RISK LEVEL
SELF - ASSESSMENT FINDINGS

Level of risk	High
Processing operation	wdwd

Pending implementation and deployment

Security policy and procedures for the protection of personal data

Measure Identifier	Measure Description	Risk level
A.1	The organization should document its policy with regards to personal data processing as part of its information security policy.	
A.2	The security policy should be reviewed and revised, if necessary, on an annual basis.	
A.3	The organization should document a separate dedicated security policy with regard to the processing of personal data. The policy should be approved by management and communicated to all employees and relevant external parties	
A.4	The security policy should at least refer to: the roles and responsibilities of personnel, the baseline technical and organisation measures adopted for the security of personal data, the data processors or other third parties involved in the processing of personal data.	
A.5	An inventory of specific policies/procedures related to the security of personal data should be created and maintained, based on the general security policy.	
A.6	The security policy should be reviewed and revised, if necessary, on a semester basis.	
	Related to ISO 27001:2013 - A.5 Security policy	

Roles and responsibilities

Measure Identifier	Measure Description	Risk level
B.1	Roles and responsibilities related to the processing of personal data should be clearly defined and allocated in accordance with the security policy.	
B.2	During internal re-organizations or terminations and change of employment, revocation of rights and responsibilities with respective hand over procedures should be clearly defined.	
B.3	Clear appointment of persons in charge of specific security tasks should be performed, including the appointment of a security officer.	
B.4	The security officer should be formally appointed (documented). The tasks and responsibilities of the security officer should also be clearly set and documented.	
B.5	Conflicting duties and areas of responsibility, for examples the roles of security officer, security auditor, and DPO, should considered to be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of personal data.	
	Related to ISO 27001:2013 - A.6.1.1 Information security roles and responsibilities	

Access control policy

Measure Identifier	Measure Description	Risk level
C.1	Specific access control rights should be allocated to each role (involved in the processing of personal data) following the need to know principle.	
C.2	An access control policy should be detailed and documented. The organization should determine in this document the appropriate access control rules, access rights and restrictions for specific user roles towards the processes and procedures related to personal data.	
C.3	Segregation of access control roles (e.g. access request, access authorization, access administration) should be clearly defined and documented.	

Measure Identifier	Measure Description	Risk level
C.4	Roles with excessive access rights should be clearly defined and assigned to limited specific members of staff.	
	Related to ISO 27001:2013 - A.9.1.1 Access control policy	

Resource/asset management

Measure Identifier	Measure Description	Risk level
D.1	The organization should have a register of the IT resources used for the processing of personal data (hardware, software, and network). The register could include at least the following information: IT resource, type (e.g. server, workstation), location (physical or electronic). A specific person should be assigned the task of maintaining and updating the register (e.g. IT officer).	
D.2	IT resources should be reviewed and updated on regular basis.	
D.3	Roles having access to certain resources should be defined and documented.	
D.4	IT resources should be reviewed and updated on annual basis.	
	Related to ISO 27001:2013 - A.8 Asset management	

Change management

Measure Identifier	Measure Description	Risk level
E.1	The organization should make sure that all changes to the IT system are registered and monitored by a specific person (e.g. IT or security officer). Regular monitoring of this process should take place.	
E.2	Software development should be performed in a special environment that is not connected to the IT system used for the processing of personal data. When testing is needed, dummy data should be used (not real data). In cases that this is not possible, specific procedures should be in place for the protection of personal data used in testing.	
E.3	A detailed and documented change policy should be in place. It should include: a process for introducing changes, the roles/users that have change rights, timelines for introducing changes. The change policy should be regularly updated.	
	Related to ISO 27001:2013 - A. 12.1 Operational procedures and responsibilities	

Data processors

Measure Identifier	Measure Description	Risk level
F.1	Formal guidelines and procedures covering the processing of personal data by data processors (contractors/outsourcing) should be defined, documented and agreed between the data controller and the data processor prior to the commencement of the processing activities. These guidelines and procedures should mandatorily establish the same level of personal data security as mandated in the organization's security policy.	
F.2	Upon finding out of a personal data breach, the data processor shall notify the controller without undue delay.	
F.3	Formal requirements and obligations should be formally agreed between the data controller and the data processor. The data processor should provide sufficient documented evidence of compliance.	
F.4	The data controller's organization should regularly audit the compliance of the data processor to the agreed level of requirements and obligations.	

