LHCM Ltd ("LHCM") Data Protection Policy Statement

8th March 2024

LHCM LTD ("LHCM") committed to maintaining full compliance with data protection laws. This Data Protection Policy ("Policy") applies to LHCM's operations and is based on General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, including as amended and applicable in the United Kingdom as a result of the European Union (Withdrawal) Act 2018 ("GDPR"), the Data Protection Act 2018 and any related guidance provided by the Information Commissioner's Office or any other competent authority. Ensuring data protection is the foundation of trustworthy business relationships and is the cornerstone of LHCM's reputation.

LHCM would like to inform you that your privacy on the internet is of the utmost importance to us. The success of our business depends on our ability to maintain the trust of our clients. During the course of our business, we gather information about our clients and users, and we would like to inform you about the type of information we gather, what we do with it and how you can correct or modify the information you entrust us with.

1. Scope

This Policy applies to LHCM and its employees. The Policy extends to all processing of personal data, relating to an identified or identifiable person. Anonymised or pseudonymised data, e.g. for statistical evaluations or studies, is not subject to this Policy.

Additional data protection policies can be created at LHCM's discretion, in compliance with the GDPR and applicable laws and regulations. This Policy can be amended in coordination with LHCM's Data Protection Officer (the "DPO"). The DPO's contact details and the latest version of this Policy can be found on LHCM's website https://lhcm.uk.

2. Principles for Processing

All processing carried out by LHCM or its employees shall be carried out in accordance with the principles

enshrined in the GDPR, being the following:

2.1. Fairness and lawfulness

When processing personal data, the individual rights of the data subjects must be protected. Personal data must be collected and processed in a legal and fair manner.

2.2. Purpose Limitation

Personal data can be processed only for the purpose/s set out prior to the collection of the personal data. Subsequent changes to the purpose/s are only possible to limited extent and require the specific consent of the data subject in each case.

2.3. Transparency

The data subject must be informed about how their data is being handled. Generally, personal data must be collected directly from the individual concerned. When the data is collected, the data subject must either be aware of, or informed of:

- The identity of the Data Controller and the DPO;
- Purposes and legal basis for processing;
- Retention period;
- Third parties or categories of third parties to whom the data might be transmitted;
- The rights of the data subject;
- Whether there is a statutory or contractual requirement to provide the data and the consequences of not providing the data;
- Details of data transfers outside the UK and EEA and how such will be protected;
- Existence of any automated decision taking;
- Source of data, where this is not obtained from the data subject.

2.4. Data minimisation

Processing of data takes place only to the extent that it is necessary in order to achieve the purpose for which processing is undertaken. Where the purpose allows and where the expense involved is proportional to the goal pursued, anonymised, pseudonymised or statistical data must be used. Personal data may not be collected in advance and stored for potential future purposes unless required or permitted by law.

2.5. Storage Limitation & Deletion

Personal data that is no longer needed after the expiration of legal or business process-related periods must be deleted. There may be an indication of interests that merit protection, retention or historical significance of this data in individual cases. If so, the data must remain on file until the interests that merit protection have been clarified legally to determine whether it must be retained.

2.6. Factual accuracy

Personal data processed must be correct, complete, and – if necessary – kept up-to-date. Suitable steps must be taken to ensure that inaccurate or incomplete data is deleted, corrected, supplemented or updated.

2.7. Confidentiality and integrity of Personal Data

Personal data is subject to data secrecy. It must be treated as confidential on a personal level and secured with suitable organisational and technical safeguards intended to prevent unauthorised access, illegal processing or distribution, as well as to protect against accidental loss, modification or destruction.

2.8. Accountability

LHCM will not only adhere to these principles but will also implement strong technical and organisational measures to be able to demonstrate compliance with such principles.

3. Reliability of data processing

Processing personal data is permitted only under the following legal bases - One of these legal bases is also required if the purpose of processing personal data is to be changed from the original purpose.

