RISK ASSESSMENT AND SECURITY MEASURE FOR PERSONAL DATA PROCESSING

Assessment of the level of risk for processing operation **The GDPR Central platform allows entities to log the different processing activities which are performed and all the information required to ensure this information is complete.** and a proposal for appropriate technical and organizational security measures.

Section I – Definition and Context of the Processing Operation

PROCESSING OPERATION DESCRIPTION	ANSWER	
Personal Data Processed	email, lastname & firstname	
Processing Purpose	To create a small user profile that allows a user to login.	
Data Subject	Employees of entities.	
Processing Means	This data is part of the user management process.	
Recipients of Personal Data	Internal	None
	External	None
Data Processor Used	Amazon AWS within the EEA (Frankfurt)	

Section II – Evaluation of the Impact

Confidentiality impact assessment: **Low**

The personal data in the platform is part of the user platform. This information is the firstname, lastname & email which are not considered critical.

Integrity impact assessment: **Low**

The email is important for the purpose of logging into the platform, the first and lastname are used to show in the platform who has taken an action, or who is responsible. If the name is changed, the visual name will be changed, but the link between action or responsible is not altered.

Availability impact assessment: **Low**

Minimal loss, + backups are in place to ensure continuity.

IMPACT ASSESSMENT		
Confidentiality	**Integrity**	**Availability**
Low	Low	Low
	Overall Impact Evaluation	Low

Section III – Analysis of the Threats per Assessment Area

Network and Technical Resources threat probability: Low

- **Is any part of the processing of personal data performed through the internet? Yes**
  The GDPR Central platform is a cloud only solution.
- **Is it possible to provide access to an internal personal data processing system through the internet (e.g. for certain users or groups of users)? Yes**
  For maintenance purposes the system administrators are able to get access to the backend system using secure methods.
- **Is the personal data processing system interconnected to another external or internal (to your organization) IT system or service? No**
- **Can unauthorized individuals easily access the data processing environment? No**
  The systems are protected by strong authentication means, strong configuration, firewalls and systems which are kept up to date at all times.
- **Is the personal data processing system designed, implemented or maintained without following relevant documented best practices? No**
  The system has been constructed using CIS (hardening guides) and ISO27K1 (security governance) in mind which include the design, the operations and the destruction of the environment and processes.

Processes/Procedures related to the processing of personal data threat probability: Low

- **Are the roles and responsibilities with regard to personal data processing vague or not clearly defined? Yes**
  Clearly defined.
- **Is the acceptable use of the network, system and physical resources within the organization ambiguous or not clearly defined? Yes**
  There is an acceptable use of assets policy in place.
- **Are the employees allowed to bring and use their own devices to connect to the personal data processing system? No**
- **Are the employees allowed to transfer, store or otherwise process personal data outside the premises of the organization? No**
- **Can personal data processing activities be performed without log files being created? No**

Parties/People involved in the processing of personal data threat probability: Low

- **Is the processing of personal data performed by an undefined number of employees? No**
- **Is any part of the data processing operation performed by a contractor/third party (data processor)? No**
- **Are the obligations of the parties/persons involved in personal data processing ambiguous or not clearly stated? No**
- **Is the personnel involved in the processing of personal data unfamiliar with security matters? No**
- **Do the persons/parties involved in the data processing operation neglect to securely store and/or destroy personal data? No**

Business sector and scale of processing threat probability: Low

- **Do you consider your business sector as being prone to cyberattacks? No**
- **Has your organization suffered any cyberattack or other type of security breach over the last two years? No**
- **Have you received any notifications and/or complaints with regard to the security of the IT system (used for the processing of personal data) over the last year? No**
- **Does your processing operation concern a large volume of individuals and/or personal data? No**
- **Are there any security best practices specific to your business sector that have not been adequately followed? No**

ASSESSMENT AREA	PROBABILITY	
Network and Technical Resources	Low	1
Processes/Procedures related to the processing of personal data	Low	1
Parties/People involved in the processing of personal data	Low	1
Business sector and scale of processing	Low	1
Overall Threat Occurrence Probability	Low (4)	

Section IV – Evaluation of Risk

	IMPACT LEVEL			
THREAT OCCURRENCE PROBABILITY		Low	Medium	High / Very High
	Low	X		
	Medium			
	High			

Section V – Organizational Security Measures

It should be noted that 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. Furthermore, the proposed list of measures does not take into account other additional sector specific security requirements, as well as specific regulatory obligations, arising for example from the ePrivacy Directive or the NIS Directive. In an attempt to further facilitate this procedure a mapping of the proposed group of measures with the ISO/IEC 27001:2013 security controls is also included.

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.	
	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.	
	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.	
	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.	
	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.	
	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.	
	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.	
	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).	
	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.	
	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.	
	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.	
	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	
	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.	

Measure Identifier	Measure Description	Risk level
	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.	
	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).	
	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.	
	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.	
	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.	
	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.	
	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.	
	Related to ISO 27001:2013 - A.11 – Physical and environmental security	