MakoLab

Dear Supplier,

In order to ensure an appropriate level of quality, information security, environmental protection and occupational safety throughout the supply chain, we ensure that our suppliers meet the requirements established by MakoLab S.A..

For this purpose, please fill in the answers to questions on the individual requirements.
The responses form part of the qualification and supplier evaluation process for MakoLab S.A. and the basis for continuous improvement of the quality of our services and the development of our business relationships.

Your answers are treated confidentially and used only for the purposes indicated above.

MakoLab

Company Name	
Address	
Contact Person filling in: First name and surname Position e-mail phone	
Scope of cooperation	
Date of filling out	

MakoLab

Information Security Management

No.	Guidelines/Area	Questions	Additional questions	Answer (Yes/ Partly/ No/Not applicable)	Comments
1	Security objectives	Does the Supplier have an Information Security Management System in place if so, what system is it?			
2			Is the Supplier certified?		
3			Can the Supplier provide a certificate for inspection and a declaration of use?		
4		Where is the registered office of the Supplier's company from which work for MakoLab S.A. will be performed, i.e. is it located in the Republic of Poland, the European Union or outside the European Union?			
5			Where is the data processed (in the Republic of Poland, in the European Union, outside the European Union)?		
6		Have the risks associated with the project been identified and assessed?			
7			Is there a documented process for estimating risks in relation to information security?		
10		Have safeguards adequate to the identified risks been defined and applied?			
			How is the risk of losing a resource, e.g. business continuity plans, mitigated?		
11			How is the risk of not having the required resources to perform tasks mitigated?		
13	Classification of information	Has/does the classification of information transmitted, stored and processed in the context of the performance of tasks for MakoLab S.A. been applied according to the classification rules defined at MakoLab S.A.? Appendix 1 - Principles for classifying information			
14			Is the classification used in MakoLab known?		

15			Does the supplier have its own classification of information?		
16			How is the information of the information security class protected?		
17	**Information security**	Is the confidentiality and integrity of information transmitted over public transmission channels protected, according to its security class?			
18			What type of information is exchanged with MakoLab?		
19			How is information exchanged and protected in terms of confidentiality and integrity?		
20		Have all persons performing tasks for MakoLab S.A. signed declarations of confidentiality and of having read security requirements and relevant policies for their implementation?			
24	**Supply chain security**	Has security been ensured throughout the supply chain of the service/product provided?			
25	**Personnel safety**	Does the Supplier have and implement documented policies regarding its personnel, which include providing its personnel, who perform tasks for MakoLab S.A., with information about the security requirements of cooperation with MakoLab S.A.?			
26	**Mobile devices security**	Does the Supplier have and implement a documented policy on the use of mobile devices that ensures the security of performing remote work for MakoLab S.A. and the mobile devices used?			
27			How are employees' computers secured in terms of data encryption, anti-virus protection, password policy?		
29			How are employees' phones and other mobile devices secured, in terms of data encryption, anti-virus protection, password policy?		
31			How secure are memory sticks and other external media?		
			How is the use of the above safeguards verified and documented?		
32	**Security of removable storage media**	Does the Supplier have and implement policies regarding the secure transfer and deletion of data from media containing data related to the performance of tasks for MakoLab S.A., ensuring effective data protection?			
33			How is data transferred in the project?		
34			How is access to this data restricted?		
35			Is the granting of rights to the data transferred documented in any way?		

36			How is data removed from media? When are they removed? Is this documented?		
37			What happens to the data an employee has access to after leaving a project or company?		
38			Do the supplier's employees perform work on private equipment?		
39	**Security of entrusted assets**	Are asset users aware of the safe use of the assets provided?			
40			Is the company employee trained in the security of the information to which they have access? Is this documented?		
41			Is there a formal process for reminding people of information security rules? Is this documented?		
42		Will users return the assets or, if they are data, delete them in an effective manner once the commissioned tasks are completed?			
43			What happens to the project data and other data transferred by MakoLab on employees' computers after the project is completed?		
44			What happens to the project data and other data transferred by MakoLab on employees' computers after cooperation with the company has ended - also when the employee works on a private computer?		
45	**Security of remote work**	Does the Supplier have and implement policies on the use of networks and network services to ensure the security of remote access including the use of VPNs?			
46			How are accesses to network shares, backups organised?		
47			How are accesses to knowledge bases and product/project backlogs organised?		
48	**Security of the design process**	Does the Supplier operate in accordance with the principles of secure software and systems development, ensuring the existence and implementation of documented checkpoints for the implementation of security requirements, version control of the code and documentation produced, and compliance with documented programming standards communicated during the implementation of the work?			
49			How are requirements (in particular information security requirements) collected from the customer?		
50			What areas of requirements are collected?		
51			How are requirements documented?		