3.1. Customer data

3.1.1. Processing connected to contractual relationships:

- Personal data of clients can be processed in order to establish, execute and terminate a contract;
- Prior to a contract – during the contract initiation phase – personal data can be processed to prepare contracts, to fulfil regulatory obligations or to fulfil other requests of the prospective client that relate to contract conclusion;
- Prospective clients can be contacted during the contract preparation process using the information that they have provided. Any restrictions requested by the prospective clients must be complied with, unless necessary for the preparation of the contract or contractual relationship.

For advertising measures, LHCM must observe the requirements under the next sub-article;

- If the data subject contacts LHCM to request information (e.g. request to receive information material about a product), data processing to meet this request is permitted.

3.1.2. Data processing for advertising purposes:

- Personal data can be processed for advertising purposes or market and opinion research, provided that this is consistent with the purpose for which the data was originally collected;
- The data subject must be informed about the use of their data for advertising purposes;
- If data is collected only for advertising purposes, the disclosure from the data subject is voluntary. The data subject shall be informed that providing data for this purpose is voluntary;
- When communicating with the data subject, consent shall be obtained from such data subject in order to process the data for advertising purposes;
- When giving consent, the data subject should be given a choice among available forms of contact such as regular mail, e-mail and phone;
- If the data subject refuses the use of their data for advertising purposes, it can no longer be used for these purposes and data must be blocked from use for such purposes;
- Any other restrictions from specific countries regarding the use of data for advertising purposes must be observed.

3.1.3. Consent to data processing:

- Data can be processed following consent by the data subject;
- Before giving consent, the data subject must be informed in accordance with 3.3. of this Policy;
- The declaration of consent must be obtained in writing or electronically for the purposes of documentation;
- The granting of consent must be documented.

3.1.4. Data processing pursuant to legal authorisation:

- The processing of personal data is also permitted if legislation requests, requires or allows this;
- The type and extent of data processing must comply with the relevant statutory provisions.

3.1.5. Data processing pursuant to legitimate interest:

- Personal data can also be processed if it is necessary for LHCM's legitimate interests. Legitimate interests are generally of a legal or commercial nature;

- Before data is processed, it is necessary to determine whether there are any data subject interests that merit protection and whether these override LHCM's legitimate interests.

3.1.6. Processing of sensitive data:

- Sensitive personal data can be processed only if the law requires it or the data subject has given explicit consent;
- This data can also be processed if it is mandatory for asserting, exercising or defending legal claims in relation to the data subject;
- If there are plans to process sensitive data, the DPO must be informed in advance and must authorise such.

3.1.7. Automated individual decisions:

- Automated processing of personal data that is used to evaluate certain aspects (e.g. creditworthiness) cannot be the sole basis for decisions that have negative legal consequences or which could significantly impair the data subject;
- The data subject must be informed of the facts and results of automated individual decisions and must be provided with the possibility to respond and obtain human intervention;
- To avoid erroneous decisions, a test and plausibility check must be made by an employee.

3.1.8. User data and internet:

- If personal data is collected, processed and used on websites or in software, the data subjects must be informed of this and, if applicable, given information regarding cookies;
- Any cookie information must be integrated so that it is easy to identify, directly accessible and consistently available to the data subjects;
- If user profiles (tracking) are created to evaluate the use of websites and software, the data subjects must always be informed accordingly;
- Personal tracking may only be effected if it is permitted under the applicable law or upon obtaining the consent of the data subject;
- If tracking uses a pseudonym, the data subject should be given the chance to opt out in the privacy statement.

3.2. Employee data

3.2.1. Data processing before and during employment relationship:

- During an employment relationship between LHCM and one of its employees or prospective employees, personal data can be processed if needed to initiate, carry out and terminate the employment agreement;
- When initiating an employment relationship, applicants' personal data can be processed. If the applicant is rejected, their data must be deleted in observance of the required retention period, unless the applicant explicitly agrees to remain on file for any future selection processes;
- For the duration of an employment relationship, processing must always relate to the purpose of the employment agreement if none of the following circumstances for authorised data processing apply;
- If it should be necessary during the application procedure to collect information on an applicant from a third party, the requirements of the corresponding legislation have to be observed;
- In cases of doubt, consent must be obtained from the data subject;
- There must be legal authorisation to process personal data that is related to the employment relationship but was not originally part of the performance of the employment agreement. This can include legal requirements, collective regulations with employee representatives, consent of the employee, or LHCM's legitimate interests.

