Security Objective	Requirements	Measure	Answer	Notes
Information Security principles	ISO/IEC 27001:2013, Clause 5 ISO/IEC 27001:2013, A.5.1.1	Are a set of policies and procedures in place for information security and data protection?	Yes	A formalised privacy and cybersecurity organisational model is in place
		Is there a formalised Information Security Policy?	Yes	A General Information Security Policy is in place
	ISO/IEC 27001:2013, A.5.1.2	Are information security and data protection policies and procedures periodically reviewed?	Yes	All the policies and the procedure regarding the information security organisational model are periodically reviewed
	ISO/IEC 27001:2013, Clause 6	Has the risk related to information security and data protection been regulated?	Yes	A formalised risk management procedure is in place
		Are risks being priorized and managed?	Yes	The risk is managed in accordance with the risk management procedure
Management of internal System Administrators	Prov. Data Protection Authority 27/11/2008, art. 4.2	Are the functions concerning the system administrator profile identified with regard to all levels of management, both hardware and software?	Yes	A candidate assessment procedure is in place
	Prov. Data Protection Authority 27/11/2008, art. 4.2	Does each sysadmin receive a formal individual appointment as system administrator?	Yes	An appointment letter Is formalised for each system administrator
	Prov. Data Protection Authority 27/11/2008, art. 4.1	Are individual skills of a system administrator properly assessed before him/her being designated as such?	Yes	An assessment of the skills of the appointed system administrator is carried out
	Prov. Data Protection Authority 27/11/2008, art. 4.2	Is there a formal appointment letter for each system administrator which lists his/her roles, privileges and area of activities?	Yes	An appointment letter is drawn up with the specific areas of operations
	Prov. Data Protection Authority 27/11/2008, art. 4.3	Are the identification details of the persons appointed as system administrators recorded in a list?	Yes	There is a list of system administrators
	Prov. Data Protection Authority 27/11/2008, art. 4.3	Is the list of system administrators constantly updated?	Yes	The list of system administrators is periodically reviewed
	Prov. Data Protection Authority 27/11/2008, art. 4.4	Is the work of a person appointed as system administrator properly audited at least once a year?	Yes	An annual review is carried out
	Prov. Data Protection Authority 27/11/2008, art. 4.5	Are all logical accesses of system administrators logged?	Yes	LogStation which collects all the logs sent by individual machines on which an agent is installed. LogStation uploads the logs to an ElasticSearch cluster with Grafana frontend that developers access to analyse the logs. A log management policy is in place.
	Prov. Data Protection Authority 27/11/2008, art. 4.5	Are system administrators' logical access records accompanied by time references and access description?	Yes	LogStation which collects all the logs sent by individual machines on which an agent is installed. LogStation uploads the logs to an ElasticSearch cluster with Grafana frontend that developers access to analyse the logs. A log management policy is in place

	Prov. Data Protection Authority 27/11/2008, art. 4.5	Are records of system administrators' logical accesses stored for at least six months?	**Yes**	A log retention policy is in place. For each log there is a retention period. A log management policy is also in place.
Human resources security and training	ISO/IEC 27001:2013, A.7	Is a background check performed on a new candidate?	**Yes**	A background check procedure is in place
		Is a security awareness program put in place for all staff?	**Yes**	Security training is provided for all employees every five years. The Udemy for Business Platform, used to deliver the courses, is available to all employees
		Is the process related to personnel changes put in place?	**Yes**	Is in place a formalised workflow related to personnel changes
		Is training provided for new hires in relation to their roles?	**Yes**	The need for the new employee to attend security training is assessed in relation to the skills he/she possesses
		Do the responsible for managing corporate security receive technical training regarding cybersecurity and data protection at least once a year?	**Yes**	Security training is provided for all employees every five years. The Udemy for Business Platform, used to deliver the courses, is available to all employees
		Is the competence of the persons in charge of company security tested at least once a year?	**Yes**	The competence of the persons in charge of company security is tested annually
		Do all employees receive general training on security and data protection issues at least once a year?	**Yes**	All employees receive a specific training on security and data protection issues annually
Authentication	Annex B of D.Lgs. 196/2003 (GDPR oriented) as amended by D.Lgs. 101/2018, artt. 1, 2, 3, 5, 7, 8, 10 ISO/IEC 27001:2013, A.9	Does each employee pass a strong authentication procedure before accessing his/her user accounts?	**Yes**	An SSO system on Active Directory is implemented. In addition, 2FA is mandatory on several systems
		Are authentication credentials individual for each employee?	**Yes**	There are no shared accounts
		Is the password assigned to an employee changed by himself/herself on first use and thereafter at periodic intervals?	**Yes**	Passwords have a duration of 180 days
		Is an alert sent to a system administrator if an employee has not used his/her credentials for at least six months?	**Yes**	An outsourced SOC with SIEM function is in place
		Are the credentials of an employee deactivated, or are his/her authorisation profiles changed, in line with any changes in the employee’s duties?	**Yes**	The process of creating/changing accounts is tracked via Jira issues. In case of resignation, the various permissions are deleted. In addition, an annual access control is carried out
Protection of data and devices	Annex B of D.Lgs. 196/2003 (GDPR oriented) as amended by D.Lgs. 101/2018, artt. 4, 9	Does each employee safeguard the confidentiality of his/her credentials?	**Yes**	Specific policies and procedures are in place providing for this type of control (i.e. Access Control Policy, IT tools policy)
		Does each employee safeguard his/her login sessions?	**Yes**	Specific policies and procedures are in place providing for this type of control (i.e. Access Control Policy, IT tools policy)

