CEI GLOBAL UK LIMITED ("CEI")

DATA HANDLING GUIDELINES

THE SCOPE OF THESE GUIDELINES

- These guidelines (the "**Guidelines**") cover your confidentiality and data handling obligations as Staff of CEI, particularly in the context of data privacy requirements in Europe. The EU General Data Protection Regulation (the "**GDPR**") is a European law applying across Europe from Friday 25 May 2018.

- The GDPR places obligations on organisations with regards to how they must handle EU personal data.

- This Employee Guide is intended to provide guidance to CEI employees in relation to CEI's legal obligations with respect to handling EU personal data. It will be applicable to all business functions as most business functions will process EU personal data at some point in the customer journey.

- All Staff are required to comply with both the spirit and the letter of these Guidelines (and any other policies and documents referred to in it). Subject to applicable law, failure to comply with these Guidelines may lead to disciplinary action up to and including termination of employment in accordance with applicable policies, procedures and works rules.

- These Guidelines replace and supersede any previous guidelines addressing the same or similar issues, whether formal or informal. CEI reserves the right in its absolute discretion to alter, amend or terminate these Guidelines in whole or in part at any time with or without notice. The applicable version of these Guidelines will be maintained on in CEI's UK policies folder. You should always check that you are referring to the latest version of these Guidelines if you have previously downloaded hard copies of these Guidelines.

- Whilst these Guidelines have been designed to address most situations encountered in the workplace, scenarios may arise that are not covered by these Guidelines. Any questions regarding matters not covered by these Guidelines, including whether a contemplated use or action is permitted under the terms of these Guidelines should be addressed to the CEI Operations team.

TERMINOLOGY

The below key terminology used throughout these Guidelines mean the following:

- "**Communications**" includes, without limitation, emails, instant messages, voicemail messages and text messages (or equivalent), app-based messaging (such as WhatsApp), phone calls, social media posts (including on LinkedIn), and any other form of electronic or telecoms communication.

- "**Devices**" includes landline phones at CEI's offices, mobile phones, BlackBerry devices, SIM cards, desktop computers, tablets, laptops, cameras provided to Staff by CEI [and any other such devices used by Staff on a 'Bring Your Own Device' basis ("**BYO devices**")].

- "**CEI Information**" means information created by, distributed with, or stored on, the Systems, together with hard copy documents created by, provided to, or which otherwise come into the possession of, Staff in the course of their employment with CEI which belongs or relates to the business of CEI and/or its actual or prospective clients, suppliers and Staff.

- "**Staff**" includes employees and interns engaged directly in the business of CEI as well as certain other workers engaged in the business of providing services to CEI (even though they are not classed as employees), to the extent that they have access to the Systems. Any references to "employment" and "contract of employment" in these Guidelines should

be interpreted accordingly.

- "**Systems**" include telephone, computer, internet and Wi-Fi systems, software and portals, accounts and/or networks belonging, controlled or used by CEI that are used to transmit, undertake and/or receive Communications or are otherwise used in the course of CEI's business, including any CRM systems.

YOUR CONFIDENTIALITY AND DATA HANDLING OBLIGATIONS

Your confidentiality obligations

- CEI Information is CEI's property. All Staff owe CEI an extensive duty of confidentiality via their contracts of employment and at law. Staff are individually responsible for any and all CEI Information in their control and must ensure that all CEI Information is kept secure and confidential at all times in the course of their employment. Staff must immediately report any actual or suspected loss of any CEI Information and/or any actual or anticipated breach of these confidentiality obligations to the Chief Operating Officer (COO). It is imperative that any suspicion of a breach, or actual breach, of data security, confidentiality, or any other loss of data or CEI Information is reported in this way as a matter of urgency – often swift action can make the difference between a matter being resolved satisfactorily and an unacceptable incident occurring.

- At any point during your employment with CEI and/or at its termination, subject to applicable law, you shall submit any personal computer and/or mobile device (and any and all backups of such computer and/or mobile device) which is used for business purposes (for example, to access CEI resources and Systems) to CEI's IT team to be reviewed, for wiping of CEI Information and for software removal. You must provide all necessary co-operation and assistance to CEI's IT team in relation to this process.

