



Directorate - General of Human Resources

REMOTE WORK POLICY

Table of Contents

1. PURPOSE	3
2. SCOPE	3
3. RESPONSIBILITY	3
4. DESCRIPTION	4
A. Voluntary Remote Working	4
B. Transparency and Equal Rights	5
C. Jobs Suitable for Remote Working	5
D. Remote Working Requirements	5
E. Place of Work, Secrecy and Confidentiality	6
F. Safety and Health	7
G. Application and Approvals Flow	7
H. Working hours – Availability	8
I. Rights and Obligations – Right to Disconnect	8
J. Remote working duration	8
K. IT Infrastructure	9
L. Expenses	9
M. Compliance with current policies	9
N. Ensuring Business Continuity	9
O. Similar application to non-salaried employees	10

HR 6 REMOTE WORK POLICY

1. PURPOSE

The purpose of the Policy is to define the remote working framework for MYTILINEOS, enabling employees to apply, on a voluntary basis, for remote working at agreed intervals approved by the company, in accordance with the provisions of Law 4808/2021.

Working remotely, where this is feasible on a role-by-role basis, can improve employee productivity and effectiveness, reduce the environmental footprint of office operations and employee commuting to/from work, attract and retain Human Resources, and contribute to work-life balance.

2. SCOPE

The Remote Work Policy applies to employees of MYTILINEOS and its subsidiaries in Greece, whose work can be provided either entirely or partially remotely in an effective manner. If the individual employment contract stipulates otherwise than the current Policy, the individual contract, as in force, shall prevail.

The main criterion for an employee's eligibility for remote work is that the nature and type of work should not adversely affect the employee's productivity and efficiency.

3. RESPONSIBILITY

Compliance with and updating of the Policy is the responsibility of the Directorate General for Human Resources.

The Chief People Officer is the process owner. The table below shows the key roles of all stakeholders involved in the process as well as their main responsibilities:

KEY PROCESS ROLES		
Role	Description	Main Responsibilities
Chief Executive Director(s) & Chief Officers	Refers to the Chief Executive Director of the respective Business Segments, as well as the Chief Officer of the respective Division of the Central Functions, as depicted in the organization chart of the organization.	The Chief Executive Director of each Business Sector, and the Chief Officer of each Central Functions Division (hereinafter jointly referred to as the "Head"), gives the final approval for the percentage of employees who may be working remotely. In addition, he/she has approved the roles that can work remotely.

KEY PROCESS ROLES		
Role	Description	Main Responsibilities
Chief People Officer	Refers to the Chief People Officer, as reflected in the organisational chart of the organisation.	The Chief People Officer is responsible for changing/amending the current Policy and advising the other Heads on implementation of this Policy.
Directors	Refers to the Director of the respective Business Segment or Central Functions, as reflected in the organisational chart of the organisation.	Each Director is responsible for determining which roles under their responsibility can work remotely, ensuring the required productivity and effectiveness. He/she approves the remote working schedule for his/her Division.
HRBPs	Refers to HR Business Partners, as reflected in the organisational chart of the organisation.	HRBPs act as business advisors in relation to the roles that can work remotely, their percentage, as well as the implementation of the Policy and of the applicable relevant Legislation.
HR Operations	This refers to the responsible personnel in the Human Resources Operations Division, as reflected in the organisational chart of the organisation.	The competent employees are responsible for collecting and maintaining the entire record of employees working remotely. They ensure that the necessary actions are taken based on the applicable Legislation and requirements of Public Authorities. They offer guidance and advice to HRBPs regarding observance of the Policy and the requirements of Labour Law.

4. DESCRIPTION

This section describes in detail the various steps for proper implementation of the Policy.

A. Voluntary Remote Working

Remote working is voluntary for the employee in the sense that it can be applied following an agreement between the employee and the employer upon hiring or at a later date. To apply remote working, the employee must have signed a relevant individual agreement, explicitly specifying the remote working terms.

By way of exception, in the case of a documented health risk to the employee, as well as in the case of employees with permanent or temporary health problems, if the nature of their duties makes it possible to perform them through remote working and if the health risk can be mitigated or avoided with remote working, the employer must accept the relevant request of the employee always with the consent of the Occupational Physician, unless there is a special and important reason for its rejection, which it must set out and justify in writing to the employee.