devices	ISO/IEC 27001:2013, A.8	Does each employee safeguard all devices assigned to him/her against accidental damage or theft?	Yes	Specific policies and procedures are in place providing for this type of control (i.e. Access Control Policy, IT tools policy)
Authorisation	Annex B D.Lgs 196/03 (GDPR oriented) as amended by D.Lgs 101/18 artt. 12, 13, 14, 15 ISO/IEC 27001:2013, A.9	Does each employee have clearly defined authorisation profiles?	**Yes**	Employee authorisation profiles are properly managed in accordance with information security best practices
		Are authorisation profiles defined according to the principles of minimisation, least privilege and need-to-know?	**Yes**	The management of authorisation profiles respects the principles of minimization, least privilege and need to know
		Are authorisation profiles periodically reviewed?	**Yes**	Policies and procedures are in place regarding the secure management of authorisation profiles
		Is it possible to list the authorisations assigned to a given authorisation profile?	**Yes**	All authorisation profiles are registered and monitored, as provided by corporate policies
Defence	Annex B D.Lgs 196/03 (GDPR oriented) as amended by D.Lgs 101/18 artt. 16, 17 ISO/IEC 27001:2013, A.8,12,13	Are all corporate hardware/software systems supported by their manufacturers and constantly kept up-to-date?	**Yes**	A centralized system is in place for managing updates
		Are those corporate hardware/software systems that are no longer supported by their manufacturers confined from other systems, i.e. are they physically confined in secure premises which are accessible only by strong authentication?	**Yes**	Devices that are no longer used or supported by suppliers are physically confined or destroyed using an outside service
		Are state-of-the-art protection tools used on all company hardware/software systems?	**Yes**	Antivirus and antimalware systems are present. There are two verification layers, the first Google Workspace and the second provided by an enterprise firewall with IDS, IPS and WAF functions
		Is the network configuration robust?	**Yes**	The network is configured in accordance with company policies and procedures which encompass appropriate segmentation. A firewall with IDS, IPS and WAF functions is also implemented
Data Availability	Annex B D.Lgs 196/03 (GDPR oriented) as amended by D.Lgs 101/18 artt. 18, 23	Is all data backed up at least weekly?	**Yes**	Periodic backups are carried out on a daily basis. Backups are present in multiple copies in separate and distant infrastructures that can be accessed online
		Can all data be promptly restored from backups?	**Yes**	All data can be restored through the backup systems in place
Data Protection	Annex B D.Lgs 196/03 (GDPR oriented) as amended by D.Lgs 101/18 artt. 20 ISO/IEC 27001:2013,	Are personal data stored in encrypted form?	**Yes**	Encryption is implemented on databases and assets where deemed necessary and as indicated by current legislation
		Are personal data only transferred electronically in encrypted form?	**Yes**	Policies are in place regarding the secure transfer of personal data
		Are retention times defined for customers data?	**Yes**	Retention times for customers data are established
	ISO/IEC 27001:2013	Are responsibilities about data protection assigned?	**Yes**	A DPO has been appointed.