3.2.2. Data processing pursuant to legal authorisation:

- The processing of personal employee data is also permitted if the applicable law requests, requires, allows or authorises it;
- The type and extent of data processing must be necessary for the legally authorised data processing activity and must comply with the relevant statutory provisions;
- If there is some degree of flexibility afforded, the interests of the employee that merit protection must be taken into consideration.

3.2.3. Collective agreements on data processing:

- If a data processing activity exceeds the purposes intended for the fulfilment of a contract, it may be permissible if authorised through a collective agreement;
- Collective agreements are pay scale agreements or agreements between employers and employee representatives, within the scope allowed under the employment law;
- The agreements must cover the specific purpose of the intended data processing activity and must be drawn up within the parameters of the applicable data protection law.

3.2.4. Consent to data processing:

- Employee data can be processed upon consent of the employee concerned;
- Declarations of consent must be submitted voluntarily. Involuntary consent is void;
- The declaration of consent must be obtained in writing or electronically for the purposes of documentation;
- Before giving consent, the data subject must be informed in accordance with this Policy.

3.2.5. Data processing pursuant to legitimate interests:

- Personal data can also be processed if it is necessary to enforce LHCM's legitimate interests which are generally of a legal or financial nature;
- Personal data may not be processed based on a legitimate interest if, in individual cases, there is evidence that the interests of the employee merit protection;
- Before data is processed, it must be determined whether there are interests that merit protection which override LHCM's legitimate interests;
- Control measures that require processing of employee data can be taken only if there is a legal obligation to do so or there is a legitimate reason. Even if there is a legitimate reason, the proportionality of the control measure must also be examined;
- The justified interests of the company in performing the control measure (e.g. compliance with legal provisions and internal company rules) must be weighed against any interests meriting protection that the employee affected by the measure may have in its exclusion and cannot be performed unless appropriate;
- LHCM's legitimate interests and any interests of the employee meriting protection must be identified and documented before any measures are taken. Moreover, any additional requirements under the applicable law must be taken into account.

3.2.6. Processing of sensitive data:

- Sensitive personal data can be processed only under certain conditions;
- Sensitive data is data about racial and ethnic origin, political beliefs, religious or philosophical beliefs, union membership, health and sexual life, genetic data and biometric data of the data subject. Under the applicable law, further data categories can be considered as sensitive. Moreover, data that relates to a crime can often be processed only under special requirements under the applicable law;
- The processing must be expressly permitted or prescribed under the applicable law. Additionally,

processing can be permitted if it is necessary for the responsible authority to fulfil its rights and duties in the area of employment law;

- The employee can also expressly and explicitly consent to processing of such data;
- If there are plans to process sensitive data, the DPO must be informed in advance and must decide whether to authorise such.

3.2.7. Automated decisions:

- If personal data is processed automatically as part of the employment relationship, and specific personal details are evaluated (e.g. as part of personnel selection or the evaluation of skills profiles), this automatic processing cannot be the sole basis for decisions that would have negative consequences or significant problems for the affected employee;
- To avoid erroneous decisions, the automated process must ensure that a natural person evaluates the content of the situation, and that this evaluation is the ultimate basis for the decision;
- The data subject must also be informed of the facts and results of automated individual decisions and must be provided with the possibility to respond.

