Technical and organisational measures

GW Solutions LTD — Version 2.0, 11 June 2026 (supersedes the version dated 28 May 2020)

The Processor shall ensure to take the technical and organizational measures necessary to ensure compliance with the provisions of applicable data protection laws. The Processor designates every Measure with either the symbol "☐" where a measure is not implemented or "☑" where a measure is implemented. Where examples are provided (e.g.) the Processor specifies or marks the applicable measures. The word "include" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly. The Processor is certified to ISO/IEC 27001 (Information Security Management); the certificate is published at https://www.iban.com/files/docs/iso27001.pdf. The Processor fulfils the requirements through the following measures:

1. Confidentiality pursuant to Art. 32 section 1 lit. b GDPR

1.1. Admittance Control

Admittance control measures are designed to prevent unauthorized access to data processing facilities used to store or process personal data. As with any other measure, admittance control measures should be combined with organizational measures (e.g. instructions providing for the locking of the offices in absentia).

Technical Measures	Organisational Measures
☑ Alarm	☑ Key rules / List / ☐ Centralization of Keys
☑ Automatic access control system (e.g. date and time based systems)	☑ Front desk / Reception / Porter
☑ Biometric access control	☑ Admittance logbook / record
☑ Manual locking system (e.g. physical keys)	☑ Employee passes / ☑ Guest passes (e.g. service providers and externals, such as cleaners and maintenance personnel)
☐ PIN or Code locking System	☑ Guest accompanied by Employees
☐ RFID or Smart cards / transponder systems	☐ Diligent selection of security personnel and other auxiliary service providers (e.g. cleaners and maintenance personnel) according to predefined policies
☐ Photo-IDs	☑ Definition of security areas
☑ Electronic monitoring / surveillance (e.g. video surveillance, IR surveillance, motion detectors, etc.)	☐ Definition of authorization groups
☑ Physical Entrance Barriers (e.g. fences, barbed wire tops, gated windows on floor level, shaft and duct barriers, etc.)	☐ Nighttime Patrols
☑ Doors with knob outside	☐ Others (specify)
☐ Others (specify)	

1.2. System Access Control

In addition to admittance control, the aim of system access control is to prevent unauthorized persons from using data processing systems in which personal data is stored, processed or used.

Technical Measures	Organisational Measures
☑ Login with traditional credentials (i.e. username + password)	☑ Centralised management of user permissions
☐ Login with biometric credentials (e.g. fingerprint and iris scans)	☐ Centralised administration of user profiles (e.g. Active Directory, Kerberos, etc.)
☑ Two factor authentication	☐ Central password management (e.g. LastPass)
Anti-Virus Software on all ☑ clients / ☑ servers / ☐ mobile devices	☑ Secure Password policy (e.g. minimum length, special characters, expiration term)
Firewall on all ☑ clients / ☑ servers / ☐ mobile devices	☑ Delete / Destroy policy

Technical Measures	Organisational Measures
☑ Intrusion Detection Systems (DDoS, blocking passwords on failed attempts, inactivity and process for resetting blocked access IDs)	☑ Clean desk policy
☑ Mobile Device Management	☑ General Directive on Data Protection and/or Security
Encryption on all ☑ clients / ☑ servers / ☑ mobile devices / ☑ other data carriers (e.g. USB sticks, CF and SD cards)	☑ Mobile Device Policy
☑ Use of VPN for remote access	☐ BYOD Policy
☐ BIOS protection (separate password)	☑ System Access Logging
☑ Locking / disabling external interfaces (USB)	☑ OTP (one-time password) policy for temporary access
☑ Automatic access blocking (i.e. access is blocked after a predefined amount of time of inactivity and reconnection requires re-entering of credentials)	☑ Manual Desktop Lock Guide
☐ Server Rack Locks	☐ Others (specify)
☐ Others (specify)	

1.3. Data Access Control

The aim of data access control measures is to ensure that persons authorised to use a data processing system may only access the data subject to their access authorisation and that personal data cannot be manipulated (e.g. read, copied, modified or deleted) without authorisation.

Technical Measures	Organisational Measures
☑ Data access restrictions (including role-based access control - RBAC, authentication of individual critical transactions using TAN, etc.)	☑ User rights administration
☑ Assignment of minimum authorizations (regarding the term, scope and purpose of the access)	☐ Avoid the concentration of functions
☑ Logging of data manipulations	☑ Minimize administrative rights
☐ Others (specify)	☐ Others (specify)

1.4. Data Separation

The aim of data separation measures is to ensure that data obtained for different purposes can be processed separately.