52			How is it verified that a requirement has been met?		
53			Is the software produced verified for safety? In what way? Is this documented?		
54			Is the code versioned and how?		
55	**Change management**	Does the Supplier ensure that documented change management procedures are in place for the applications, systems being developed, ensuring that changes are recorded and approved by authorised persons, and that there are change management procedures in place for the applications and systems being developed?			
56			How are changes to the project/production handled?		
57			Are changes documented?		
58			How is the change implemented?		
59	**Protection of design and operating documentation**	Does the Supplier ensure protection of the design and operation documentation created and processed for MakoLab S.A., in particular that it is made available only to persons who are authorised to access such information, that the design documentation is marked with a security class according to MakoLab's classification, and that it is stored in a repository that protects the confidentiality and integrity of the stored documentation? Appendix 1 - Principles for classifying information			
60			How is knowledge about the project collected?		
61			Who has access to this knowledge?		
62			What are the rules for granting access to knowledge with different security classes? Is this documented?		
63			Who manages access?		
64			Does the knowledge resource have a safety copy?		
67		Does the Supplier have adequate procedures in place to collect any evidence related to the security incident?			

68	Security incidents		Are security incidents being recorded?		
69			How does registration take place?		
70			Are there reviews of incidents and what happens to them next?		
			Are the actions taken documented? In what way?		
65		Does the Supplier undertake to report electronically to MakoLab S.A. any security incidents that are related to tasks performed or products manufactured for MakoLab?			
66			How does the supplier notify MakoLab S.A. of such an incident (email, telephone, other)?		
72	Separation of development and test environments	Does the Supplier ensure (at least at the level of a virtual or physical machine) the separation of development and test environments intended for the realisation of tasks for MakoLab S.A. from environments performing tasks for other clients?			
73			Are there separate dev/test/uat/prod environments?		
74			Who manages these accesses?		
75			Who has access to the production environment?		
76	Event log	Does the Supplier provide logging of user and administrator access events to the development and test systems and ensure that they are securely stored for a period of not less than 3 years? (The supplier must make the stored records available upon request to MakoLab S.A.)			
77	Backup protection	Does the Supplier provide physical security for the security copies and, where appropriate to the level of information protection required, encryption of the security copies?			
78	Secure source code repository	Is the source code stored in a secure source code repository?			
79	Source code protection	Does the Supplier ensure the integrity and confidentiality of the source codes during transfer?			

80	**Security of offices, premises and facilities**	Does the Supplier provide adequate security for the spaces in which work is performed for MakoLab S.A.?			
81			Is there monitoring in the premises?		
82			Is there an alarm system in the premises?		
83			Is access to the premises restricted and in what way?		
84			Is it possible to section off the room for a dedicated project (e.g. restrict access to the room to project team members only)?		
85			How is the server room secured?		