Measure Identifier	Measure Description	Risk level
F.5	The employees of the data processor who are processing personal data should be subject to specific documented confidentiality/ non-disclosure agreements.	
	Related to ISO 27001:2013 - A.15 Supplier relationships	

Incidents handling / Personal data breaches

Measure Identifier	Measure Description	Risk level
G.1	An incident response plan with detailed procedures should be defined to ensure effective and orderly response to incidents pertaining personal data.	
G.2	Personal data breaches should be reported immediately to the management. Notification procedures for the reporting of the breaches to competent authorities and data subjects should be in place, following art. 33 and 34 GDPR.	
G.3	The incidents' response plan should be documented, including a list of possible mitigation actions and clear assignment of roles.	
G.4	Incidents and personal data breaches should be recorded along with details regarding the event and subsequent mitigation actions performed.	
	Related to ISO 27001:2013 - A.16 Information security incident management	

Business continuity

Measure Identifier	Measure Description	Risk level
H.1	The organization should establish the main procedures and controls to be followed in order to ensure the required level of continuity and availability of the IT system processing personal data (in the event of an incident/personal data breach).	
H.2	A BCP should be detailed and documented (following the general security policy). It should include clear actions and assignment of roles.	
H.3	A level of guaranteed service quality should be defined in the BCP for the core business processes that provide for personal data security.	
H.4	Specific personnel with the necessary responsibility, authority and competence to manage business continuity in the event of an incident/personal data breach should be nominated.	
H.5	An alternative facility should be considered, depending on the organization and the acceptable downtime of the IT system.	
	Related to ISO 27001:2013 - A. 17 Information security aspects of business continuity management	

Confidentiality of personnel

Measure Identifier	Measure Description	Risk level
I.1	The organization should ensure that all employees understand their responsibilities and obligations related to the processing of personal data. Roles and responsibilities should be clearly communicated during the pre-employment and/or induction process.	
I.2	Prior to up taking their duties employees should be asked to review and agree on the security policy of the organization and sign respective confidentiality and non-disclosure agreements.	
I.3	Employees involved in high risk processing of personal data should be bound to specific confidentiality clauses (under their employment contract or other legal act).	

Measure Identifier	Measure Description	Risk level
	Related to ISO 27001:2013 - A.7 Human resource security	

Training

Measure Identifier	Measure Description	Risk level
J.1	The organization should ensure that all employees are adequately informed about the security controls of the IT system that relate to their everyday work. Employees involved in the processing of personal data should also be properly informed about relevant data protection requirements and legal obligations through regular awareness campaigns.	
J.2	The organization should have structured and regular training programmes for staff, including specific programmers for the induction (to data protection matters) of newcomers.	
J.3	A training plan with defined goals and objectives should be prepared and executed on an annual basis.	
	Related to ISO 27001:2013 - A.7.2.2 Information security awareness, education and training	

Access control and authentication

Measure Identifier	Measure Description	Risk level
K.1	An access control system applicable to all users accessing the IT system should be implemented. The system should allow creating, approving, reviewing and deleting user accounts.	
K.2	The use of common user accounts should be avoided. In cases where this is necessary, it should be ensured that all users of the common account have the same roles and responsibilities.	
K.3	An authentication mechanism should be in place, allowing access to the IT system (based on the access control policy and system). As a minimum a username/password combination should be used. Passwords should respect a certain (configurable) level of complexity.	
K.4	The access control system should have the ability to detect and not allow the usage of passwords that don't respect a certain (configurable) level of complexity.	
K.5	A specific password policy should be defined and documented. The policy should include at least password length, complexity, validity period, as well as number of acceptable unsuccessful login attempts.	
K.6	User passwords must be stored in a "hashed" form.	
K.7	Two-factor authentication should preferably be used for accessing systems that process personal data. The authentication factors could be passwords, security tokens, USB sticks with a secret token, biometrics etc.	
K.8	Device authentication should be used to guarantee that the processing of personal data is performed only through specific resources in the network.	
	Related to ISO 27001:2013 - A.9 Access control	

