It shall be the responsibility of the Data Protection Officer to decide where a Data Protection Impact Assessment is required in addition to approve, with executive management, any system or process subject to the DPIA, and any implementing measures.

4.1.3 EXECUTIVE OVERSIGHT

4.1.3.1
Executive oversight and buy-in is a core component of ensuring that this policy is implemented effectively.

4.1.3.2
The Hybrid Theory Management Team is ultimately responsible for ensuring that Hybrid Theory meets its legal obligations. The Management Team will be kept regularly apprised of Hybrid Theory's implementation and adherence to this Data Protection Policy by the Data Protection Officer.

4.1.3.3
Where possible, the Management Team should have an item on the agenda that is relevant to data protection, and where the Data Protection Officer can seek approval of any specific measures required to target certain risks.

4.1.4 ROLES AND RESPONSIBILITIES

4.1.4.1
As required under the GDPR, Hybrid Theory will appoint a Data Protection Officer. The Data Protection Officer will only report to executive management of Hybrid Theory and will have no other line responsibilities or duties that involve processing personal data other than in a DPO capacity.

The Data Protection Officer that Hybrid Theory have appointed is Emser Ltd. The Data Protection Officer will be responsible for:

- Keeping the Hybrid Theory Management Team updated about data protection responsibilities, risks and issues;
- Reviewing all data protection procedures and related policies, in line with an agreed schedule
- Handling data protection questions from staff and Data Processors;
- Dealing with Data Subject Requests from Data Subjects;
- Vetting any contracts or agreements with third parties that may handle the company's sensitive data before they go over to a legal body for final approval;
- Oversee general and specific data protection training for employees;
- Responding to and notifying the appropriate supervisory authorities in relation to any data breaches that occur;
- Carrying out and approving any Data Protection Impact Assessments, where required;

4.1.4.2
The Chief Technology Officer (CTO) will be responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards;
- Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.

4.1.4.3
The Head of Products will be responsible for:

- Approving any public-facing data protection statements attached to communications such as emails and letters.
- Approving any amendments to client or third-party agreements that the Head of Products in responsible for.
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

4.2 PRINCIPLES

4.2.1 DATA PROTECTION

Hybrid Theory has adopted the following principles to govern its collection, use, retention, transfer, disclosure and destruction of Personal Data.

Term	Definition
Principle 1: Lawfulness, Fairness and Transparency	Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. This means, Hybrid Theory must tell the Data Subject what Processing will occur (transparency), the Processing must match the description given to the Data Subject (fairness), and it must be for one of the purposes specified in the applicable Data Protection regulation (lawfulness).
Principle 2: Hybrid Theory Limitation	Personal Data shall be collected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those Purposes. This means Hybrid Theory must specify exactly what the Personal Data collected will be used for and limit the Processing of that Personal Data to only what is necessary to meet the specified Hybrid Theory.
Principle 3: Data Minimisation	Personal Data shall be adequate, relevant and limited to what is necessary in relation to the Purposes for which they are Processed. This means Hybrid Theory must not store any Personal Data beyond what is strictly required.
Principle 4: Accuracy	Personal Data shall be accurate and kept up to date. This means Hybrid Theory must have in place processes for identifying and addressing out-of-date, incorrect and redundant Personal Data.
Principle 5: Storage Limitation	Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the Purposes for which the Personal Data is Processed. This means Hybrid Theory must, wherever possible, store Personal Data in a way that limits or prevents identification of the Data Subject.
Principle 6: Integrity & Confidentiality	Personal Data shall be 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. Hybrid Theory must use appropriate technical and organisational measures to ensure the integrity and confidentiality of Personal Data are maintained at all times.

4.2.2
ACCOUNTABILITY

The Data Controller shall be responsible for the implementation of this policy, and should be able to demonstrate compliance with it as required. This means Hybrid Theory must demonstrate that the six Data Protection Principles (outlined above) are met for all Personal Data for which it is responsible.