Technical Measures	Organisational Measures
☑ Separation of production and test environments	☑ Separation of access control through authorization policy
Physical separation of data on ☑ clients / ☑ servers / ☑ other data carriers	☑ Network Separation / Segmentation (including by routers and switches)
☐ Others (specify)	☐ Others (specify)

1.5. Pseudonymisation (Art. 32 section 1 lit. a GDPR; Art. 25 section 1 GDPR)

The aim of pseudonymisation measures is to process personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, provided that this additional information is processed separately and is likewise subject to appropriate technical and organisational measures.

Technical Measures	Organisational Measures
☑ If pseudonymization is used: separation of the identification data and storage thereof in a separate and secure system (encrypted where possible)	☑ Policy to anonymize / pseudonymize data in the event of disclosure or after expiry of the legal deletion period where feasible
☐ Others (specify)	☐ Others (specify)

2. Integrity pursuant to Art. 32 section 1 lit. b GDPR

2.1. Data Disclosure Control

The aim of the data disclosure control measures is to ensure that personal data cannot be manipulated (e.g. read, copied, modified or deleted) without authorisation during transmission by electronic means or during transport or storage on other data carriers, and that it can be verified and ascertained where personal data is being transmitted by such means.

Technical Measures	Organisational Measures
Secure data transmission between servers and clients by: ☑ Secure Socket Layer / Transport Layer Security (SSL/TLS) ☑ Valid certificates in web applications (https) ☑ Secure Shell ☐ Secure Network Communication (SNC) ☑ Secure FTP (SFTP) ☐ IPSec ☐ VPN ☐ RPC with RC4 encryption option ☐ SQL Net with Advanced Security Option (ASO) ☐ Encrypting XML files with XML encryption for SOAP protocols ☐ Other measures (specify)	☑ User rights administration (determining instances/persons authorized to receive/transmit data)
Secure backend transmission by: ☑ Secure Shell ☑ Secure FTP (SFTP) ☐ IPSec ☐ VPN ☐ RPC with RC4 encryption option ☐ SQL Net with Advanced Security Option (ASO) ☐ Encrypting XML files with XML encryption for SOAP protocols ☐ Other measures (specify)	☑ Transmission Policy (ensuring the lawfulness of transmission to other countries)
Secure transmission to external systems by: ☑ Secure Shell ☑ Secure FTP (SFTP) ☐ IPSec ☐ VPN ☐ RPC with RC4 encryption option ☐ SQL Net with Advanced Security Option (ASO) ☐ Encrypting XML files with XML encryption for SOAP protocols ☐ Email encryption using S/MIME or PGP ☐ Other measures (specify)	☐ Others (specify)
Security gateways (including at the network handover points): ☑ Firewalls ☑ IP Filters (whitelists/blacklists) ☐ NIPS (network intrusion prevention systems) ☐ Proxies or load balancers with IP filters ☐ Other measures (specify)	
☐ Separation / segmentation within back end systems	
☑ Document shredder compliant with at least level 3 DIN 66399	
☐ External document shredder (pursuant to DIN 32757 or comparable)	
☑ Physical destruction of data carriers (pursuant to NIST SP 800-88 destruct or comparable)	

Technical Measures	Organisational Measures
☑ Logical deletion of data carriers (in accordance with either NIST SP 800-88 clear or purge, UK HMG InfoSec No 5, or BSI VSITR)	
☐ Others (specify)	

2.2. Data Input Control

The aim of the data input control measures is to ensure that it is possible to verify and determine whether and by whom personal data have been entered, modified or deleted from data processing systems. It must also be clarified which data is logged, who has access to logs, by whom and at what occasion/time they are checked, how long storage is required and when the logs are deleted.

Technical Measures	Organisational Measures
☑ Technical logging of data entry, modification and deletion	☑ Overview of which programs can be used to enter, change or delete which data
☑ Manual or automated control of the protocols	☑ Tracking of data entry, modification and deletion through individual user names (not user groups)
☑ Allocation of rights to enter, modify and delete data on the basis of an authorisation concept	☑ Clear responsibilities for deletions
☐ Others (specify)	☐ Others (specify)

2.3. Subprocessor Control (Outsourcing)

The aim of the subprocessor control measures is to ensure that data processed on behalf of the Controller is processed only in accordance with the Controller’s instructions. If the Processor uses contractors for the purpose of processing an order, the following items shall always be regulated in writing (DPA) with these contractors.