Functions	ISO/IEC 27001:2013, A.6.1	Are responsibilities for corporate cybersecurity assigned?	**Yes**	Security roles within the organisation have been formally assigned (e.i. CISO)
		Is all staff aware of the assigned security roles?	**Yes**	All personnel are aware of the assigned security roles.
Third-party management	Art. 28 GDPR ISO/IEC 27001:2013, A.15	Do the contracts with outsourcers and suppliers include security requirements relevant to the service or product provided?	**Yes**	A document entitled "Guidelines for data controllers" concerning the contracting of outsourcers and their designation as data controllers pursuant to Article 28 of EU Regulation 679/2016 is in place.
		Is consistency with contracted security requirements periodically checked through properly contracted and scheduled second-party audits?	**Yes**	In accordance with the third party management policy, second party audits are carried out on suppliers
		Are the responsabilities for asset management by outsourcers defined?	**Yes**	Roles and responsibilities for the management of outsourced assets are formalised by specific agreements
		Are third party incidentes recored?	**Yes**	The third party management policy requires that supplier incidents must be recorded
Asset management	ISO/IEC 27001:2013, A.8	Is onboarding of new staff carried out in relation to assets?	**Yes**	A formalized onboarding procedure is in place
		Is there an inventory of assets?	**Yes**	There is an inventory of assets managed by the RackTables online tracking tool that reports Serial Number, location, rack location and other information useful to the asset management
		Are there procedures in place for the safe transfer of assets?	**Yes**	Specific policies and procedures are in place for asset management that also address best practice related to asset transfers
		Is there a process in place within the organisation to remove assets and credentials of employees who are no longer working in the infrastructure?	**Yes**	A formalised offboarding procedure is in place
		Is the use of removable media (including mobile devices) regulated?	**Yes**	Specific policies and procedures are in place for the management of mobile devices and removable media
		Is BYOD (Bring Your Own Device) regulated?	**Yes**	Specific policies are in place for BYOD
		Are removable media encrypted or destroyed before being discarded or sanitised before being reallocated?	**Yes**	Devices that are no longer used or supported by suppliers are destroyed using an outside service
		Are removable media containing personal data encrypted?	**Yes**	Removable storage media containing personal data are encrypted
Physical security	ISO/IEC 27001:2013, A.11	Are employees identified before they can enter the premises?	**Yes**	All physical access are monitored and registered
		Are visitors identified before they can enter the premises?	**Yes**	All physical accesses are monitored and recorded. Specific procedures are also in place for visitor management
		Are employees badges centrally managed?	**Yes**	A specific software is used for badge management
		Are data centres protected with advanced perimeter protection measures?	**Yes**	A badge is provided to access to the perimeter, with a locked gate. Furthermore, there are security cameras and a night surveillance service.

Access Control	ISO/IEC 27001:2013, A.9, 13	Are technical and organizational security measures in place to monitor logical access?	**Yes**	Policies and procedures are in place in order to manage access control. The authentication process is robust
		Is remote access to the corporate network regulated?	**Yes**	A formalised remote working procedure is in place
		Is network management regulated?	**Yes**	A formalised network management policy is in place
		Is the company network divided into separated VLANs?	**Yes**	The network is segmented into VLANs
System integrity	ENISA Technical Guidelines on Digital Providers SO11	Are there processes for sanitising database inputs?	**Yes**	The sanitization of the inputs is delegated to each BU, which is responsible for writing and configuring the applications
		Are passwords and encryption keys centrally managed?	**Yes**	Policies and procedures are in place regarding the secure management of passwords and encryption keys
		Is there a ban on deactivating protection measures on client machines?	**Yes**	Only Sysadmins can disable protection measures, upon specific request
Evaluation	ISO/IEC 27001:2013, A. 12.6.1, A. 18.2.2	Are vulnerability assessment sessions conducted on a yearly basis on all systems processing personal data?	**Yes**	Weekly scans are performed with vulnerability assessment tools and periodic reports are generated
		Are penetration testing sessions conducted on a yearly basis on all systems processing personal data?	**Yes**	Penetration Testing activity is carried out periodically, at least annually
		Are appropriate remediation actions implemented following any negative results from the vulnerability assessment and penetration testing sessions?	**Yes**	Vulnerabilities are always managed and patched
Incident and violation management	Artt. 33 e 34 GDPR ISO/IEC 27001:2013, A. 16	Are there practices, protocols and procedures relating to incident handling and are all security events and/or security incidents managed through a formalised procedure with established roles?	**Yes**	A procedure is in place for the management of incidentes, including a protocol to be followed in case of a security incident ora a data breach
		Are there training plans to raise awareness among employees about incident handling procedures?	**Yes**	An awareness program on security incident management is in place
		Have a SIEM and/or a SOC been implemented?	**Yes**	SIEM and SOC are implemented
		Is an incident log compiled and maintained, containing at least information on discovery, analysis, containment, mitigation and recovery from security incidents?	**Yes**	An incident handlng procedure that manage the various phases of an incident, including the recording of security events, is in place
Business continuity & Disaster recovery	ISO/IEC 27001:2013, A. 17	Is the use of resources continuously monitored?	**Yes**	A continuous monitoring of business continuity resources is in place
		Are resources increased when their use ceeds a given threshold for a given period?	**Yes**	A continuous monitoring of business continuity resources is in place
		Is the data centre redundant at a sufficient distance?	**Yes**	Adeguate redundancy is in place regarding data centres