MakoLab Protection of Personal Data

No.	Guidelines/Area	Questions	Answer (Yes/ Partly/ No/Not applicable)	Comments
1	Protection of Personal Data	Do you have a security policy in place for the processing of personal data that complies with the principles of the GDPR?		
2		Have the persons authorised to process personal data committed themselves to secrecy or are they subject to an appropriate statutory secrecy obligation?		
3		Have your staff been trained in the principles of personal data processing in line with the GDPR?		
4		Has a Data Protection Officer (DPO) been appointed or has a person been appointed to perform tasks related to ensuring that the Supplier's processing of personal data complies with applicable law?		
5		Will the entrusted personal data be transferred outside the EEA? E.g. due to the location of the IT system, will the data be processed by persons located outside the EEA or will these persons be able to access the data? If so, in which country?		
6		Do you use subcontractors and subcontract or plan to subcontract personal data received from MakoLab S.A.?		
7		If so, do you have written data entrustment agreements in place with your subcontractors that impose the same data protection obligations on the subcontractor as set out in the entrustment agreement with the data controller?		
8		Do you have mechanisms/procedures in place to enable you to report a breach of personal data security to the Data Controller (MakoLab S.A.) without delay?		
9		If yes, please confirm your readiness to provide MakoLab S.A. with information about a breach of security of the entrusted data within 24 hours of the breach being discovered.		
10		Are there physical safeguards in place to protect the premises/processing areas used by your organisation against unauthorised access? If yes, please describe which (e.g. lockable doors, implemented room key management, access control system, burglar alarm systems, CCTV surveillance system, etc.).		
11		Has the processing of protected data already been subject to external audits or inspections, e.g. by the President of the Personal Data Protection Office in your organisation?		
12		Do you use third parties to whom you subcontract the personal data provided by the Data Controller? If yes, please indicate the names of the entities and specify the services they provide (e.g. user support, hosting, IT system support/maintenance/development).		
13		Will external entities providing IT support services have access to entrusted personal data?		
14		Are the servers on which personal data (individual files, databases) will be stored located outside the European Union? If so, in which country?		
15		Do your organisation have measures in place to protect data processing systems from so-called malware? If so, are they subject to cyclical updates, e.g.: based on service contracts with their suppliers?		
16		Do your organisation have measures in place to protect data from loss? If so, please list them briefly: e.g. regular backup, archiving, other (which)?		
17		Is accountability for the processing of personal data ensured in your organisation, i.e. is it possible to ascertain who modified or accessed a specific person's data and when in all IT systems used to process the entrusted personal data?		
18		Does your organisation's service contracts or procedures take into account the need to prevent protected data from being disclosed to unauthorised persons, e.g. when damaged equipment needs to be repaired or replaced?		
19		When data is transferred by telecommunications or on removable media, is its confidentiality, integrity and authenticity protected by cryptographic methods (e.g. file encryption)?		
20		Do you apply such measures and methods for processing data in IT systems as e.g.: pseudonymisation and encryption of personal data, continuous assurance of confidentiality, integrity, availability and resilience of processing systems and services, rapid restoration of availability of and access to personal data in the event of a physical or technical incident, regular testing, measurement and evaluation of the effectiveness of technical and organisational measures to ensure the security of processing? Please list which ones are used.		
21		Are there measures in place in your organisation to protect data from unauthorised access? If so, please briefly list them, e.g.: individual badges and passwords for access to IT systems, access control systems, firewalls, etc.		
22		Have the workstations and laptops used in your organisation, on which personal data is processed, been protected against unauthorised activation, e.g.: by means of a login and a password which is periodically changed and which the system forces to be changed?		
23		In your organisation, is access to the operating systems of the computers where personal data is processed secured through an authentication process using a user ID and a password known only to the authorised user? If so, are there systemic mechanisms in place to enforce periodic changes to user passwords?		

MakoLab

Cloud services

No.	Guidelines/Area	Questions	Answer (Yes/ Partly/ No/Not applicable)	Comments
1		Does the Supplier have an ISO 27017 compliant standard in place?		
2		Does the Supplier have an ISO 27018 compliant standard in place?		
3		Has the Supplier put in place an extensive security structure at all levels and across all types of services?		
4		Have controls and safeguards been put in place to ensure physical security?		
5		Has the Supplier put in place extensive security procedures for access to the Supplier's and Customer's systems?		
6		Has the Supplier put in place monitoring of the services made available to customers and any changes made to their systems?		
7		Has the Supplier put in place a mechanism to ensure that changes to any application services or hardware components must be authorised based on a personal role or group role, and that authentication is required to change applications or data?		
8		Does the Supplier have mechanisms in place to facilitate the deployment, upgrade and management of software and applications?		
9		Whether the Supplier has implemented documented formal processes for requesting, recording, approving, testing and accepting changes.		

10	**Information security for cloud services**	Has the Supplier put in place policies and procedures to ensure data integrity, including for backups?		
11		Does the Supplier provide fast response times in case of problems and competent staff dedicated to contacting the customer?		
12		Does the Supplier use standard APIs and data transformations so that standard cloud connections can be quickly created?		
13		Have data centres been equipped with natural disaster protection to adequately protect equipment and data?		
14		Has an additional network connection and power supply been provided, and has a business continuity and disaster recovery plan been prepared?		
15		Are regular safety audits conducted?		
16		Is the cloud infrastructure sufficiently scalable to accommodate the growing needs of customers?		
17		Does the Supplier ensure high availability of the service to customers 24/7?		
18		Does the Supplier provide high performance and reliability so that customers can access data quickly and efficiently?		
19		Does the Supplier provide performance reports?		
20		Does the Supplier guarantee compliance with laws and regulations, including data protection regulations?		
21		Do the applicable arrangements and provisions in the contract allow the Customer to safely terminate the Service, including the return of data in the appropriate format, scope and manner?		