4.3 DATA COLLECTION

4.3.1 FORM OF COLLECTION

4.3.1.1
Hybrid Theory will collect Personal Data from employees and job applicants directly where possible. Where the applicant is referred by an agency, Hybrid Theory may collect that data from the agency, but will ensure that the agency has committed to sourcing the data on a sound legal basis (e.g. consent), unless the agency acts as a Data Processor for Hybrid Theory (i.e. only collects the Personal Data for Hybrid Theory's purposes).

4.3.1.2
Hybrid Theory will collect Personal Data from clients and suppliers directly as required for the provision of services to them, including the administration of relevant contracts.

4.3.1.3
Hybrid Theory will collect Personal Data of internet users in a pseudonymous form from third party partners, such as ShareThis and 33Across, as well as other website publishers. When receiving such data, Hybrid Theory will ensure that these third parties, as Data Controllers, collect the relevant consent from Data Subjects, or verify it is collected from website publishers. Hybrid Theory will ensure this through entering into agreements with them to control their data processing and reviewing/auditing their practices to these standards.

4.3.1.4
Hybrid Theory may also collect Personal Data of its own website and internet users, i.e. via Cookies, with their consent.

4.3.2 CONSENT

4.3.2.1
Hybrid Theory will obtain Personal Data only by lawful and fair means and, where appropriate, with the knowledge and Consent of the Data Subject concerned.

4.3.2.2
Where a need exists to request and receive the Consent, Hybrid Theory will ensure to seek such Consent via an agreement or positive action, from an individual prior to the collection, use or disclosure of their Personal Data.

4.3.2.3
Where possible, Hybrid Theory systems should be able to record consent that is collected, either through forms, or individuals accepting or clicking certain operations on the Hybrid Theory website or in email links. This should include systems such as CRM (Customer Relations Management) and other databases. The system(s) must include provisions for:

- Determining what disclosures should be made in order to obtain valid Consent.
- Ensuring the request for Consent is presented in a manner which is clearly distinguishable from any other matters, is made in an intelligible and easily accessible form, and uses clear and plain language.
- Ensuring the Consent is freely given (i.e. is not based on a contract that is conditional to the processing of Personal Data that is unnecessary for the performance of that contract).
- Documenting the date, method and content of the disclosures made, as well as the validity, scope, and volition of the Consents given.
- Providing a simple method for a Data Subject to withdraw their Consent at any time.

4.3.2.4
With respect to consent for cookie deployment and online advertising, Hybrid Theory will carry out the following to ensure consent is correctly collected:

- Hybrid Theory will register with the IAB Consent Framework operated on the websites of our third-party partners as well as through initiatives such as the Network Advertising Initiative;
- Hybrid Theory will ensure that opt-in boxes or selections are required for consent needed for marketing purposes;
- Hybrid Theory will maintain a Cookie Notice that allows website users to consent to various types of cookies being installed on their device.

4.3.3 NOTIFICATION

4.3.3.1
Hybrid Theory is required under both the GDPR and CCPA to provide Data Subjects with information related to the Processing of their Personal Data.

4.3.3.2
When the Data Subject is asked to give Consent to the Processing of Personal Data, and when any Personal Data is collected from the Data Subject, we will disclose to them information about the

purposes for which we are asking for Consent, unless one of the following apply:

- The Data Subject already has the information
- A legal exemption applies to the requirements for disclosure and/or Consent (i.e. the data is needed to be disclosed to a doctor in relation to a medical emergency affecting an employee, for example).

4.3.3.3
This information may be given orally, electronically or in writing. If given orally, the person making the disclosures should use a suitable script, as designated by the Data Protection Officer.

4.3.3.4
In general, Hybrid Theory will provide such information through the use of Privacy Notices on its website. This will include a general website Privacy Notice, a Recruitment Privacy Notice and an Employment Privacy Notice.