		Is there a formalised Business Continuity Plan and/or a Disaster Recovery Plan?	**Yes**	Formalised continuity plans are in place in order to restore the critical processes
Recording of operations	Artt. 24 e 32 GDPR, accountability priciple	Is operational intelligence software implemented that produces unalterable, complete and integrity-verifiable logs operating on the systems on which the personal data relating to the Data Controller are processed?	**Yes**	A log management policy is in place. There is also in place an outsourced SIEM with an active SOC function
Test, development and production environments	Art. 25 GDPR, privacy by design principle ISO/IEC 27001:2013, A. 14	Has best practices for safe code development been implemented?	**Yes**	Corporate policies and guidelines for secure code development inspired by OWASP guidelines are in place and followed
		Are development and production test environments separated?	**Yes**	OWASP secure development guidelines are followed
		Are the procedures for moving from test to production environments formalised?	**Yes**	A procedure on secure development is in place and is followed
		Are software and systems tested prior to production?	**Yes**	Policies and procedures are in place regarding Software Management
		Are patches installed and uninstalled via known practices?	**Yes**	Policies and procedures regarding software management include patch management
		Is test data protected by encryption ?	**Yes**	Data encryption policies also include test data
Change Management	ISO/IEC 20000:2013 ISO/IEC 27001:2013, A. 12.1.2	Are changes made to critical systems through known practices or formalised procedures?	**Yes**	Change management procedures are in place, according to the internaional best practice
Compliance	ISO/IEC 27001:2013, A. 18	Has the company followed a compliance path to the GDPR (Reg. EU 2016/679)?	**Yes**	The company follows a continuos improvement path to GDPR compliance
		Has the company followed a compliance path to ISO/IEC 27001?	**Yes**	The BU MailUp Inc. is currently in process of being certified ISO/IEC 27001 and the organisational model of MailUp is inspired by the ISO/IEC 27001 best practices
		Does the service support multiple users, each logged in with his/her own account?	**Yes**	Each user account can have different levels of permissions so that only certain features are available. This feature allows diversifying every account according to operational needs, preventing the access in another Platform area that might remain hidden. https://help.mailup.com/display/MUG/User+permissions
		Does the service include at least one administrative user, i.e. being capable to operate with high privileges within the application?	**Yes**	

		Do the common accounts have less privileges than the administrative one?	Yes	Each user account can have different levels of permissions so that only certain features are available. This feature allows diversifying every account according to operational needs, preventing the access in another Platform area that might remain hidden.
		Does the application require an authentication procedure (i.e. login) to be passed before any personal data can be processed?	Yes	
		Does the application include strong authentication?	Yes	Minimum 8 characters in length with at least one uppercase letter, one number, and one special character. Two-factor authentication (2FA) adds an additional layer of security to the authentication process by making it harder for attackers to gain access to MailUp Platform. https://help.mailup.com/display/MUG/Password+management
		For web applications and in general stateless systems, does the application generate a token to be associated to the login session?	Yes	
		Is the token associated with the session of web applications or stateless systems long enough (64 or more alphanumeric characters) and not predictable?	Yes	The application "token" is encrypted and longer than 100 chars
		Does the token associated with the session of web applications or stateless systems have an expiry time?	Yes	Yes, the token expires after 30 minutes from the last activity
		Does the application keep the password in hashed form within its database?	Yes	Passwords are "salted" with an unique key for each account and then hashed with a SHA256 algorithm
		When the user ID is associated with an email address, does the application require verification of the validity of that address?	Yes	The first "admin" account requires the user to confirm the activation by email. For additional users the verification is not required
		Does the application limit or slow down the availability of login in the event of an abnormal number of unsuccessful login attempts within a short period of time?	Yes	After 5 failures within 30 seconds login will be unavailable for 300 seconds (values can be customized)
		Does the application allow each of its administrative users to assign different levels of rights to different users?	Yes	Each user account can have different levels of permissions so that only certain features are available. MailUp Platform allows to modify users permissions and to hide sensitive data. https://help.mailup.com/display/MUG/User+permissions https://help.mailup.com/display/MUG/Sensitive+personal+data+management

