The East Room Ltd.
Data Protection Compliance Regulations
April 2019

1. Purpose of Data Protection Compliance Regulations

1.1 The purpose of these Compliance Regulations is to assist The East Room employees in adhering to the Company's Data Protection Policy and the Data Protection Acts (1988 & 2003). The Company's Data Protection Policy (available at www.eastroom.ie) and these Regulations affirm the Company's commitment to protecting the privacy rights of individuals in accordance with the Data Protection legislation. These Compliance Regulations set out a range of areas of work in which data protection issues arise and outline best practice that employees should follow.

PART 1: Explanation of Terms and Guidance on Data Protection Rules

2. Explanation of terms

- **Data**: information in a form that can be processed - includes both electronically held data and paper-based data;
- **Electronic/soft-copy data**: information held in an electronic format e.g. on computer, or information recorded with the intention that it be processed by computer;
- **Hard-copy data**: information that is recorded in paper format and is held as part of a relevant filing system or with the intention that it forms part of such a system;
- **Personal data**: data which relates to a living individual who is identifiable either from the data itself or from the data in conjunction with other information held by the Company. This can include one or more factors relating to a person's physical, physiological, mental, economic, cultural or social identity. The Acts also differentiate between 'personal data' and **'**sensitive personal data';
- **'Sensitive personal data** relates to a person's racial or ethnic origin; political opinions; religious or philosophical beliefs; physical and mental health; sexual life; criminal convictions; the alleged commission of an offence and trade union membership. The Data Protection Acts require that additional conditions be met for the processing of such data.
- **Data Subject**: an individual to whom personal data relates;
- **Data Controller**: a body that processes information about living people. The data controller must be in a position to control the contents and use of personal data and has overall responsibility for the privacy and security of that data at all times;
- **Data Processor**: a body that processes personal data on behalf of a data controller;

- **Processing**: the performing of any operation / set of operations on data, comprising:
  - obtaining, assembling, organising and storing data,
  - using, consulting and retrieving data,
  - altering, erasing and destroying data,
  - disclosing data.

3. Role of Data Protection Commissioner

3.1 The Data Protection Commissioner oversees compliance with the terms of the legislation. The Commissioner has a wide range of enforcement powers, including investigation of Company records and record-keeping practices. Should the Company be found guilty of an offence it can be fined up to €100,000 and/or may be ordered to delete data.

4. The Company's Obligations under Data Protection

4.1 As stated in the Company's Data Protection Policy, there are eight rules under data protection, which govern the processing of personal data. When processing personal data, whether in paper or electronic form, the following must apply at all times:

- Obtain and process the personal data fairly;
- Keep only for one or more specified, explicit & lawful purpose(s);
- Use and disclose only in ways compatible with the purpose(s) for which it was initially provided;
- Keep safe and secure;
- Keep accurate, complete and up-to-date;
- Ensure that it is adequate, relevant and not excessive;
- Retain for no longer than is necessary for the specified purpose(s);
- Provide a copy of his/her personal data to an individual, on request.

4.2 Obtain and process the data fairly:

- Personal data is obtained fairly if the data subject is aware of:
  - the purpose(s) for which the Company collects the data;
  - the categories of person/organisation to whom the data may be disclosed;
  - that some questions in forms may be optional;
  - the right of access to their data and their right of rectification of their data;
- Consent for the processing of personal data should be obtained from the data subject;
- **It is essential to obtain explicit consent for the processing of sensitive personal data by way of signature, opt-in box etc.**

4.3 Keep only for specified and lawful purpose(s);

- Personal data already collected for a specific purpose may not be used for further processing if the secondary purpose is not compatible with the original purpose.

4.4 Use and disclose only in ways compatible with the purposes for which it was initially given;

- Personal data should only be accessed in order to complete official functions of the Company;
- Personal data should only be disclosed to work colleagues where the data is required to fulfil an official function of the Company;
- Personal data must be kept confidentially and must never be discussed with/disclosed to any unauthorised third party, either internal or external to the Company without the prior consent of the data subject, except where there is a statutory obligation to do so (e.g. if required for the purpose of preventing, detecting or investigating offences, required urgently to prevent damage to health or serious loss/damage to property, required under law etc.);
- Personal data relating to a data subject must not be disclosed to any third party, even if they identify themselves as a parent, current/potential employer, professional body, sponsor, etc. Such disclosures must only be with the consent of the individual concerned. This includes requests for contact details (e.g. address, mobile phone number, etc);
- Where individuals (the data subjects) wish to discuss personal data relevant to themselves, the employee must confirm one or more facts that should be known only to the data subjects such as their date of birth, student number, mother's maiden name etc prior to any disclosure.

