ANNEX A: Technical and organisational security measures

Access Controls: Administrative access to our production environment is limited to a restricted number of individuals. Access to additional individuals is given only in extreme circumstances, for a specific purpose, and is limited in duration. Such access to these additional individuals is given only after the explicit approval of the security team User access is based upon termination and evaluated on a quarterly basis.

Physical and Environmental Security: General access to the office is controlled by the use of a card access system. Access to controlled areas is restricted through the use of card access and/or additional verification. All individuals without authorized access to the controlled areas must sign in and be escorted by an individual with approved controlled area access.

Application Security: Data importer has developed and implemented a strict, secure development program, based on Open Web Application Security Project (OWASP), and Microsoft Security Development Lifecycle. From the earliest phases of product design and planning, the security team takes an active role in how our products are built. Following completion, sensitive product developments are tested to ensure that application security has been thoroughly and properly addressed.

Vulnerability monitoring through penetration testing: Data importer performs at least two annual Information Security penetration tests, which are conducted by accredited and completely independent information security companies. Vulnerabilities, if found, are addressed as part of our Risk Management Policy. Dataweavers performs vulnerability assessment scanning using third-party tools at least twice a month, and after any major infrastructure change in our production environment.

Data transfer security: Data transferred to data importer through its services are encrypted in transit by default on all supporting browsers. In addition, data recorded on HTTPS pages is fully encrypted and transferred to servers over an encrypted connection.

Networks security: Dataweavers implements multiple and varied infrastructure security measures to protect customer information from unauthorized access, loss, alteration, viruses, Trojans and other similar harmful code. This includes:

- Timely and regular updates of operating systems, hardware, and any third-party software to avoid security vulnerabilities. Critical updates are deployed within one week from release on corporate as well as production systems.
- Use of firewalls and Intrusion Prevention Systems (IPS) systems to limit access and protect Dataweavers application and infrastructure services.
- Hardening of all external-facing servers according to industry best practices.
- Implementing anti-malware controls to prevent entry of malicious software.
- Securing remote access communication using multifactor authentication.
- Backing up customer data on a daily basis, on a rotating schedule.