- Staff are prohibited from copying CEI Information to outside sources, including, without limitation, the emailing of CEI Information to outside email accounts (including your own personal email accounts), uploading it to cloud-based storage areas not managed by CEI or copying the data onto a portable storage device without the permission of the COO. Where the COO provides you with permission to copy data onto a portable storage device, that device must be suitably encrypted. Personal devices such as all personal telephones should never be used to store CEI Information on (including, for example, storing business-related information, or photographing CEI Information whether for quick reference or otherwise). BYO devices are the exception to this, on condition that all CEI Information is stored strictly in accordance with the terms of these Guidelines and the BYOD Policy in place from time to time.

- CEI Information should not be removed from or accessed outside of CEI's premises without the prior consent of the COO and in accordance with CEI's applicable policies. If Staff require remote access to CEI Information, CEI will provide this through secure means, where appropriate.

- CEI Information should not be divulged improperly to individuals who are not authorised to receive it. Highly confidential information, sensitive customer, or Staff information must be password protected using appropriate password protection before being sent out via email or the internet. Any queries with respect to what information can be sent should be discussed with your line manager before any information is released.

Personal data in the context of CEI Information

- Some CEI Information contains personal data. Personal data include all information that relates to a living individual who can be identified from them and includes expressions of opinion and indications of intentions with regard to that individual. Contact information for individuals falls within this concept. Personal data also include any expression of opinion

about an individual, for example between Staff and external individuals in emails or instant messages.

Why is it important to look after personal data?

- Processing personal data incorrectly or inappropriately (e.g. by sending an individual's personal data to the wrong person(s), allowing unauthorised persons access to personal data, or transferring or using data for purposes in a way which is not consistent with CEI's legal bases for processing) may give rise to a claim against CEI, a complaint from the individual whose data it is and/or correspondence from the relevant data protection regulator in the Member State where the individual is located. Should you receive any such communication, you should forward it immediately to CEI's Legal Counsel.

- In addition, under the General Data Protection Regulation (the "**GDPR**") and local laws implementing its terms, data protection regulators have the power to levy extremely significant fines. Therefore, a breach of the requirements of the legislation carries not only a significant reputational risk for CEI, but also a potentially extremely large fine.

- Under applicable data protection law, in certain instances, inappropriate processing of personal data by an individual can also potentially amount to a crime and render that individual subject to criminal prosecution.

How should Staff be looking after personal data?

- The GDPR sets out a number of principles regarding how personal data should be processed in order to protect it. Note that when we talk about "processing", this is a very wide concept which includes for example obtaining, recording, storing or holding information or data or carrying out any operation including organisation, retrieval, use, disclosure, erasure or destruction of data.

- Below is a summary of the GDPR's data protection principles along with what they mean for how you should handle personal data and how we as an organisation are complying with them:

1. Personal data should be processed lawfully, fairly and in a transparent manner in relation to the data subject

- In plain English, this means that we must have a legal basis to process personal data, be that of our end users or simply individuals who browse our website. A simple example of a legal basis that we may rely on is that we need to process end user bank details in order to pay individuals who have won e-sports tournaments.

- If you have any questions about the legal bases that we rely on to process personal data, please read CEI's Privacy Policy (available on our website), or get in touch with our Legal team.

- The GDPR explains that controllers (i.e. organisations that decide the purpose for which data are processed - in this case, CEI) must be transparent with individuals about how their data are processed. We inform individuals about this via our Privacy Policy.

2. Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

- In our privacy policy, we explain clearly to individuals the specific purposes for which their data will be processed, and how it will be processed. In the rare instances that we rely on

consent to process personal data, we separate out the different processing activities. This enables individuals to make an informed decision about what they are consenting to.

- If we want to use personal data for a purpose that is different to the one we collected it for, we make sure that we explain this new purpose to data subjects promptly, for example via updating the relevant privacy policy or contacting them.

3. Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

- This is called the 'data minimisation' principle and means that we should only collect data that is strictly necessary for the purpose(s) that we need it for.

4. Personal data processed by an organisation should be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay

- This places an obligation on us to ensure that all of the personal data that we process are kept up to date and accurate.

- In the event that you are notified of any changes to the personal information that end users have provided, including changes to their name, address, and bank details, you should ensure that the information on our systems is updated as soon as possible and the inaccurate data erased.