4.3.3.5
Within these notices and disclosures, Hybrid Theory will present the following information to Data Subjects, where any of the CCPA, GDPR or other national laws apply:

- Contact details for the Data Protection Officer;
- Legal basis for the processing (i.e. consent, or legitimate interests where a Legitimate Interest Assessment is used);
- A description of the processing;
- The categories of Personal Data that are collected;
- The recipients, or categories of recipients, to whom the Personal Data has been or may be transmitted, along with the location of those recipients (including, under the CCPA, whether such disclosure is considered a 'sale' of Personal Data);
- Any transfers outside the EEA that occur for GDPR/EU/UK data collection (for example, including databases such as CharlieHR that host data outside the EEA);
- Any retention periods, as detailed in the Records of Processing Activities and Retention policy;
- The existence of Data Subject Rights, and how and when to exercise them, including the right to opt-out, where applicable. For more information on these rights, please see the Data Subject Rights Policy;
- A summary of the security measures in place to protect the data.

4.3.3.6
Under the CCPA, a 'sale' of Personal Data is considered to occur where being shared with certain third parties. This includes personal data or cookie data that we share with our advertising partners, clients and other organisations involved in the online advertising ecosystem. However, it does not apply where cookie data is shared with our core software as a service (SaaS) providers, such as CRM systems, HR systems, cloud storage providers and others.

4.3.3.7
Hybrid Theory will ensure that this information is provided to Data Subjects promptly, but in no case later than:

- Under the CCPA and GDPR, and other national legislation (such as that applicable in Hong Kong, Singapore and Australia) at the time of first communication, if used for communication with the Data Subject; or
- Under the GDPR, at the time of disclosure, if disclosed to another recipient, or;
- Under the GDPR, at the latest within one calendar month from the first collection or recording of the Personal Data.

4.3.3.8
If Personal Data is collected from someone other than the Data Subject, the Data Subject must be informed of the collection unless one of the following apply:

- The Data Subject has received the required information by other means.
- The information must remain confidential due to a professional secrecy obligation.
- A national law expressly provides for the collection, Processing or transfer of the Personal Data.

4.3.3.9
Where third parties are involved in collecting the Personal Data as Data Controllers (such as 33Across and Sharethis, and also, recruitment agencies etc.), Hybrid Theory will ensure that these parties are responsible for collecting and evidencing proof of providing information to Data Subjects and/or collecting Consent.

4.4 DATA USE

4.4.1 DATA PROCESSING

4.4.1.1
Hybrid Theory will use the Personal Data of individuals for the following broad purposes:

- For the administration of contracts and services provided to clients (e.g. for financial purposes);
- In the course of creating profiles of users, for the purpose of enabling clients to provide targeting advertising;
- For the purpose of sending marketing communications to potential clients;
- For technical maintenance of our website;
- For the administration and performance of employee contracts;
- For processing recruitment applications.

4.4.1.2
The use of individuals' information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object. We should not generally use (or reuse) personal data collected for one purpose for another purpose)

4.4.1.3
Hybrid Theory will Process Personal Data in accordance with all applicable laws and applicable contractual obligations. More specifically, under the CCPA, Hybrid Theory will not Process Personal Data unless at least one of the following requirements are met:

- The Data Subject has given Consent to the Processing of their Personal Data for one or more specific purposes (i.e. for the collection of Cookies);
- Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract (i.e. in relation to employment contracts and contracts with clients);
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject (such as in relation to employment law);
- Processing is necessary for the purpose of the legitimate interests pursued by the Data Controller or by a Third Party (such as in relation to marketing to existing or former clients, where a Legitimate Interest Assessment is carried out);
- Other exceptional situations, such as where Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person, necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.

.

4.4.1.4
In Hong Kong and Singapore, we should only collect Personal Data for the following purposes:

- With the consent of the individual. Here, we can collect Personal Data with 'deemed consent' – i.e. provided that we give notice of the types of processing, the individual voluntarily provides the data to us and it is reasonable that they would voluntarily provide such data;
- Where collection is necessary for a purpose in the interest of the individual, consent cannot be achieved in a timely way and the individual will not reasonably be expected to withhold consent;
- As necessary to reasonably manage or terminate an employment relationship.

4.4.1.5
Under the CCPA, no limits to data processing are required, providing the Data Subject has the opportunity to opt-out to a 'sale' of Personal Data.