3.2.8. Telecommunications and internet:

- Telephone, e-mail addresses, intranet and internet along with internal social networks are provided by LHCM primarily for work-related assignments. They are a tool and a company resource. They can be used within the applicable legal regulations and internal company policies;
- In the event of authorised use for private purposes, the laws on secrecy of telecommunications and the relevant telecommunication laws must be observed rigorously if applicable;
- There will be general monitoring of telephone and e-mail communications or intranet/internet use. Employees will be notified of such monitoring prior to being employed;
- To defend against attacks on the IT infrastructure or individual users, protective measures can be implemented for the connections to LHCM's network that block technically harmful content or that analyse the attack patterns;
- For security reasons, the use of telephone equipment, e-mail addresses, the intranet/internet and internal social networks can be logged for a temporary period;
- Evaluations of this data from a specific person can be made only in a concrete, justified case of suspected violations of law or LHCM policies;
- The evaluations must ensure that the principle of proportionality is met. The relevant applicable law must be observed in the same manner as LHCM policies and regulations.

4. Use of cookies

LHCM uses cookies to collect information. Cookies are small data files that a website stores on one's computer hard disk for the purpose of keeping records when one visits a website, thereby acting as the website's memory for such visitor, and thus optimising such visitor's experience.

Cookies enable comfort of use, for example by remembering one's login credentials and viewing preferences, thus allowing one to visit "member-only" sections of the website without the need to re-register on each visit.

Furthermore, cookies are used by LHCM to measure activity on the website and make improvements and updates.

LHCM does not use cookies to retrieve information which was not originally sent in a cookie.

5. Disclosure of Data

LHCM's employees, directors, officers and representatives are obliged by law to treat client or user data as confidential and may not pass on or use any of such data without valid legal grounds.

Any personal data benefits from this full protection and will only be disclosed to third parties such as administrative or judicial authorities if LHCM is compelled to do so pursuant to applicable law, or if one has given written consent to such disclosure. One may revoke such consent or modify its extent at any time.

Without prejudice to the above, LHCM can disclose the following information:

- General client data, such as name, address and personal registration number, to companies carrying out administrative and back-office related tasks for LHCM;
- General client data about corporate clients to financial institutions subject to professional secrecy, for the purpose of marketing and advisory services;
- Client data, as determined by LHCM's Terms of Business.

6. Transmission of Personal Data

Transmission of personal data to recipients by LHCM, both internally or externally, is subject to the authorisation requirements for processing personal data under this section. The data recipient must be required to use the data only for the defined purposes.

In the event that data is transmitted to a recipient outside the UK or European Economic Area (EEA), the third country recipient must agree to maintain a data protection level equivalent to this Policy and to the protection sought by the GDPR, whichever is highest. Alternatively, the transfer may be subjected to protective measures outlined in the GDPR for subjecting such transfers to protection equivalent to that provided by the GDPR, such as standard contractual clauses.

In the event of claims of a violation, LHCM, conjointly with the DPO must investigate, document and communicate to the data subject whether the LHCM has violated this Policy or otherwise.

7. Contract Data Processing

Data processing on Behalf means that a provider is hired or contracted to process personal data, without being assigned responsibility for the related business process. In these cases, a compliant processing agreement must be concluded with external providers and LHCM. LHCM retains full responsibility for correct performance of data processing. The provider can only process personal data as directed or instructed by LHCM or its employees. When issuing directions or instructions, the following requirements must be complied with:

- The provider must be chosen based on its ability to cover the required technical and organisational protective measures.
- The directions or instructions must be placed in writing. The instructions on data processing and the responsibilities of LHCM and the provider must be documented.
- The contractual standards for data protection provided by the DPO must be considered.
- Before data processing begins, LHCM or its employees must be confident that the provider will comply with the duties. A provider must document its compliance with data security requirements, such as by presenting suitable certification. Depending on the risk of data processing, the reviews must be repeated on a regular basis during the contractual term.
- In the event of cross-border contract data processing, the relevant national requirements for disclosing personal data abroad must be met. In particular, personal data from the UK can be processed in a third country only if the provider can prove that it has a data protection standard equivalent to this Policy and the standards set out by the GDPR, whichever is highest.