In case of public health risk and emergency conditions and needs, the Company may unilaterally

implement a remote working system for the time required until the termination of these conditions.

B. Transparency and Equal Rights

The employer must inform the employee, in a transparent manner, not only of the conditions of performance, but also of the benefits and risks of remote working and, in addition, ensure that the personal data processed are limited to what is necessary for the purpose of processing and are kept for the time necessary to achieve this purpose.

In any case, organizing remote working for any reason must not lead to inequalities and discrimination (salary, career advancement opportunities, participation in vocational training programs) and affect employees' labour, insurance and social rights, nor lead to automated individual decision-making, including profiling of remote workers.

C. Jobs Suitable for Remote Working

Each job has different requirements in terms of collaborations, customer needs and results. These differences are key when deciding whether a role can be performed remotely.

At the beginning of each calendar month, or at shorter intervals in cases of exceptional circumstances and needs, the Head, taking into account the operational needs and the proper operation of their Division, as well as the nature of the employees' duties which may be carried out by remote working, decides which positions will be eligible, as well as any other details for its implementation.

When assessing whether a particular position is suitable for remote working, the Head will consider many factors, including, but not limited to:

- Whether the nature of the work to be performed remotely is operationally feasible
- Whether the overall quantity and quality of work performed can be maintained at the remote location
- If the position is managerial, whether an Executive in the position has the tools and resources to effectively manage direct reports remotely
- Whether the collaboration required by the position is easily achieved through video conferencing or other remote communication technologies

D. Remote Working Requirements

For an employee to make use of remote working, the following must cumulatively apply:

- Both parties (employee and employer) should agree.
- The employee should be able to perform as effectively as with in-office work.
- The employee should ensure the suitability of the location where he/she will provide remote work from. Specifically, the location should have a stable and uninterrupted Internet network and electricity, the desk and chairs should be suitable for office work and be ergonomic. In general, the space should be safe for office work, and it is the employee's responsibility to ensure that the above requirements are met.
- The employee should ensure the security of information he/she handles and that such information is not accessible to third parties who may be at the location. Special attention should be paid to verbal communication either through a computer, e.g., through teams or other such means, or by telephone, as well as to the use of the computer by unauthorized persons.
- The employee using Internet and Email services provided by MYTILINEOS, must comply with the

Internet and E-mail Use Policy. Any deviation from the requirements of MYTILINEOS policies, procedures and instructions is strictly prohibited. Exceptions must have a valid business reason and require prior approval by the Head of IT Infrastructure.

- The employee is required to observe all office security practices when working outside MYTILINEOS offices to ensure the integrity and secrecy of its proprietary and sensitive information.
- The employee must ensure that the selected location meets the required specifications enabling the smooth and effective performance of his/her duties through remote working and complies with the general rules of prevention, health and safety.
- The employee should refrain from forwarding emails to his/her personal email address, especially when the message content is not encrypted.
- The employee should avoid the physical transfer or printing of personal data resulting from department/corporate documents (e.g. company contracts, retail customer contracts, etc.) to the employee's home or to a place/space other than the workplace, to ensure that personal data cannot be leaked to unauthorised third parties.
- Additional requirements may exist, depending on the nature of the work and the equipment required to perform the work.

E. Place of Work, Secrecy and Confidentiality

The employee's residence address as declared to Human Resources is the place where remote working is deemed to be provided from. If the primary remote work location differs from the employee's primary or secondary residence address on record, the employee should follow the approval flow as described in subsection G.

It is the employee's obligation to ensure that alternative and occasional work locations are suitable to ensure the proper provision of the work on his/her part, as well as the integrity and secrecy of proprietary and sensitive information. The employee must observe and comply with MYTILINEOS policies and procedures just like during in-office work, as described in subsection M.

Locations that are open to the public, such as cafés, restaurants, and airports, are not suitable alternative work locations when handling confidential information. Similarly, locations open to the public are not suitable for group meetings to perform tasks in which sensitive information will be displayed on devices, physically distributed, or orally discussed. Employees must take all necessary measures to ensure that the alternative workplace meets all conditions for appropriate data security and confidentiality.

