Version 1		
05/11/2019		
Page 1 of 1		
D&D-11-015		
Data Protection Policy		
Approved by:	Agreed by:	Issued by:
J. Managing Director	DPO	Managing Director

The Company is committed to full compliance with the requirements of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).

Personal data is any information that relates to a living individual and includes physical and digital data. Personal data shall only be:

1. Handled, accessed and processed fairly and lawfully by those with specific authority to do so in accordance with the Company procedures;
2. Stored in locations specifically designated for that purpose and in no other place;
3. Processed and/or transmitted in accordance with (a) lawful requirements and/or (b) the consent given by the individual to whom the personal data relates. Personal data shall not be used for any other purpose;
4. Kept for as long as necessary and as long as is permitted by the Company procedures and legislation requirements. All originals and copies of the personal data information shall then be erased and/or deleted;
5. Transferred to any other party not bound by the Company's Management System only when such a transfer is explicitly permitted by the Company's procedures and only on the provision that the recipient confirms prior to receipt, that the personal data will be handled pursuant to the Company requirements and/or the GDPR procedures.

In addition, the company shall implement the principles of:
1. Data minimization: Data collected on a subject should be adequate, relevant and limited to what is *necessary in relation to the purposes for which they are processed.*
2. Data Accuracy: Data must be accurate and where necessary kept up to date.

As part of reporting obligations, all employees are required to report to their Line Manager or Data Protection Officer (DPO), on becoming aware of any:

1. Loss of personal data, whether originals or copies, including (a) documents, (b) computers and portable devices and/or (c) media containing personal data;
2. Unauthorized access to personal data;
3. Use of personal data for a purpose other than the reason for which consent has been given;
4. Personal data that is stored in a place other than its designated location;
5. Accidental release or loss of data either within the Company or outside of the Company;
6. Malicious program that infects any (a) computer, (b) portable device and/or media on which personal data is stored or processed;
7. Personal data that is not properly secured;
8. Personal data becoming available in the public domain.

Detailed information and guidance on Company's procedures in dealing with GDPR can be found on Company's GDPR related procedures that are part of the company's Management System.