European Hereditary Tumour Group

EHTG Security Measures

The European Hereditary Tumour Group's IT systems are safe and secure; we have fully assessed the likely risks associated with all of our processes that involve collection, storage, use and disposal of individual data.

Our key controls and security measures for keeping information secure involve:

- **Boundary firewall** to stop breaches.
- **Secure configuration** at EHTG is important, we regularly evaluate our devices to remove unused software and we regularly change software or hardware default passwords to reduce potential vulnerabilities.
- EHTG has a robust data **back-up strategy** in place in case of a disaster such as fire, flood or theft, making use of cloud facilities which our IT service provider facilitates on a fully EU GDPR compliant basis, with appropriate security measures in place.
- There is **restricted access control** to our system; all staff have individual username and password, and each has a personal account with appropriate permissions according to the job they undertake.
- Our Wi-Fi system has strong and unique passwords, one designated for personnel and a second one just for guests to our office.
- Passwords and other access are cancelled immediately after a staff member stops working at EHTG.
- Regarding **malware protection**, all our devices have anti-virus software, which is regularly scanned to ensure its effectiveness remains up to date. Our devices are regularly scanned, and the network and files are monitored to prevent or detect threats.
- **Patch management and software updates** are kept up to date at EHTG; all of our computer equipment is regularly maintained and kept up to required standards, along with software to maintain operational efficiency and counteract any security vulnerability.
- We ensure the same **security** levels on all **laptops** whilst away from the office, whether working remotely, or running an event. We have parallel security arrangements and agreements with third party companies that we work with.
- Data security sent by **email** is essential to our business operations. Therefore, we attached documents which are password-protected, with unique passwords for each event communicated/disclosed by telephone with the right person to provide a level of trust that the email has not been intercepted.
- Security through the **post** is equally important for us. We have a policy not to send personal data through the post; where this is unavoidable, we always send by first class registered post or by courier.
- EHTG has in place a **data protection training plan** for all new staff that start with the organisation and a continuous training programme to keep personnel up-to-date and aware of security measures and procedures they must follow in their daily tasks. In this way we protect ourselves from accidental disclosures, being responsible and trained to recognise threats, phishing emails, risks and maintaining a security-aware culture.
- All **our digital photography and video** recording of an event are transferred to a secure location and then deleted them from the CD/data stick or computer that originally delivered them.
- EHTG cares about **physical security at its office;** servers are stored in a dedicated room. Hard copy files required for accounting purposes are also stored in a separate room. Both rooms are locked and accessed by security code. General office access is protected with a security alarm system operating with a key-fob facility to identify who has opened and locked up the premises.

EHTG Secretariat: c/o Integrity International Events Ltd.
The Coach House, 7 St Alban's Road, Edinburgh EH9 2PA UK
Tel: +44 (0) 131 624 6040 e-mail: ehtg@integrity-events.com www.ehtg.org

- Our **Data retention** and **data disposal procedures** prevent us from keeping data longer than is necessary, along with out-of-date or inaccurate files. If we need to keep information for archive purposes, we make sure that it is moved to a more secure location to prevent its access from unauthorised personnel.

Last reviewed: 20th February 2018.