Remote workers agree to conduct all business meetings at locations that ensure the confidentiality of company information/data.

Employees must have secure network connectivity at all work locations. Employees are expected to understand the dangers of unsecured Wi-Fi networks and exercise increased caution when connecting to public Wi-Fi access points.

Company information and data must always be protected in a manner proportionate to their sensitivity and criticality and in compliance with applicable policies and procedures.

Devices provided by MYTILINEOS, including but not limited to computers, telephones, and cloud services, must be used solely by the remote worker. Family members, friends and any third parties are not allowed to use MYTILINEOS devices. Remote workers must never lend their laptop, credentials for MYTILINEOS systems or cloud-based services, or any other computer that stores information about the business activities of MYTILINEOS to others.

When conducting teleconferences, taking into account the relevant prohibitions and restrictions provided by law (Article 6 par. 6 of Law 4807/2021) for the provision of remote working, the remote worker shall be entitled, pursuant to the principle of data minimization, to activate the capability of the platform used (e.g. Teams) to participate using a microphone only, and not have the camera on all the time, especially when there are reasons that require it (e.g. protection of minors). In addition, it is recommended that the remote worker select features of the platform used that allow hiding the background by blurring or by adding an image (virtual background) to avoid the risk of revealing personal information that may arise from viewing.

Regarding videoconference recording, it is permitted only during lawful professional practice for the purpose of providing evidence of a commercial transaction or other communication of a professional nature, provided that both parties, after prior notification of the purpose of the recording, offer their consent. In any case, to perform such processing, the employer shall, prior to processing, take appropriate measures to protect personal data and, where necessary, carry out an impact assessment. An act of the Data Protection Authority determines how parties are informed and offer their consent, and how and for how long recorded conversations and the relevant data are kept.

F. Safety and Health

The employee must ensure that the selected location meets the minimum required specifications enabling the smooth and effective performance of his/her duties through remote working and complies with the general rules of prevention, health and safety. It is presumed that when working remotely the remote worker complies with all health and safety rules and that the remote working location meets the above specifications, as well as the requirements of subsection D.

In the event of an injury or any other incident related to the health and safety of the employee during work from home, the remote worker must immediately (or as soon as circumstances permit) report it to his/her line manager or to Human Resources

G. Application and Approvals Flow

An employee who wishes to work remotely, submits a written request to his/her line manager at least one (1) week before the start of remote working. The employee's request shall specify a) the number of remote working days, which should not exceed two (2) days per week and b) the address of the location where remote working will be provided from, which may not differ from the employee's primary or secondary residence already declared and included in the data kept by the Human Resources Operations Division. By way of exception, in the event of a health risk to the employee, as well as in the case of employees with permanent or temporary health problems, the provisions of subsection A shall apply.

Each Division Head, considering the operational needs, the need for the proper operations of the relevant function, and the employee's responsibilities, shall notify the employee, in writing or by electronic means, of his/her decision regarding the request within two (2) days from submission.

Before approving an employee's application, managers should ensure that the specific roles can perform under remote working without the employee's performance falling short of in-office work. In addition, they should ensure that approvals are given considering the equal treatment of employees by avoiding discriminatory decisions (whether favourable or unfavourable) towards specific workers.

Managers shall communicate the decisions on remote working requests to the Head and the respective HR Business Partners, as well as to the Human Resources Operations Division, no later than the last day of each current week. The Human Resources Operations Division is responsible for maintaining the overall remote working record, coordinating and monitoring the process, and implementing actions required by Labour Law.

The maximum percentage of employees per General Division of the Company that may be employed simultaneously through remote working may not exceed twenty-five percent (25%) of all the employees of that General Division who are eligible for remote working by the nature of their duties.