4.4.1.6
The following types of processing will be prohibited and will not be performed by Hybrid Theory:

- Any collection of Inferred Data that includes, or is derived from, Special Category Personal Data. We will ensure this through our agreements with data brokers, website publishers and blacklists in our AI system;
- Any Profiling on the basis of Special Category Personal Data (profiling includes creating audience segments using such data). We will ensure this through applying blacklists in our AI system;
- Any Automated Decision-Making, including Profiling, on features or behavioural aspects that are likely to be specific to children. Automated decision-making also refers to processes such as creating audience segments as well as characterising data sets into particular groups. We will ensure this through blacklists in our AI system.

4.4.2 TYPES OF PERSONAL DATA

4.4.2.1
The following are types of Personal Data that Hybrid Theory will collect and/or process:

- Identifiers, such as first name, last name, username or similar identifier or other unique online identifier collected via our website or other websites.
- Contact Data, such as email address and phone number.
- Technical Data, which includes Internet protocol (IP) address,

device identifiers, login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform, and other information.

- Behavioural Data or Inferred data, which includes interests and preferences which we receive in relation to websites that individuals have viewed and their interactions with various web pages, as collected through our cookies and cookies installed by our third-party providers. This data is limited to non-personally identifiable data – i.e. data that does not include 'real-world' identifiers, such as name, address, email address, etc. It may also include Inferred Data – i.e. whereby we assign characteristics such as related to lifestyle or interests that we ascribe to by nature of viewing history. We take all measures to ensure these do not include Special Category Data.

4.4.2.2
In relation to recruitment, the following Personal Data may also be collected:

- Date of birth;
- Qualifications and employment history;
- Interview notes during an application;
- Information about past criminal convictions (limited only to confirming whether you have such convictions or not).

4.4.2.3
In relation to employees, the following Personal Data may also be collected:

- Medical information;
- Bank details and other financial information;
- Salary and payment information;
- Benefits and related information;
- Performance history;
- Sick leave details;
- Passport and other identification details.

4.4.2.4
All personal identifiers (including Cookie IDs and associated data) collected from third-party suppliers, such as Sharethis and 33Across will generally be treated as Personal Data under the GDPR and CCPA, among other legislation. This means that all the relevant protections under the GDPR should be applied to it. Such data should be placed in databases when data subjects can exercise their rights

over it. The mechanisms for exercising rights over these types of data, including Cookie IDs and associated data, is discussed further in the Data Subject Rights Policy.

4.4.2.5
Hybrid Theory will avoid processing any Special Categories of Data, in either a commercial or employment context. This is because further safeguards and specific legal justifications will have to apply to the processing of such data.

4.4.2.6
Hybrid Theory will only process Criminal Convictions data in the following circumstances:

- At the final stage or recruitment applications, Data Subjects may be asked if they have Criminal Convictions;
- This will only consist of recording the simple yes/no response as to whether an individual has Criminal Convictions, and should be asked with consent.
- Any specific records of Criminal Convictions data, such as the content of Criminal Convictions, will not be recorded, as it cannot be justified without a legal obligation and should not be collected with employees' consent in the recruitment context.

4.4.3 DATA QUALITY

4.4.3.1
Hybrid Theory will adopt all necessary measures to ensure that the Personal Data it collects and Processes is complete and accurate in the first instance, and is updated to reflect the current situation of the Data Subject.

4.4.3.2
The measures adopted by Hybrid Theory to ensure data quality include:

- Ensuring that third-party partners from whom data is collected provide sufficient assurances that such data is collected accurately and is not tampered with;
- Personal Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets;
- Personal Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database. It is the Marketing Manager's/Head of Product's responsibility to ensure marketing databases are checked against industry suppression files every six months;
- Correcting Personal Data known to be incorrect, inaccurate,

incomplete, ambiguous, misleading or outdated, even if the Data Subject does not request rectification. As such, Personal Data, including Pseudonymous Data, must be processed on systems that allow it to be redacted and correct. Suitable HR databases should also be used for this purpose, and paper records kept to a minimum, where possible;

- Keeping Personal Data only for the period necessary, to satisfy the permitted uses or applicable statutory retention period. This will particularly include expiry periods for Cookies and Inferred Data;
- The removal of Personal Data if in violation of any of the Data Protection principles or if the Personal Data is no longer required.
- For databases storing data collected about EU or UK citizens, ensuring the possibility of restriction, at the request of a Data Subject, rather than deletion of Personal Data, in certain situations.

