Data Protection Policy

1. Purpose

Hatch Mansfield holds personal data about its employees, clients, suppliers and other individuals for a variety of business purposes.

This data protection policy sets out how **Hatch Mansfield** protects personal data and ensures that staff understand the rules governing their use of personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the Data Controller (DC) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

2. Scope

This policy applies to all staff. They must be familiar with this policy and comply with its terms. This policy supplements other policies relating to internet and email use. Hatch Mansfield may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

3. Responsibility

Our Financial Director has overall responsibility for the day-to-day implementation of this policy.

Fair and lawful processing

Hatch Mansfield must process personal data fairly and lawfully in accordance with individuals' rights. This generally means that Hatch Mansfield should not process personal data unless the individual whose details we are processing has consented to this happening, Hatch Mansfield has a legal requirement or a legitimate interest to hold and process the data.

The authority to hold and process data will be relevant and appropriate to the type of data and the reason for holding and processing that data.

Financial Director's Responsibilities:

- Keeping the board updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all staff members and those included in this policy
- Answering questions on data protection from staff, board members and other stakeholders
- Responding to individuals such as clients and employees who wish to know which data is being held on them by Hatch Mansfield
- Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing
- Ensuring all systems, services, software and equipment meet acceptable security standards with the co-operation of our IT support company
- Ensuring security hardware and software are checked and scanned regularly by Computer Strategies to ensure it is functioning properly

- Ensuring third-party services, such as cloud services the company is considering using to store or process data, are EU GDPR compliant with the co-operation of Computer Strategies

Account & Associate Director Responsibilities:

- Approving data protection statements attached to emails and other PR/communications copy
- Addressing data protection queries from clients, target audiences or media outlets
- Co-ordinating our Data Controllers to ensure all PR/communications initiatives adhere to data protection laws and the company's Data Protection Policy

The processing of all data must be:

- Necessary to deliver our services
- In our legitimate interests and not unduly prejudice the individual's privacy
- In most cases this provision will apply to routine business data processing activities.

Our client contracts contain a Data Protection Clause informing clients regarding data protection.

The notice:

- Sets out the purposes for which Hatch Mansfield holds personal data on clients and employees
- Highlights that work may require information to be given to third parties such as professional advisers
- Provides that clients have a right of access to the personal data that we hold about them

Sensitive Personal Data

In most cases where we process sensitive personal data we will require the data subject's explicit consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

Accuracy and Relevance

Hatch Mansfield will ensure that any personal data it processes is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. Hatch Mansfield will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform our Financial Director.

Your Personal Data

You must take reasonable steps to ensure that personal data Hatch Mansfield holds about you is accurate and updated as required. For example, if your personal circumstances change, please inform the Financial Director and the Office Manager so that they can update your records.

Data Security

You must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the Financial Director will establish what, if any, additional

specific data security arrangements need to be implemented in contracts with those third-party organisations.

Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it.
- Printed data should be shredded when it is no longer needed. If you print a piece of confidential information, you must retrieve it from the printer immediately.
- Data stored on a computer is protected by strong passwords that are changed regularly. All staff are automatically required to change their password every three months. There is a lockout policy in place.
- Memory sticks / back up drives containing data must be locked away securely when they are not being used or the data erased immediately after use.
- The Financial Director must approve any cloud application used to store personal data, for example, Dropbox.
- Servers are kept in a secure location and only accessible to approved personnel.
- Data is backed up daily in line with the company's backup procedures.
- All servers containing sensitive data must be approved and protected by security software and strong firewall.

Data Retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

Transferring Data Internationally

There are restrictions on international transfers of personal data. You must not transfer personal data anywhere outside the UK without first consulting the Financial Director.

Subject Access Requests / Requests for Erasure

Please note that under the Data Protection Act 1998, individuals are entitled, subject to certain exceptions, to request access to information held about them or that such information be erased.

If you receive a subject access request or request for erasure, you should refer that request immediately to the Financial Director. We may ask you to help us comply with those requests.

Please contact the Financial Director if you would like to correct or request information that we hold about you. There are also restrictions on the information to which you are entitled under applicable law.

Processing Data in Accordance with the Individual's Rights

You should abide by any request from an individual not to use their personal data for direct marketing purposes and notify the Financial Director about any such request.

Please contact the Financial Director for advice on direct marketing before starting any new direct marketing activity.

Training

All staff will receive training on this policy. New joiners will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our policy and procedure.

Training is provided through an in-house seminar on a regular basis.

It will cover:

- The law relating to data protection
- Our data protection and related policies and procedures.

Completion of training is compulsory.

GDPR Provisions

Where not specified previously in this policy, the following provisions will be in effect on or before 25 May 2018.