H. Working hours – Availability

Working hours remain the same as with in-office work. During working hours, the employee should be available and respond immediately to the work needs that arise. Specifically:

- Employees must be able to perform the same tasks, assignments, and other work obligations in their home office as they do when they work on MYTILINEOS premises.
- Employees are expected to be available to their supervisors, managers and colleagues during the agreed working hours and make their availability clear from their instant messaging work status (e.g.: Microsoft Teams).
- Employees should ensure that they can be reached by phone, instant messaging (e.g.: Microsoft Teams) or other communication tools used in the employee's department.
- MYTILINEOS expects the same level of professionalism and responsiveness from its remote workers as it does from employees working on the Company's premises.
- Employees must be available to attend scheduled meetings and participate in other required office activities depending on the needs of the respective Central Services or BU activity.
- Overtime must be pre-approved in writing by the employee's manager. Deviations from the agreed timetable must be approved in advance by the Head. The policy of MYTILINEOS will be observed for all absences.

I. Rights and Obligations – Right to Disconnect

Remote workers enjoy the same rights and obligations as employees performing their duties in-office at the organisation's premises, and are not excluded from the company's procedures such as promotions, raises, career advancement opportunities, participation in vocational training programs, etc.

A remote working employee has the right to disconnect, which consists of his/her right to completely abstain from providing his/her work and not to communicate digitally and not to respond to phone calls, emails, or any form of communication outside working hours and during his/her legal leaves of absence.

Within the framework of its managerial prerogative, the employer may take the necessary measures related to checking the remote worker's work performance in a way that respects his/her privacy and fundamental rights and is in line with the protection of personal data. The use of a webcam or a keystroke recorder to check the employee's performance is prohibited. Furthermore, monitoring outgoing Internet traffic for the above purposes, using appropriate software (e.g., TLS appliance), is not justified, when they can be achieved by softer preventive means.

J. Remote working duration

Upon approval of the application, the employee is considered to be working remotely and the employee can work from the declared remote working location in the manner agreed on a case-by-case basis between the employee and his/her respective Line Manager and General Manager.

K. IT Infrastructure

The use of devices (e.g., laptops) that are not certified equipment of MYTILINEOS for the performance of the remote workers' duties during remote working is expressly prohibited. It is also prohibited to carry other IT equipment from the office to the remote working location (e.g., monitors, docking station, printers, etc.).

L. Expenses

The Company shall pay an amount to cover the cost of remote working and use of the remote worker's home space, only for remote working days and in proportion to the percentage of remote working in relation to the total working time, the amount of which may not be less than the minimum statutory amount applicable each time, as defined by the relevant legal or regulatory provisions. Payment shall be made each month and relate to the month preceding the payment.

The Company will in any case bear the cost caused to the employee by this form of work and in particular the cost of equipment, unless it is agreed to use the employee's equipment, telecommunications, equipment maintenance and fault repair.

Meanwhile, the Company is obliged to provide the employee with technical support for provision of his/her work and undertakes to reimburse any repair costs of the devices used for work or to replace them in case of fault. This obligation relates to devices owned by MYTILINEOS and have been given to the employee for the performance of his/her duties.

M. Compliance with current policies

It is of utmost importance that the employee observes and complies with MYTILINEOS policies and procedures just like during in-office work.

Examples of policies that all employees must adhere to are:

- Code of Business Conduct
- MYTILINEOS Employment Rules
- Human Rights Policy
- Internet and E-mail Use Policy (PLC.IT.SEC.04)
- Information Security Strategy, General Principles and Governance Policy (PLC.IT.SEC.01)
- Acceptable Use of Information Systems and Code of Conduct (PLC.IT.SEC.03)
- Leave of Absence Planning and Granting Procedure
- Personal Data Protection Policy

An employee should be able to demonstrate the required flexibility in any change of the remote working schedule and be prepared to immediately return to his/her physical workplace, when and if requested by his/her line manager.

N. Ensuring Business Continuity

Remote workers must notify their line manager in a timely manner of situations that affect their ability to complete their tasks.

A remote worker should have identified alternative appropriate working arrangements in situations that may affect the employee and therefore business continuity, including, but not limited to, Internet and power outages.

O. Similar application to non-salaried employees

As to the way the remote working framework is organised, the above policy also applies mutatis mutandis to consultants, associates and other professionals who offer services to the company under a works contract or independent services contract or other legal relationship, if and to the extent that they are consistent with the nature of their contractual relationship.