4.4.4 DIRECT MARKETING

4.4.4.1
Hybrid Theory will follow all regulation in the area of direct marketing, under the Privacy and Electronic Communications Regulations 2003 (which governs Direct Marketing activities within the EU), which applies to telephone, SMS and email communications. The following will also apply to Direct Marketing under legislation in Hong Kong and Singapore.

4.4.4.2
Hybrid Theory will be required to collect consent before engaging in the follow types of 'marketing':

- Contacting individuals in relation to roles at Hybrid Theory;
- Contacting potential business leads who we are unsure of whether they would be within Hybrid Theory's target market of businesses/ clients (although generally these parties should not be contacted);

4.4.4.3
Consent must meet the following standard:

- The consent must be freely given, specific, informed and unambiguous, i.e. Hybrid Theory must not use consent for sending of marketing materials in an employment context, and the relevant notice for the consent must specifically explain what is being asked for (i.e. what type of marketing material will be sent);
- The consent must be expressed by a statement or clear affirmative action. Silence, pre-ticked boxes or inactivity should therefore not constitute consent, so boxes must be actively ticked, for example;
- The consent must be as easy to withdraw as it was to provide consent in the first place (which means an email or other facility to opt-out should be easily provided);

- The consent language must be intelligible and use clear and plain language;

- The organisation must be able to demonstrate that the individual has consented, meaning Hybrid Theory must keep a Salesforce or HTML ticket or other record and relevant email copies of consent, as applicable.

4.4.4.4
Contacting recipients via email to establish whether consent is in place also constitutes direct marketing and is prohibited without first obtaining consent.

4.4.4.5
Hybrid Theory will be required to obtain consent before contacting business leads received from third parties unlike the third party that provided that business lead can verify that the business lead would have a reasonable expectation is receiving products and services from Hybrid Theory. In order to do so, the lead must be sourced from. For leads where Hybrid Theory has i) a business relationship; ii) who voluntary gave Hybrid Theory their contact details, or; iii) who are within Hybrid Theory's target market, consent will not be needed to contact them.

4.4.4.6
The Data Subject (including staff at businesses who are leads) must be informed at the point of first contact that they have the right to object, at any stage, to having their data Processed for such purposes. This can be achieved through a link to Hybrid Theory's Privacy Policy in email communications, whereas telecommunications are a lesser priority.

4.4.4.7
If the Data Subject puts forward an objection, digital marketing related Processing of their Personal Data must cease immediately, and their details should be kept on a suppression list with a record of the opt-out decision, rather than being completely deleted.

4.5 DATA RETENTION

4.5.1
Hybrid Theory will adopt all necessary measures to ensure that the Personal Data it collects and processes is complete and accurate in the first instance, and is updated to reflect the current situation of the Data Subject, as outlined above.

4.5.2
To ensure fair processing, Personal Data will not be retained by Hybrid Theory for longer than necessary in relation to the purpose for which it was originally collected, or for which it was further Processed.

4.5.3
The length of time for which Hybrid Theory needs to retain Personal Data is set out in the Data Retention Policy and/or Records of

Processing Activities. This takes into account the legal and contractual requirements, both minimum and maximum, that influence the retention periods set forth in the schedule. All Personal Data should be securely deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

4.6 DATA SECURITY

4.6.1
Hybrid Theory will adopt physical, technical, and organisational measures to ensure the security and protect the confidentiality, integrity and availability of the Personal Data, defined as follows:

4.6.1.1
Confidentiality means ensuring that only people who have a need to know and are authorised to use the Personal Data can access it;

4.6.1.2
Integrity means ensuring that Personal Data is accurate and suitable for the purpose for which it is processed;

4.6.1.3
Availability means ensuring that authorised users are able to access the Personal Data when they need it for authorised purposes.