Suitable tools can be:

a) Agreement on UK standard contract clauses for contract data processing in third countries with the provider and any subcontractors;

b) Participation of the provider in a certification system accredited by the UK for the provision of a

sufficient data protection level;

c) Acknowledgment of binding corporate rules (BCRs) of the provider to create a suitable level of data protection by the responsible supervisory authorities for data protection.

8. Data Subject Rights

Every data subject has the following rights. Their assertion is to be handled immediately by the responsible unit within LHCM, or alternatively by the DPO, and cannot pose any disadvantage to the data subject.

- The data subject may request information as to which personal data relating to them has been stored, how the data was collected, and for what purpose. If there are further rights to view documents under the relevant employment laws, these will remain unaffected. Such information must be provided in a machine-readable format.
- If personal data is transmitted to third parties, information must be given about the identity of the recipient or the categories of recipients.
- If personal data is incorrect or incomplete, the data subject can demand that it shall be corrected, supplemented, or record additional statements.
- The data subject has an absolute right to object to the processing of their data for purposes of advertising or market or opinion research, in which case the data must be restricted from these types of uses.
- The data subject may request that their data be deleted or restricted if the processing of such data has no legal basis, or if the legal basis has ceased to apply. The same applies if the purpose behind the data processing has lapsed or ceased to be applicable for other reasons. Existing retention periods and conflicting interests meriting protection must be observed. Where processing is based on LHCM's legitimate interests and the data subject has requested it to be deleted, it shall be restricted until the grounds for processing are verified, and subsequently if no grounds are found for continued processing based on LHCM's legitimate interests, the data must be deleted.
- The data subject generally has a right to object to their data being processed, and this must be taken into account if the protection of their interests takes precedence over the interest of the data controller owing to a particular personal situation. This does not apply if alternative legal grounds for processing exist.
- A client or employee who has any questions or concerns in this regard can contact the DPO as indicated under Section 14.

9. Confidentiality of Processing

Personal data is subject to data secrecy. Any unauthorised collection, processing, or use of such data by employees is prohibited. Any data processing undertaken by an employee that has not been authorised as part of their legitimate duties is unauthorised. The "need to know" principle applies. Employees may have access to personal information only insofar as it is appropriate for the type and scope of task in question. This requires a careful breakdown and separation, as well as implementation, of roles and responsibilities. Employees are forbidden from using personal data for private or commercial purposes, to disclose it to unauthorised persons, or to make it available in any other way. Employees must be informed at the start of the employment relationship about the obligation to protect data secrecy and respect data protection law and this Policy. This obligation shall remain in force even after the termination of employment relationships. Any employee who does not comply with such, will be liable to a serious breach of their relative employment contract, and would thus be liable to immediate termination, save any other relevant action which may be vested in LHCM.

10. Processing Security

Personal data must be safeguarded from unauthorised access and unlawful processing or disclosure, as well as accidental loss, modification or destruction. This applies regardless of whether data is processed electronically or in paper form. Before the introduction of new methods of data processing, particularly new IT systems; technical and organisational measures to protect personal data must be defined and implemented. These measures must be based on the state of the art, the risks of processing, and the need to protect the data. The responsible department within LHCM must consult with technical staff and the DPO in order to identify the best way forward. The technical and organisational measures for protecting personal data must be adjusted and updated continuously in tandem with technical developments and organisational changes.

11. Data Protection Control

Compliance with this Policy and applicable law, particularly the GDPR, is checked regularly with data protection audits and other controls. The performance of these controls is the responsibility of the DPO, or any external auditors hired for these purposes. LHCM's Board of Directors must be informed of the primary results as part of the related reporting duties. On request, the results of data protection controls will be made available to the responsible data protection authority. The responsible data protection authority can perform its own controls of compliance with the law and this Policy, as permitted under the applicable law.

12. Data protection incidents

All employees must immediately inform their supervisor and the DPO about cases of violations or suspected violations of this Policy or applicable data protection law (data protection incidents).

In cases of improper transmission of personal data to third parties, improper access by third parties to personal data ("Security Breaches"), or loss of personal data, the required company reports (an "Information Security Incident Report") must be made immediately so that any reporting duties under the applicable law can be complied with.

