Data Collection, Processing and Storage: Technical and Organisational Measures

Adform hereby warrants that Adform has implemented and will maintain the technical and organizational security measures reasonably required for safeguarding Data against corruption, loss or access from any unauthorized third party

Details of Technical and Organizational Measures currently maintained are listed below:

General description of measures	Description of measures implemented
Access control (premises) Preventing unauthorized persons from gaining access to data processing systems	• Access control systems (smart cards, biometric control, personal codes) • Access limited to authorized IT personnel • List of authorized people (manager approval required) • Surveillance systems (alarm system, door prop alarm, motion detectors, 24x7 CCTV) • Lockable cabinets (servers, storage media) • Glass break sensors • Visitor logbook (time and purpose of entry, time of exit)
Access control (systems) Preventing data processing systems from being used without authorisation	• On-premise storage only • Database security controls restrict access; controlled and audited by internal and external auditors • Access rights based on roles and need to know • Approval process for access rights; periodical reviews and audits • Password policy • Automatic blocking of access (e.g. password, timeout) • Protocol of failed log-ons
Access control (data) Ensuring that persons entitled to use a data processing system have access only to the data to which they have a right of access, and that personal data cannot be read, copied, modified or removed without authorisation	• Access rights based on roles and need to know • Approval process for access rights; periodical reviews and audits • Anti-virus and firewall systems • Signed confidentiality undertakings • Secure retention of storage media • Secure and certified disposal of data and storage media
Transmission control Ensuring that personal data cannot be read, copied, modified or removed with-	• Encrypted transfer (Secure Socket Layer/Transport Layer Security (SSL/TLS) in connection with valid certificates, secure shell, Secure Network Communication, Secure FTP (SFTP), IPSec, VPN technolo-

out authorisation during electronic transmission or transport, and that it is possible to review and establish which bodies are to receive the personal data	gies, RPC with encryption option RC4, SFTP, SQLNet with Advanced Security Option (ASO), encryption of XML data files with XML Encryption on SOAP protocols • Logging • Prohibition to use private devices (e.g. USB devices) • Transport security measures (e.g. locked containers, recording handover, written receipts)
Input control Ensuring that it is possible to review and establish whether and by whom personal data have been input into data processing systems, modified or removed	• Access rights based on roles and need to know • Approval process for access rights; periodical reviews and audits • Logging
Job control Ensuring that the personal data is processed exclusively in accordance with the instructions	• Diligently selecting (sub-)processors and other service providers • Documenting selection procedures (privacy and security policies, audit reports, certifications) • Backgrounds of service providers are checked; subsequent monitoring • Standardized policies and procedures (including clear segregation of responsibilities); documentation of instructions received from data controller or main processor • Specific process for urgent jobs (including subsequent written confirmation) • Signed confidentiality undertakings
Availability control Ensuring that personal data is protected from accidental destruction and loss	• Redundant uninterruptible power supply (UPS) • Air-conditioning, temperature and humidity controls (monitored 24x7) • Disaster-proof housing (smoke detection, fire alarm, fire suppression, water detection, raised flooring, protection against severe weather conditions, pest repellent system) • Electrical equipment monitored and logged, 24x7 support • Daily backup procedures • Disaster recovery plan • Routinely test-running data recovery • Anti-virus/firewall systems • Redundant Data centres, servers, storage drives, internet providers and network equipment

Separation control Ensuring that data collected for different purposes can be processed separately	• Separate systems for HR data, production data, supplier data, customer data • Storage of different client data separated logically by software • Separation between production and test data • Detailed management of access rights

Adform reserves the right to make changes and updates to the above list of applied Technical and Organizational Measures to accommodate developments in the industry from time to time. The latest current details of Technical and Organizational Measures maintained by Adform can always be accessed at http://site.adform.com/datacollection