Privacy Notice - transparency of data protection

Being transparent and providing accessible information to individuals about how we will use their personal data is important for our organisation. The following are details on how we collect data and what we will do with it:

What information is being collected?	Legally required data. Contact details for business and marketing communications. Private client data in order to fulfil sales orders, payments and deliveries. Employee data (past and present) including personal data in order to carry out employer / employee relationship & activities. Guest data for trips and events, including personal data such as dietary requirements.
How is it collected?	Email, post, third party suppliers
Why is it being collected?	To carry out the function and related activities of a wine importing and distribution business.
How will it be used?	Within legal boundaries and in an appropriate manner for the activity.
Who will it be shared with?	Account teams, third party delivery companies. HMRC for legal requirements.
Identity and contact details of staff with key responsibilities.	Primary; Kirsty McCubbin, Financial Director kirstymccubbin@hatch.co.uk 07387261097 Secondary; Daniel Hart, Commercial Manager danielhart@hatch.co.uk 07887804943 All staff act as Data Controllers to some extent.
Details of transfers to third country and safeguards	Only for legitimate interest with wine suppliers, such as customer visits to those suppliers
Retention period	Past employee records – 6 years CVs, interview notes … - 6 months PAYE, SSP, SMP – 3 years

	Accounts, tax records – 6 years

Conditions for Processing

Hatch Mansfield will ensure any use of personal data is justified using at least one of the conditions for processing and this is specifically documented in our Data Impact Assessment which is audited internally annually. All staff who are responsible for processing personal data are trained to be aware of the conditions required for processing. The conditions for processing will be available to data subjects in the form of a privacy notice.

Justification for Personal Data

Hatch Mansfield will process personal data in compliance with all six data protection principles, which are listed below:

1. processed lawfully, fairly and in a transparent manner in relation to the data subject;
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes;
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject;
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

Hatch Mansfield will document the additional justification for the processing of sensitive data, and will ensure any biometric and genetic data is considered sensitive.

Consent

The data that Hatch Manfield may collect for which it does not have a legal or legitimate interest is subject to active consent by the data subject. This consent can be revoked at any time.

Data Portability

Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within 30 days, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done for free.

Right to be Forgotten

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

Privacy by Design and Default

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The Financial DIrector will be responsible for conducting Privacy Impact Assessments and ensuring that all IT projects commence with a privacy plan.

When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

International Data Transfers

No data may be transferred outside of the EEA without first discussing it with the Financial Director. Specific consent from the data subject must be obtained prior to transferring their data outside the EEA.

Data Audit and Register

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant. The Financial DIrectopr will report to the Board annually.

Reporting Breaches

All members of staff have an obligation to report actual or potential data protection compliance failures to the Financial Director, for example, if you suspect someone has accessed your PC or company mobile telephone without your consent. This allows us to:

- Investigate the failure and take remedial steps if necessary;
- Maintain the record of compliance failures,
- Notify the Supervisory Authority (currently the Information Commissioner's Office) of any compliance failures that are material either in their own right or as part of a pattern of failures within 72 hours of detecting the breach. See our Business Resilience Plan.

Security measure	**This security measure is in place (Yes/ No)**	**Additional information/ specification of the security measure that is in place**
Encryption of personal data		Ensure Laptops, back up drives and mobiles are encrypted
Access to personal data based on function	Yes	Secured with windows accounts and restricted to authorized staff
Regular check of the correct authorization	Yes	Annual audit of accounts
Data is stored physically and digitally and locked	Yes	Digital data is secured on server
Systems are secured automatically in the case of an incident.	Yes	Anti-virus is installed on the servers and PCs. Anti-malware installed on PCs. Secure password and lockout policy in place on accounts
Creating back-ups in a secured environment	Yes	Backup are completed to secure device and then uploaded to secure datacentre in the cloud
Secured connection with internet or other systems	Yes	Line is secure and traffic to and from the email server is encrypted, Firewall in place

In case of data breach detection

- Found that person or persons have accessed personal data without prior approval
- Data has been copied from servers without prior approval
- Outside breach of security measures

The breach needs to be reported to the Financial Director who will determine the severity of the breach and whether the ICO needs to be informed. Data shall be restored from the backup in the event of data loss.

Monitoring

Everyone must observe this policy. The Financial Director has overall responsibility for this policy who will monitor it regularly to make sure it is being adhered to. Annual audits of staff's access to data will be carried out and overseen by the Financial Director.

4. Policy Compliance

Hatch Mansfield takes compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the Financial Director.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Definitions

Business purposes	The purposes for which personal data may be used by us: Personnel, administrative, financial, regulatory, payroll and business development purposes. Business purposes include the following: - Compliance with our legal, regulatory and corporate governance obligations and good practice - Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests - Ensuring business policies are adhered to (such as policies covering email and internet use) - Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking - Investigating complaints - Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments - Monitoring staff conduct, disciplinary matters - Marketing our business - Improving services

Personal data	Information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, clients, suppliers and marketing contacts.

	Personal data we gather may include: individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.
Sensitive personal data	Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings—any use of sensitive personal data should be strictly controlled in accordance with this policy.