5. Personal data should be kept for no longer than is necessary for the purposes for which the personal data are processed

- CEI has systems and policies in place to ensure that data are not held for longer than is necessary for the purposes we need them for, unless we are subject to a legal requirement to hold the data for longer.
- It is imperative that you play your part in ensuring that we do not process personal data for longer than we need to by storing and accessing personal data only through the relevant system. That way, we can properly monitor the use of the data and when we last had meaningful contact. Locally stored information will not be subject to our ability to monitor appropriate data retention and could inadvertently place CEI in a position where it is in breach of the law. The same applies for hard copy documents. It is therefore prohibited for Staff to store data outside of the appropriate Systems and disciplinary action may be taken against Staff who fail to comply with this requirement in accordance with applicable policies, procedures and works rules.

6. Personal data should be processed in a manner that ensures appropriate security of the personal data using appropriate technical or organisational measures

- CEI has a number of technical security measures in place to safeguard the personal data that we process. However, it is also important that our Staff play an active role in protecting this personal data.

- Below is a non-exhaustive list of how Staff can help CEI to comply with this principle. Some of the advice is also applicable more generally to how Staff can help to protect CEI Information:

Do:

- Use email with care, particularly where emails contain personal data or sensitive personal data relating to individuals. You must password protect attachments that contain personal data;

- Check with your line manager when sending emails or documents containing personal data to third parties other than end users in the ordinary course of business, particularly those based overseas;
- Take care when sending personal data in the internal or external mail;
- Use only the appropriate Systems for storage, use and sending of any Staff data;
- In circumstances where we have contractual obligations to supply certain personal data to an end user, particularly on a regular basis, contact the COO, who will be able to advise on the best methods to be adopted;
- Report any data breaches immediately to the COO and CEI's Legal Cousel;
- Always attend all relevant data protection training sessions and updates;
- Immediately upload hard copy documents onto CEI's file system then dispose of them appropriately (see below);
- Bear in mind that destroying or disposing of personal data counts as processing, therefore care should be taken in ensuring the appropriate means of disposal of any personal data. In particular, any hard copy papers containing personal data (e.g. meeting notes) should be either shredded or placed into secure destruction bins after appropriate loading onto the Systems. Under no circumstances should documents containing personal data be placed in ordinary waste bins;
- Take care not to lose or leave any Devices unattended. For example, Devices should not be left in cars overnight; and
- Ensure Devices are securely locked when not being accessed by you.

Don't:

- Leave computer screens unlocked or files containing personal data unattended;
- Disclose passwords to any unauthorised Staff;
- Email end user data or other CEI Information to your personal email account or to an unauthorised third party account or otherwise up or download it in an unauthorised way;
- Mislead individuals about whether you intend to share their information and who you intend to share it with;
- Refer to personal data in conversations in public spaces or where there is a risk of it being overheard; and
- Store personal data outside of the appropriate Systems – locally saved information is not subject to appropriate safeguards.

Frequently asked data protection questions

What should I do if an individual requests copies of the information that CEI holds about them?

- Under the GDPR, individuals such as end users can make "data subject access requests" to organisations that they believe are processing their personal data. They are entitled to be provided with copies of all the personal data that the organisation processes on them. As noted above, this includes opinions. It is therefore crucial that any additional information that you record (e.g. contact centre notes) are objective and do not contain subjective, rude or discriminatory comments. This could prove embarrassing to both you and to CEI. You should also be aware that if you make coded comments about an individual, an explanation of what these mean may also have to be provided if a data subject access request is received. The timescale for complying with any such request is extremely short and therefore you must act immediately.

- If you receive such a request, you must immediately contact CEI's Legal Counsel and they will help deal with the request.

Do individuals have any other rights in relation to the personal data that CEI processes about them?

- In certain circumstances, individuals also have the right to request that their personal data that CEI processes are amended or erased, or that the processing of their personal data is restricted or stopped. If you receive such a request, please contact CEI's Legal Counsel via the contact details above without delay and they will deal with the request.

What should I do if I receive a request for copies of an individual's personal data from a third party?

- Unless the third party is an authorised recipient of the data and proper processes are followed, all requests, (written or verbal) should immediately be forwarded to CEI's Legal Counsel. This includes requests from organisations such as the police, tax and immigration authorities, and the individual's bank. **Under no circumstances should you provide any personal data directly to a third party in response to a request, even where the individual appears to have consented to the information being provided.**

OTHER RELEVANT POLICIES

- These Guidelines should be read in conjunction with all other applicable laws and procedures relevant to data protection and Systems use.