13. Responsibilities and Sanctions

LHCM's executive bodies are responsible for data processing in their area of responsibility. Therefore, they are required to ensure that the legal requirements, and those contained within this Policy, for data protection are met. Management staff are responsible for ensuring that organisational, HR, and technical measures are in place so that any data processing is carried out in accordance with data protection law and policy. Compliance with these requirements is the responsibility of the relevant employees. If official agencies perform data protection controls, the DPO must be informed immediately.

The DPO is the contact person on site responsible for data protection. The DPO must perform checks and must familiarise employees with the content of data protection law and policies. The relevant management is required to assist the DPO with these efforts. The departments responsible for business processes and projects must inform the DPO in good time about new or foreseen processing activities of personal data. The DPO must be informed before processing begins. Management and departmental heads must ensure that employees are sufficiently trained in data protection. Improper processing of personal data, or other violations of the data protection laws, can be criminally prosecuted and result in claims for compensation or damages. Violations for which individual employees are responsible can lead to sanctions.

14. Data Protection Officer (the "DPO")

The Data Protection Officer (the "DPO"), must be internally independent of professional orders, work towards compliance with the applicable data protection regulations, and with this Policy and must furthermore supervise its compliance. The DPO is appointed by the LHCM Board of Directors. Specific exceptions to data protection must be agreed with the DPO. Any employee shall promptly inform the DPO of any data protection risks, breaches or any other issues relevant to data protection. Any data subject may approach the DPO, at any time to raise concerns, ask questions, request information or make complaints relating to data protection

or data security issues. If requested, concerns and complaints will be handled confidentially. Decisions made by the DPO to remedy data protection breaches must be upheld by LHCM. Inquiries by supervisory authorities must always be reported to the DPO.

The DPO may be contacted as follows:

LHCM LTD,
Data Protection Officer,
30 Churchill Place, London,
England, E14 5RE,
United Kingdom
dpo@lhcm.uk

15. Information Commissioner's Officer

If the data subject not satisfied with the response of the DPO, they have the right to complain to the Information Commissioner's Officer, an independent UK authority that has been set up to uphold information rights. Further details and contact information of the Information Commissioner's Officer can be found on its website at https://ico.org.uk.

Definitions

- **Data is anonymised** if personal identity can never be traced by anyone, or if the personal identity could be recreated only with an unreasonable amount of time, expense and labour.
- **Data is pseudonymised** by identifying fields within a database which could lead to the identification of a natural person and replacing them with pseudonyms, with the purpose of rendering the relevant data as data which is not personal.
- **Consent** is the voluntary, legally binding agreement to data processing.
- **Data protection incidents** are all events where there is justified suspicion that personal data is being illegally captured, collected, modified, copied, transmitted or used. This can pertain to actions by third parties or employees.
- **Data subject** under this Policy is any natural person whose data can be processed.
- **The European Economic Area (EEA)** is an economic region associated with the EU, and includes Norway, Iceland and Liechtenstein.

- **Sensitive data** is data about racial and ethnic origin, political opinions, religious or philosophical beliefs, union membership or the health and sexual life of the data subject. Under the applicable law, further data categories can be considered highly sensitive or the content of the data categories can be structured differently. Moreover, data that relates to a crime can often be processed only under special requirements under the applicable law.
- **Personal data** is all information about certain or identifiable natural persons. A person is identifiable for instance if the personal relationship can be determined using a combination of information with even incidental additional knowledge.
- **Processing personal data** means any process, with or without the use of automated systems, to collect, store, organise, retain, modify, query, use, forward, transmit, disseminate or combine and compare data. This also includes disposing of, deleting and blocking data and data storage media. As a general rule, any use of personal data is considered as processing of such personal data.
- **Client** is any natural person who receives any service whatsoever from LHCM.
- **Third countries** under this Policy are all countries outside the UK.
- **Transmission** is all disclosure of protected data by the responsible entity to third parties.