Logging and monitoring

Measure Identifier	Measure Description	Risk level
L.1	Log files should be activated for each system/application used for the processing of personal data. They should include all types of access to data (view, modification, deletion).	
L.2	Log files should be timestamped and adequately protected against tampering and unauthorized access. Clocks should be synchronised to a single reference time source	

Measure Identifier	Measure Description	Risk level
L.3	Actions of the system administrators and system operators, including addition/deletion/change of user rights should be logged.	
L.4	There should be no possibility of deletion or modification of log files content. Access to the log files should also be logged in addition to monitoring for detecting unusual activity.	
L.5	A monitoring system should process the log files and produce reports on the status of the system and notify for potential alerts.	
	Related to ISO 27001:2013 - A.12.4 Logging and monitoring	

Server/Database security

Measure Identifier	Measure Description	Risk level
M.1	Database and applications servers should be configured to run using a separate account, with minimum OS privileges to function correctly.	
M.2	Database and applications servers should only process the personal data that are actually needeeds to process in order to achieve its processing purposes.	
M.3	Encryption solutions should be considered on specific files or records through software or hardware implementation.	
M.4	Encrypting storage drives should be considered	
M.5	Pseudonymization techniques should be applied through separation of data from direct identifiers to avoid linking to data subject without additional information	
M.6	Techniques supporting privacy at the database level, such as authorized queries, privacy preserving data base querying, searchable encryption, etc., should be considered.	
	Related to ISO 27001:2013 - A. 12 Operations security	

Workstation security

Measure Identifier	Measure Description	Risk level
N.1	Users should not be able to deactivate or bypass security settings.	
N.2	Anti-virus applications and detection signatures should be configured on a weekly basis.	
N.3	Users should not have privileges to install or deactivate unauthorized software applications.	
N.4	The system should have session time-outs when the user has not been active for a certain time period.	
N.5	Critical security updates released by the operating system developer should be installed regularly.	
N.6	Anti-virus applications and detection signatures should be configured on a daily basis.	
N.7	It should not be allowed to transfer personal data from workstations to external storage devices (e.g. USB, DVD, external hard drives).	
N.8	Workstations used for the processing of personal data should preferably not be connected to the Internet unless security measures are in place to prevent unauthorised processing, copying and transfer of personal data on store.	
N.9	Full disk encryption should be enabled on the workstation operating system drives	
	Related to ISO 27001:2013 - A. 14.1 Security requirements of information systems	

Network/Communication security

Measure Identifier	Measure Description	Risk level
O.1	Whenever access is performed through the Internet, communication should be encrypted through cryptographic protocols (TLS/SSL).	
O.2	Wireless access to the IT system should be allowed only for specific users and processes. It should be protected by encryption mechanisms.	
O.3	Remote access to the IT system should in general be avoided. In cases where this is absolutely necessary, it should be performed only under the control and monitoring of a specific person from the organization (e.g. IT administrator/security officer) through pre-defined devices.	
O.4	Traffic to and from the IT system should be monitored and controlled through Firewalls and Intrusion Detection Systems.	
O.5	Connection to the internet should not be allowed to servers and workstations used for the processing of personal data.	
O.6	The network of the information system should be segregated from the other networks of the data controller.	
O.7	Access to the IT system should be performed only by pre-authorized devices and terminal using techniques such as MAC filtering or Network Access Control (NAC)	
	Related to ISO 27001:2013 - A.13 Communications Security	

Back-ups

Measure Identifier	Measure Description	Risk level
P.1	Backup and data restore procedures should be defined, documented and clearly linked to roles and responsibilities.	
P.2	Backups should be given an appropriate level of physical and environmental protection consistent with the standards applied on the originating data.	
P.3	Execution of backups should be monitored to ensure completeness.	
P.4	Full backups should be carried out regularly.	
P.5	Backup media should be regularly tested to ensure that they can be relied upon for emergency use.	
P.6	Scheduled incremental backups should be carried out at least on a daily basis.	
P.7	Copies of the backup should be securely stored in different locations.	
P.8	In case a third party service for back up storage is used, the copy must be encrypted before being transmitted from the data controller.	
P.9	Copies of backups should be encrypted and securely stored offline as well.	
	Related to ISO 27001:2013 - A.12.3 Back-Up	

Mobile/Portable devices

Measure Identifier	Measure Description	Risk level
Q.1	Mobile and portable device management procedures should be defined and documented establishing clear rules for their proper use.	
Q.2	Mobile devices that are allowed to access the information system should be pre-registered and pre-authorized.	
Q.3	Mobile devices should be subject to the same levels of access control procedures (to the data processing system) as other terminal equipment.	

