Wolfestone Holdings Data Protection and Security Regime

1. All data (including XTRF and XTM) is stored on servers located in secured room with controlled access in company HQ premises.
2. The network is protected by UTM firewall device.
3. Access to data:
   a. Vendors and clients:
      i. Main platform for file and data exchange is XTRF:
         1. XTRF Vendor and XTRF Client portals;
            a. Access via HTTPS secured using SHA-256 with RSA encryption.
      ii. File exchange using e-mail:
         1. Company uses email encryption on request of customer or vendor;
         2. All files containing personal data are sent to vendors or clients in archived format protected by a password;
         3. The password required to open the archived file is sent separately via text message.
      iii. XTM translation platform using XTRF interface:
         1. Vendors are using XTM as their main tool for translation;
         2. Vendors can access only content of the file in XTM in order to translate, not the file itself.
   b. Employees:
      i. Access rights:
         1. Access rights are controlled by Microsoft Group Policy Management;
         2. Employees are grouped based on necessity to access certain data relevant to the responsibilities described in job description.
      ii. Data storage:
         1. XTRF project management portal:
            a. Access via HTTPS secured using SHA-256 with RSA encryption.
         2. Remote drives:
            a. Access from local network secured by UTM firewall device, only by authorised personnel based on Microsoft Group Policy Management policies with differentiated access levels depending on access right relevant to the position;
            b. Controlled access from external networks secured by LogMeIn Hamachi VPN connection.
      iii. Access to company network:
         1. Only company devices have access to the company network;

2. Guests and private devices of employees can only connect to a network separated from company's network with no access to data in company network.

iv. Portable devices:

1. All company devices leaving company premises (laptops, mobile phones, tablets, etc.) are encrypted;
2. All private devices of employees that expressed consent to use their private devices for work purposes (i.e. remote work) are encrypted.

4. Data backup:

a. On-site backup device:

i. Data is retained for 6 years;
ii. After 6 years data is securely deleted.

b. Off-site, EU based data center:

i. Deleted files are retained for 12 months in the backup from the date of deletion;
ii. Data is retained for 6 years;
iii. After 6 years data is securely deleted.

c. Data is archived to on-site backup device after 12 months:

i. Archived data is retained for 6 years;
ii. After 6 years data is securely deleted.

d. E-mail backup:

i. We're are using Office365 as our e-mail platform and all emails are stored and archived on Microsoft servers;
ii. Microsoft assured their compliance with GDPR regulations (details: https://www.microsoft.com/en-us/TrustCenter/Privacy/gdpr/default.aspx);
iii. All emails are retained for 6 years;
iv. After 6 years emails are deleted and being a subject to Microsoft data retention policy which means data are securely deleted by overwriting.

e. Skype backup:

i. Skype, as a part of Microsoft portfolio companies, follows exactly the same regulations as Office365 and emails;
ii. We retain Skype conversations for 6 years;
iii. After 6 years, conversation is securely deleted.

5. Secure data deletion:

a. Data qualified for secure deletion (either after 6 years period of retention or in case there is no longer legitimate reason for keeping data) is overwritten with not less than 24 overwriting cycles using Recuva software.