4.5 Keep safe and secure;

- Use and storage of personal data in electronic format must be subject to stringent controls (e.g. use of password protection, timed log-out of systems, encryption of PC folders and portable devices, regular backup, use of anonymisation software etc);
- Authorised users of personal data must ensure that personal data they have access to as part of their duties is kept securely at all times and is protected from inadvertent disclosure, loss, destruction, alteration or corruption;
- Personal data must not be stored or transported on unencrypted laptops, USB devices or other portable devices and every effort must be made to ensure the security of the encrypted devices (e.g. do not store a laptop in your car or allow unauthorised individuals to view computer screens displaying sensitive information);
- When upgrading/changing a PC, always ensure the contents of the hard drive of your old PC are irrevocably deleted by an authorised employee in the Information Technology Division (ITD) at the University of Limerick;
- Screens, printouts, documents, and files showing personal data must not be accessible to unauthorised persons;
- Personal data held in paper format must be stored securely in cabinets in locked rooms;

4.6 Keep accurate and up-to-date;

- Administrative procedures should include review and local audit facilities so that personal data is accurate, complete and kept up-to-date.

4.7 Ensure that it is adequate, relevant and not excessive;

- The personal data held by The East Room should be adequate to enable the Company achieve its purposes, and no more. Personal data must not be collected or held on a 'just in case' basis.

4.8 Retain for no longer than is necessary for the specified purpose/purposes;

- Personal data should be held for the periods specified in The East Room Records Management & Retention Policy (www.eastroom.ie). The retention and confidential destruction of personal data must be carried out in accordance with that policy.

4.9 Provide a copy of his/her personal data to an individual, on request.

- The Acts provide for the right of access by the data subject to his/her personal data. Where an access request is received, it should be directed to the Managing Director at The East Room **within a maximum of three days of receipt of the request** in order to enable the Company to comply with the entitlements of the requester within the timeframes specified in the Acts.

5. Employment References

5.1 Employment references received by the Company may be subject to a data protection access request and confidentiality vis-a-vis the individual to whom the reference relates cannot be guaranteed.

6. Use of Filming for company purposes etc.

6.1 Management and staff at the Company may use webcams/recording devices and cameras (e.g. for development of digital marketing tools). In such circumstances, consent should be obtained from individuals in advance of the commencement of recording; or an appropriate warning sign should be posted clearly within the area covered by the webcam/device. Care is required in order to prevent the unauthorised transfer of images of individuals (deemed personal data). In addition, recordings should only be retained for as long as is necessary after the purpose for undertaking recording has been fulfilled.

7. Responsibilities of data subjects

7.1 Employees, students and other data subjects are responsible for:

- ensuring that any information they provide to the Company is accurate and up to date;
- informing the Company of any changes of information that they have provided, such as changes of address etc.

8. Breaches of The East Room Data Protection Policy & Compliance Regulations

8.1 Breaches of the terms and conditions of this Policy and the Company's Data Protection Compliance Regulations (available at www.eastroom.ie) could result in major reputational and financial damage to the Company

9. Further information

9.1 These Regulations set out key areas of work at the Company where data protection issues may arise and outline best practice in dealing with them. However, it is not envisaged that these Regulations contain an exhaustive list of all areas of work to which Data Protection principles apply and employees should contact the, The East Room Ltd, University of Limerick (telephone 061 202186 email: eastroom@ul.ie) to obtain clarification where necessary.

9.2 Extensive information is also available from the Data Protection Commissioner's website, www.dataprotection.ie, or from the Office of the Data Protection Commissioner, Canal House, Station Road, Portarlington, Co. Laois.

10. Review

10.1 These Compliance Regulations will be reviewed regularly in light of any legislative changes.