Measure Identifier	Measure Description	Risk level
Q.4	Specific roles and responsibilities regarding mobile and portable device management should be clearly defined.	
Q.5	The organization should be able to remotely erase personal data (related to its processing operation) on a mobile device that has been compromised.	
Q.6	Mobile devices should support separation of private and business use of the device through secure software containers.	
Q.7	Mobile devices should be physically protected against theft when not in use.	
Q.8	Two factor authentication should be considered for accessing mobile devices	
Q.9	Personal data stored at the mobile device (as part of the organization's data processing operation) should be encrypted.	
	Related to ISO 27001:2013 - A. 6.2 Mobile devices and teleworking	

Application lifecycle security

Measure Identifier	Measure Description	Risk level
R.1	During the development lifecycle best practises, state of the art and well acknowledged secure development practices, frameworks or standards should be followed.	
R.2	Specific security requirements should be defined during the early stages of the development lifecycle.	
R.3	Specific technologies and techniques designed for supporting privacy and data protection (also referred to as Privacy Enhancing Technologies (PETs)) should be adopted in analogy to the security requirements.	
R.4	Secure coding standards and practises should be followed.	
R.5	During the development, testing and validation against the implementation of the initial security requirements should be performed.	
R.6	Vulnerability assessment, application and infrastructure penetration testing should be performed by a trusted third party prior to the operational adoption. The application shall not be adopted unless the required level of security is achieved.	
R.7	Periodic penetration testing should be carried out.	
R.8	Information about technical vulnerabilities of information systems being used should be obtained.	
R.9	Software patches should be tested and evaluated before they are installed in an operational environment.	
	Related to ISO 27001:2013 - A.12.6 Technical vulnerability management & A.14.2 Security in development and support processes	

Data deletion/disposal

Measure Identifier	Measure Description	Risk level
S.1	Software-based overwriting should be performed on all media prior to their disposal. In cases where this is not possible (CD's, DVD's, etc.) physical destruction should be performed.	
S.2	Shredding of paper and portable media used to store personal data shall be carried out.	
S.3	Multiple passes of software-based overwriting should be performed on all media before being disposed.	
S.4	If a third party's services are used to securely dispose of media or paper based records, a service agreement should be in place and a record of destruction of records should be produced as appropriate.	

Measure Identifier	Measure Description	Risk level
S.5	Following the software erasure, additional hardware based measures such as degaussing should be performed. Depending on the case, physical destruction should also be considered.	
S.6	If a third party, therefor data processor, is being used for destruction of media or paper based files, it should be considered that the process takes place at the premises of the data controller (and avoid off-site transfer of personal data.	
	Related to ISO 27001:2013 - A. 8.3.2 Disposal of media & A. 11.2.7 Secure disposal or re-use of equipment	

Physical security

Measure Identifier	Measure Description	Risk level
T.1	The physical perimeter of the IT system infrastructure should not be accessible by non-authorized personnel.	
T.2	Clear identification, through appropriate means e.g. ID Badges, for all personnel and visitors accessing the premises of the organization should be established, as appropriate.	
T.3	Secure zones should be defined and be protected by appropriate entry controls. A physical log book or electronic audit trail of all access should be securely maintained and monitored	
T.4	Intruder detection systems should be installed in all security zones.	
T.5	Physical barriers should, where applicable, be built to prevent unauthorized physical access.	
T.6	Vacant secure areas should be physically locked and periodically reviewed	
T.7	An automatic fire suppression system, closed control dedicated air conditioning system and uninterruptible power supply (UPS) should be implemented at the server room	
T.8	External party support service personnel should be granted restricted access to secure areas.	
	Related to ISO 27001:2013 - A.11 – Physical and environmental security	

Note: The adequacy of measures to specific risk levels should not be perceived as absolute. Depending on the context of the personal data processing, the organization can consider adopting additional measures, even if they are assigned to a higher level of risk.