4.6.2
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.

4.6.3
A summary of the Personal Data related security measures is provided below:

4.6.3.1
Preventing unauthorised persons from gaining access to data processing systems in which Personal Data are Processed, through the use of access controls and password usage on databases and systems. In particular, passwords should be changed regularly and contain a minimum of 8 characters with a random mixture of letters and numbers, and upper and lower-case letters;

4.6.3.2
Preventing persons entitled to use a data processing system from accessing Personal Data beyond their needs and authorisations, additionally through the employment of role and rule-based access controls;

4.6.3.3
Data relating to individual cookie IDs or any log-level data should only be accessed via authorised individuals using unique Amazon Web Services generated credentials;

4.6.3.4
Ensuring that Personal Data in the course of electronic transmission during transport cannot be read, copied, modified or removed without authorisation, such as through the use of secure channels and/or encryption in transit;

4.6.3.5
Ensuring 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 (including logs of access to database and the modification of data, where possible);

4.6.3.6
Regularly evaluate and test the effectiveness of safeguards to ensure security of Processing of Personal Data, including through the use of penetration tests by Firewalls;

4.6.3.7
Only store data using approved systems, such as Amazon Web Services, Google, Atlassian, CharlieHR, Salesforce or other authorised cloud storage provider. Cloud storage providers are only authorized if data is protected by sufficient security software and a firewall. Data should not be stored on hard-drives of devices or removable storage media;

4.6.3.8
Data should be backed up frequently in an automated way only and only via an authorised cloud storage service provider;

4.6.3.9
When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.

4.7 DATA SUBJECT RIGHTS

4.7.1
The process for attending to the following Data Subject rights is outlined in detail in Hybrid Theory's Data Subject Rights Policy.

This will encompass the following rights:

- Right of access to personal data;
- Right of objection to processing;
- Right of objection to automated decision-making and profiling;
- Right to restriction of processing, in certain circumstances;
- Right to data portability, in certain circumstances;
- Right to data rectification/correction, in certain circumstances;
- Right to data erasure, in certain circumstances;

- Right to opt-out to data processing, including the Do Not Sell My Personal Information right in California;

- Right to withdraw consent (such as in Singapore)

4.7.2
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.

4.7.3
Data Subjects are entitled to, based upon a request made in and upon successful verification of their identity, the following information about their own Personal Data.

4.7.4
A response to each request will be provided within the applicable periods for each jurisdiction specified in the Data Subject Rights Policy. That period may be extended by the specified periods where necessary, taking into account the complexity and number of the requests (i.e. if numerous difficult or onerous requests are received).

4.7.5
Hybrid Theory are entitled to request appropriate verification must confirm that the requestor is the Data Subject, as well as appropriate information to identify their Personal Data. This could include, for example, requiring Data Subjects to share their Cookie IDs before their data can be located. Hybrid Theory are not obliged to provide information (i.e. Personal Data) to Data Subjects where it cannot reasonably be located.

THIRD PARTY DATA

4.7.6
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, we must make sure to redact or withhold information as may be necessary or appropriate to protect that person's rights. This is a decision for the Data Protection Officer to carry out.

4.7.7
When Personal Data is collected indirectly (for example, from a third party or publicly available source), Hybrid Theory will provide the Data Subject with all the information required by the GDPR, CCPA and other relevant legislation as soon as possible after collecting/ receiving the data. Hybrid Theory will also check with the third-party (such as, for example, a recruitment agency, client, or third-party data provider) that the Personal Data was collected by the third party in accordance with the GDPR, CCPA and other relevant legislation and on which legal basis that the processing of that Personal Data takes place. This will particularly apply to us when sourcing business leads.

4.8 DATA PROTECTION TRAINING

4.8.1
All Hybrid Theory employees that have access to Personal Data will have their responsibilities under this policy outlined to them as part of their staff induction training. Employees will be given this policy to study as part of their mandatory data protection training.