22		Is there a risk of vendor lock?		
23		Are the applied solutions not a barrier to changing the supplier?		

MakoLab

Quality Management

Number	Guidelines/Area	Questions	Answer (Yes/ Partly/ No/Not applicable)	Comments
1.	Quality Management System	Does the Supplier have an implemented and certified Quality Management System in accordance with EN ISO 9001:2015? - If the Supplier has a certificate - please attach. - If the Supplier does not have a certified Quality Management System in accordance with EN ISO 9001:2015, skip to the questions below:		
2.		Does the Supplier have a Process Map and/or in some other form identified processes and the links between them?		
3.		Is there an analysis of risks and opportunities in the processes and are actions taken to mitigate risks and take advantage of opportunities?		
4.		Are staff competences being developed?		
5.		Does the Supplier supervise the production process?		
6.		Does the Supplier supervise its sub-suppliers?		
7.		Are corrective/preventive/improvement actions being implemented?		
8.		Has a process/way of overseeing non-compliant outputs been established?		

9.		Has a process/process for handling complaints been established?		
10.		Is there supervision of compliance with legal requirements?		
11.		Does the Supplier survey customer satisfaction?		

MakoLab

Environmental Management

Number	Guidelines/Area	Questions	Answer (Yes/ Partly/ No/Not applicable)	Comments
1.	Environmental Management System	Does the Supplier have an implemented and certified Environmental Management System in accordance with EN ISO 14001:2015? - If the Supplier has a certificate - please attach. - If the Supplier does not have a certified Environmental Management System in accordance with EN ISO 14001:2015, please skip to the questions below:		
2.		Does the Supplier carry out an analysis of risks and opportunities in relation to the environment?		
3.		Does the Supplier monitor the environmental impact of its activities?		
4.		Does the Supplier seek to reduce the amount of waste generated by its operations?		
5.		Does the supplier have a policy of reusing materials and products where possible?		
6.		Has the Supplier implemented a recycling programme?		
7.		Are there measures in place to reduce the negative impact on the environment?		
8.		Have specific environmental objectives been set?		

9.		Are the services/products provided by MakoLab environmentally friendly?		
10.		Has the supplier implemented an emergency preparedness and response process/procedure to prevent/mitigate adverse environmental impacts?		
11.		Does the Supplier require its subcontractors/sub-suppliers to comply with environmental requirements?		
12.		Does the Supplier require its subcontractors/sub-suppliers to reduce waste?		
13.		Does the Supplier require its sub-suppliers to apply a policy of reuse of materials and products where possible?		
14.		Does the Supplier reinforce environmental awareness among employees?		
15.		Does the Supplier monitor compliance with legal requirements in relation to the environment?		
16.		Does the Supplier submit environmental impact reports as required by law?		

MakoLab

Occupational health and safety management

No.	Guidelines/Area	Questions	Answer (Yes/ Partly/ No/Not applicable)	Comments
1.	Occupational Health and Safety Management System	Does the Supplier have an ISO 14001:2018 compliant Health and Safety Management System implemented and certified? - If the Supplier has a certificate - please attach. If the Supplier does not have an ISO 45001:2018 certified Health and Safety Management System, please skip to the questions below:		
2.		Does the Supplier identify risks and opportunities regarding OHS and manages them?		
3.		Are actions being taken to minimise risks and eliminate hazards?		
4.		Does the supplier prevent work-related injuries and health complaints?		
5.		Does the Supplier provide healthy and safe workplaces?		
6.		Is a workplace risk assessment in place?		
7.		Is health and safety training provided?		
8.		Is employee consultation and participation in health and safety activities ensured?		
9.		Is there monitoring of health and safety activities?		

10.		Are working conditions monitored?		
11.		Has the organisation developed procedures to respond to potential emergencies?		
12.		Have safety criteria been defined for subcontractors?		
13.		Are outsourced processes supervised in terms of health and safety?		