Technical Measures	Organisational Measures
☑ Selection of the contractor with due diligence (especially with regard to data protection and data security)	☑ Issuing and receiving instructions policy (detailing which personnel shall be authorized to issue and receive instructions regarding the data processing)
☑ Instruction execution rules and limitations (ensuring that the order is only executed as set forth in the agreement or otherwise provided by the Processor)	☑ Prior review of the safety measures implemented by the contractor and their documentation
☐ Adequacy assurance if contractor outside EEA (EU Standard Contractual Clauses, adequacy decision or comparable transfer mechanism)	☐ Effective control rights vis-à-vis the Controller
☑ Obligation for the appointment of a data protection officer by the contractor (where applicable)	☑ Obligation of the contractor’s employees to maintain data secrecy
☑ Regulation on the use of further subcontractors	☑ Ensuring the destruction of data after completion of the order
☑ In case of long-term cooperation: ongoing review of the contractor and its level of protection	☐ Others (specify)

3. Availability and resilience pursuant to Art. 32 section 1 lit. b GDPR

3.1. Data Availability

The aim of data backup measures is to ensure that personal data is protected against accidental destruction or loss.

Technical Measures	Organisational Measures
☑ Video surveillance in server room	☑ Backup & Recovery concept (formulated)
☑ Fire and smoke detection systems in server room	☐ Emergency plan (e.g. BSI IT-Grundschutz 100-4)
☑ Fire extinguisher or fire suppression system in the server room	☑ Storage of backup media in a safe place outside the server room

Technical Measures	Organisational Measures
☑ Server room monitoring temperature and humidity	☑ Regular tests of backup operations and logging of results
☑ Server room air-conditioned	☑ Monitoring of the backup operation
☑ UPS	☑ No sanitary connections in or above the server room
☐ Server room with socket strips	☐ Separate partitions for operating systems and data
☑ Alarm system in case of unauthorized access to server room	☐ Others (specify)
☑ RAID system / hard disk mirroring	
☐ Data protection safe (S60DIS, S120DIS, other suitable standards with displacement seal etc.)	
☐ Others (specify)	

3.2. Data Security Management

The aim of data security management measures is to ensure that personal data processing and compliance with statutory provisions is managed on an organisational level.

Technical Measures	Organisational Measures
☑ Software solutions for data protection management	☑ Internal / external data protection officer: Kostadin Markov / GW Solutions LTD / k.markov@iban.com
☑ Security certification according to ISO/IEC 27001 (certificate published at https://www.iban.com/files/docs/iso27001.pdf)	☑ Internal / external Information Security Officer: Andrey Manolov / GW Solutions LTD / manolov@banksoft.com
☐ Other documented security concept	☑ Central documentation of all procedures and regulations for data protection, accessible by all employees as required (maintained as part of the ISO/IEC 27001 ISMS documentation)
	☑ Employees trained and committed to confidentiality / data secrecy
	☑ Regular awareness training for employees - conducted at least annually (in accordance with ISO/IEC 27001)
	☑ A review of the effectiveness of the technical and organisational measures - conducted at least annually
	☐ Data Protection Impact Assessments (DPIA) are carried out if necessary
	☐ Compliance with the information requirements of Art. 13 and 14 GDPR
	☐ Formalised policy for processing data subject requests under GDPR is in place
	☐ Others (specify)

3.3. Incident Response Management

The aim of incident response management measures is to ensure that assistance in responding to security breaches is provided by the Processor.

Technical Measures	Organisational Measures
☑ Use of firewall and automated updates	☑ Documented procedure for the detection and reporting of security incidents / data breaches (especially with regard to the obligation to report to the supervisory authority)
☑ Use of spam filters and automated updates	☑ Documented procedure for dealing with security incidents

Technical Measures	Organisational Measures
☑ Use of virus scanners and automated updates	☑ Integration of DPO and (C)ISO in security incidents and data breaches
☑ Intrusion Detection System (IDS)	☑ Documentation of security incidents and data breaches, e.g. via ticket system
☐ Intrusion Prevention System (IPS)	☑ Formal process and responsibilities for post-processing security incidents and data breaches
☐ Others (specify)	☐ Others (specify)

4. Other

4.1. Privacy by design and by default

Technical Measures	Organisational Measures
☑ Personal data is only collected and processed to the extent necessary for the respective purpose	☑ Where the data subject can influence the amount of data processing, the service by default offers the less intrusive setup
☑ Easy exercise of the right to withdraw consent by data subjects, including by technical means	☐ Others (specify)
☐ Others (specify)	

Company: GW Solutions LTD

Name: Andrey Manolov

Date: 11 June 2026

Signature: _____