4.8.2
In addition, Hybrid Theory's Data Protection Officer will provide for, and oversee, regular Data Protection guidance for Hybrid Theory staff.

4.8.3
The training and procedural guidance set forth will consist of, at a minimum, the following elements:

- The Data Protection Principles set forth in this policy;
- Each Employee's duty to use and permit the use of Personal Data only by authorised persons and for authorised purposes, as set out in this policy.
- The need for, and proper use of, the forms and procedures adopted to implement this policy, such as for the collection of consent;
- Data security training around:
  - the correct use of passwords, the use of encryption, VPNs and other access or security mechanisms;
  - securely storing manual files, printouts and electronic storage media;
  - information on how to detect a phishing email;
- Proper disposal of Personal Data by using secure shredding facilities as well as on electronic devices;
- Any special risks associated with particular departmental activities or duties, such as specific rules for direct marketing, as set out in this policy.

4.9 DATA TRANSFERS

4.9.1
Hybrid Theory may transfer Personal Data to internal or Third-Party recipients located in another country where that country is recognised as having an adequate level of legal protection for the rights and freedoms of the relevant Data Subjects. An international 'data transfer' is said to occur when access is given or information is transferred (digitally or physically) to organisations or individuals outside of the country of initial processing.

4.9.2
For the GDPR (including in the UK), transfers are limited to countries outside the EEA, as well as nominated others, such as Uruguay, Argentina, Canada, New Zealand, Israel, and the USA, subject to the Privacy Shield.

4.9.3
For other jurisdictions, such as Singapore and Hong Kong, extraterritorial data transfers are limited to situations where the destination country or jurisdiction providers for comparable standards to Singaporean or Hong Kong laws. This should be assessed on a case-by-case basis with the collaboration of the Data Protection Officer.

4.9.4
Where transfers need to be made to countries lacking an adequate level of legal protection (i.e. those outside the EEA), they must be made in compliance with an approved transfer mechanism. This will include either:

- Putting in place safeguards for the transfer of personal data to the USA, such as by registering with the Privacy Shield framework (as applicable under the GDPR);
- Signing Standard Contractual Clauses, as provided by the European Commission, with relevant organisations in countries to which Personal Data will be sent from the EEA (as applicable under the GDPR).
- Putting into place agreements that require such parties to commit to data security requirements, respecting individual rights, limit the situations in which they can process or disclose Personal Data, and other requirements (as generally applicable).
- Otherwise, collecting the consent of the Data Subject directly for the data transfer (as generally applicable) (this is unlikely to apply in the employment context).

4.9.5
Under the GDPR, in other exceptional circumstances, Hybrid Theory may only transfer Personal Data where one of the transfer scenarios listed below applies:

- The transfer is necessary for the performance of a contract with the Data Subject (such as for the provision of products and services under such a contract);
- The transfer is necessary for the implementation of pre-contractual measures taken in response to the Data Subject's request;
- The transfer is necessary for the conclusion or performance of a contract concluded with a Third Party in the interest of the Data

Subject (such as in relation to travel booking under an employment contract, for example);

- The transfer is legally required on important public interest grounds;
- The transfer is necessary for the establishment, exercise or defence of legal claims;
- The transfer is necessary in order to protect the vital interests of the Data Subject (such as in relation to a medical emergency).

4.9.6
Whether any of the grounds above apply should be assessed on a case-by-case basis.

TRANSFERS TO THIRD PARTIES

4.9.7
Hybrid Theory will only transfer Personal Data to, or allow access by, Third Parties when it is assured that the information will be processed legitimately and protected appropriately by the recipient. Where staff or business managers are considering using a third party, a request should be sent to the Data Protection Officer to ensure that the organisation is reviewed from a privacy and data security perspective.

4.9.8
Where processing of Hybrid Theory's Personal Data by a third party takes place, Hybrid Theory will first identify if, under applicable law, the Third Party is considered a Data Controller or a Data Processor of the Personal Data being transferred.

4.9.9
Where the Third Party is deemed to be a Data Controller, Hybrid Theory will enter into an appropriate agreement with the Controller to clarify each party's responsibilities in respect to the Personal Data transferred.