MakoLab

Sustainable development

No.	Guidelines/Area	Questions	Additional questions	Answer (Yes/ Partly/ No/Not applicable)	Comments
1	Corporate Social Responsibility	Does the Supplier have an ISO 26000 compliant Social Responsibility Management System in place?			
2		Does the Supplier publish a corporate social responsibility report?			
3	Compliance Management System	Does the Supplier have an ISO 37301 compliant Compliance Management System implemented and certified? - If the Supplier has a certificate - please attach.			
4	Anti-corruption Management System	Does the Supplier have an ISO 37001 compliant Anti-Corruption Management System in place and certified? - If the Supplier has a certificate - please attach.			
5	Supply Chain Safety Management System	Does the Supplier have an ISO 28000 compliant Supply Chain Safety Management System in place and certified? - If the Supplier has a certificate - please attach.			
6	Code of Conduct/Business Ethics Policy	Does the Supplier have a Code of Conduct and/or a Business Ethics Policy?			
7		Has the Supplier set up a system/solution to allow complaints and notifications of potential violations?			
8		Has the Supplier put in place whistleblowing regulations and protection against retaliation?			
9		Has the Supplier introduced financial responsibility regulations?			
10		Has the Supplier implemented anti-corruption and anti-money laundering regulations?			
11		Has the Supplier introduced regulations on fair competition and antitrust?			
12		Has the Supplier introduced conflict of interest regulations?			
13		Has the Supplier implemented data protection and security regulations?			
14		Has the Supplier put in place regulations for the disclosure of confidential information?			
15		Has the Supplier introduced intellectual property regulations?			

16		Has the Supplier introduced export control and economic sanctions regulations?			
17		Has the Supplier introduced regulations for counterfeit parts?			
18	**Labour Law**	Does the Supplier have Labour Regulations or any other document governing rights and obligations under Labour Law?			
19		Has the Supplier put in place wage and benefit regulations?			
20	**Training/Communication/Awareness**	Are staff trained on all implemented standards/codes/policies/procedures?			
21	**Human rights and gender equality**	Does the Supplier have a Human Rights Policy?			
22		Has the Supplier put in place regulations for child and juvenile labour?			
23		Has the Supplier introduced ethics regulations for recruitment?			
24		Has the Supplier introduced regulations on freedom of assembly?			
25		Has the Supplier introduced regulations on modern slavery, forced labour, human trafficking?			
26		Does the Supplier have regulations on equality, non-discrimination, diversity (including women's/men's/non-binary rights)?			
27		Has the Supplier introduced regulations on land, forest and water rights and forced eviction?			
28		Has the Supplier introduced regulations on the rights of minorities and indigenous peoples?			
29		Has the Supplier introduced regulations on the use of private or public security forces?			
30		Has the Supplier introduced health and safety regulations?			
31	**Energy Management System**	Does the Supplier have an ISO 50001 compliant Energy Management System in place and certified or has it undergone an energy audit? - If the Supplier has a certificate - please attach.			
32		Is there reporting of greenhouse gas emissions?			
33		Does the Supplier monitor energy efficiency?			

34		Does the Supplier use solutions that support decarbonisation, e.g. through the use of renewable energy sources?			
35		Are all substances and materials that the offered product contains or are used in the course of manufacturing/providing the service supervised and subject to control?			
36		Does the Supplier provide product safety data sheets?			
37		Does the Supplier declare compliance with REACH/ROHS requirements?			
		Does the Supplier declare that it applies supervision of the responsible use of raw materials:			
			Aluminium/Bauxite		
			Chromium		
			Cobalt		
			Copper		
			Cotton		
			Glass (silica sand)		
			Gold		
			Graphite (natural)		
			Skin		
			Lithium		
			Magnesium		
			Manganese		
			Mika		
38					

38	**Raw materials management**		Molybdenum		
			Nickel		
			Niob		
			Palladium		
			Platinum		
			Polysilicon		
			Rare earth elements		
			Rhodium		
			Natural rubber		
			Steel/iron		
			Tantalum		
			Tin		
			Wolfram		
			Zinc		
		Does the Supplier require its sub-suppliers to use the listed raw materials responsibly?			
			Aluminium/Bauxite		
			Chromium		
			Cobalt		

Copper		
Cotton		
Glass (silica sand)		
Gold		
Graphite (natural)		
Skin		
Lithium		
Magnesium		
Manganese		
Mika		
Molybdenum		
Nickel		
Niob		
Palladium		
Platinum		
Polysilicon		
Rare earth elements		
Rhodium		

Natural rubber		
Steel/iron		
Tantalum		
Tin		
Wolfram		
Zinc		