# Description of the Technical and Organisational Measures concerning GDPR

## 1 Confidentiality

1.1 Access Control (Physical Access)

- Server Room and Racks that hold servers and switches are locked
- Access to this Server Room and Racks is limited to IT Staff
- Offsite Backup Server is located in an external location. The Server Room is locked and also limited to IT Staff

1.2 Access Control (System Authorisation)

- Data is transferred via Secure FTP or a dedicated mail address (mailings@albedecoker.com)
- The storage locations are encrypted and have file auditing enabled
- Access to the storage locations is limited to authorized users only

1.3 Access Control (Data Authorisation)

- Data is stored in a dedicated place on multiple servers
- The folders on these servers have encryption, file auditing and user control access enabled
- Files containing personal information will be kept on the servers for the time needed to complete the assignment.
- After completion of the assignment these files will be deleted.

1.4 Purpose of Use Control

- Data files will be split in different files that can only be combined by using a unique identifier
- The files will be spread over multiple servers, this ensures that personal data can't be linked to a natural person in case of a data breach

1.5 Pseudonymisation

- Because data files are split en spread over multiple servers it will be impossible to link personal data to an identifiable natural person

## 2 Integrity

2.1 Disclosure Control

- The use of USB devices is blocked by our security policy
- All internal data transfers are encrypted and logged
- Only employees authorized to process personal data can access the files

2.2 Input Control

- All folders that contain personal data have File Auditing enabled

## 3 Availability

3.1 Availability Control

- All Files containing personal data are backed up to a secure server in an offline location
- This server also has encryption and file auditing enabled
- This server is replicated to tapes that are kept in a vault

3.2 Restoration in a Timely Manner

- Data can be restored from the offsite backup server after authorization from IT Staff

## 4 Process for Regularly Testing, Assessing and Evaluating

4.1 Data Protection Management, Incident Response Management, Privacy by Default Settings

- There is a monthly evaluation of the security procedures in place

4.2 Job Control

- We will only work with GDPR compliant subcontractors