4.9.10
Where the Third Party is deemed to be a Data Processor, we will enter into an adequate Processing agreement with the Data Processor. The agreement must require the Data Processor to protect the Personal Data from further disclosure and to only Process Personal Data in compliance with Hybrid Theory instructions. In addition, the agreement will require the Data Processor to implement appropriate technical and organisational measures to protect the Personal Data, as well as procedures for providing notification of Personal Data Breaches.

4.9.11
When outsourcing services to a Third Party (including Cloud Computing services), Hybrid Theory will identify whether the Third Party will Process Personal Data on its behalf and whether the outsourcing will entail any international Data Transfers. Where appropriate, Hybrid Theory will not transfer any data to such third

parties until these arrangements have been verified. These will include arrangements as specified in the section above.

4.9.12
Hybrid Theory will only disclose or share Personal Data with listed third parties, including Appnexus, and cloud-service providers, such as Amazon Web Services, Google, Atlassian, CharlieHR, Salesforce after undergoing a due diligence process and agreeing the necessary contractual arrangements as specified above.

4.9.13
Hybrid Theory may be required to disclose personal to law enforcement authorities in certain situations. Under these circumstances, Hybrid Theory will disclose requested data as the minimum possible required.

4.10 DATA BREACH REPORTING

4.10.1
Under all applicable legislation (with the exception of Hong Kong), Hybrid Theory are required to report certain Personal Data Breaches to supervisory authorities and potential individuals. A member of staff who suspects that a Personal Data Breach has occurred due to the theft or exposure of Personal Datta must immediately notify the Data Protection Officer providing a description of what occurred, by emailing privacy@hybridheory.com

4.10.2
The Data Protection Officer will then be responsible for classifying the severity of the incident or Personal Data Breach (which may require notification to Supervisory Authorities and individuals), and deciding any action required, in accordance with the Incident Management Policy.

4.10.3
All reported incidents will be investigated to confirm whether or not a Personal Data Breach has occurred. For severe Personal Data Breaches, Hybrid Theory must inform the relevant supervisory authority as specified in the Incident Management Policy, which will be the responsibility of the Data Protection Officer.

4.10.4
The Data Protection Officer should update Hybrid Theory's Incident Management Log, including pertinent facts relating to the incident, effects and remedial actions taken in relation to any Security Incidents or Personal Data Breaches.

4.10.5
Further guidance can be found in the Incident Management Policy.

05. Policy Maintenance

5.1 Publication
This policy shall be available to all Employees through the Hybrid Theory intranet.

5.2 Effective Date

5.3 Revisions

06. Related Documents

- Data Subject Rights Policy
- Incident Management Policy
- Data Retention Policy
- Privacy Notice
- Employment Privacy Notice
- Recruitment Privacy Notice

Appendix A - Adequacy for Personal Data Transfers (EU/UK)

The following table includes:

1. The countries recognised as having an adequate level of legal protection for the rights and freedoms of Data Subjects in relation to the Processing of their Personal Data.

2. The safeguards that can provide adequate protection when transfers are made to countries lacking an adequate level of legal protection.

3. Derogations

Adequate Countries

The following is a list of countries recognised as having an adequate level of legal protection for the rights and freedoms of Data Subjects in relation to the Processing of their Personal Data:

1. **EU Countries:** (Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK)

2. **EEA Countries:** Iceland, Liechtenstein, Norway

3. **Third Countries:** Andorra, Argentina, Canada (commercial organisations); Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, United States (Privacy Shield certified organisations).

Non-Adequate Countries

The Following are a list of safeguards that can provide adequate protection when transfers are made to countries lacking an adequate level of legal protection.

1. Model Clauses
2. Binding Corporate Rules
3. Codes of Conduct
4. Certification Mechanisms

Derogations

1. Explicit Consent

2. Compelling Legitimate Interests

3. Important reasons of Public Interest

4. Transfers in response to a foreign legal requirement

5. Data Protection Act approved contracts between Data Controllers and Data Processors