Privacy by design	Art. 25 GDPR, privacy by design principle	Does the application prevent each of its users that has not a sysadmin profile from changing the permission levels assigned to themselves or other users?	**Yes**	
		Are the personal data processed saved in an encrypted storage, using encryption techniques?	**Yes**	Backups are encrypted and personal data are masked by default
		Are the data processed through the application appropriately classified?	**Yes**	Email and mobile no. are classified. The user however may add additional fields that are not classified by default. He could however restrict the visibility of specific fields https://help.mailup.com/display/MUG/Sensitive+personal+data+management
		Does the application transmit network traffic in a protected form using state-of-the-art security protocols?	**Yes**	We use TLS/SSL cryptographic protocols that employ symmetric encryption based on a shared key to provide secure communications. These ensure data integrity for the network. To provide even greater security, we use a block cipher algorithm within TLS/SSL, which is called AES-256 (Advanced Encryption Standard). This replaces public key cryptography technology DES (Data Encryption Standard) as well as RSA 2048
		Are the processed data subject to backup at least daily?	**Yes**	
		Are all the service dependencies and its toolchain currently supported by their vendors and kept up-to-date?	**Yes**	
		Is a changelog regarding the service's updates provided to the Data Controller?	**Yes**	
		Is the application periodically subjected to vulnerability assessment and penetration testing sessions to assess its robustness to cyber attacks?	**Yes**	
		Does the application generate access logs?	**Yes**	
		Are the logs maintained for at least six months?	**Yes**	
		Does the application code not contain credentials or other cryptographic secrets?	**Yes**	
		Is the application code developed according to secure coding guidelines?	**Yes**	Devlopers are aware of security coding guidelines (OWASP)
		Does the application allow to define and modify retention times for the various types of data it stores?	**Yes**	Retention of statistical data is defined at the contract level according to the subscrption level Even if not in an automated fashion the data controller can manage retention times using the APIs

		Does the application record the last update date of each record?	Yes	
		Does the application allow one of its administrators to "mark" data as limited through the means of an unsubscription?	Yes	The Platform allows unsubscribing recipients with the option "Unsubscription due to the right to be forgotten". All additional data collected will be deleted except for the email address and the subscription date, which can be used to demonstrate consent in the future, if needed. Such data usage is, in any case, limited to the sole purpose of demonstrating the provision of information and recording the relative consents. It will be possible at any time to go for the definitive erasure by deleting the recipient. https://help.mailup.com/display/MUG/Email+recipients#Emailrecipients-righttobeforgottenUnsubscriptionduetorighttobeforgotten
		Does the application prevent the processing of limited data by means of an unsubscribe code?	Yes	We use a specific "unsubscription code" to mark data as limited and the data subject will be escluded from futher sendings BUT data is still accessibile to the controller without restrictions
		Does the application allow the aggregation in a comprehensible way of all the data that it stores regarding a data subject?	Yes	The Platform contains a section where there is all the information related to the individual recipient and where the latest activities of the recipient are also available (subscriptions, mailings, openings, clicks, cancellations and errors). https://help.mailup.com/display/MUG/Recipient+profile
		Does the application allow to record aggregated data in one or more files in a commonly used format?	Yes	Once generated, the file containing the recipient's data will be exported in .csv format as the default extension, alternatively, you can choose whether to export it in XML format. https://help.mailup.com/display/MUG/Export
		Does the application allow the import of aggregated data relating to a data subject, together with metadata useful to correctly identify them and adopting an interoperable format?	Yes	The Platform "Import" function allows a variety of formats to be imported (manually adding an individual recipient; importing a CSV/TXT; file importing an Excel; file importing an XML; file using copy and paste text into MailUp, and have the system automatically detect and extract email addresses and mobile phone numbers; using one of the integrations with external systems available). https://help.mailup.com/display/MUG/Import
		Does the application exclusively use databases and servers located within the European Union?	Yes	

		If the application is public, does it include screens dedicated to information and privacy policies so that the data subject can view them at any time?	**Yes**	On the Platform's website, you will find the "Privacy Policy" document which enables you to understand how your Personal Data will be managed when you use the Platform. https://www.mailup.com/privacy-statement/