

# Privacy Regulation (GDPR)- Directive (EU) 2016/680 & Safety & Hygiene at Work (SHW)



## Notes



**"ICON WOM-EN"** - Integrating Innovation and Promoting Cluster Organization in WOMen Enterprises

Action 4.2 Educational Platform - Action 4.3. Educational Material  
Implementation: PIKEI OE- PROTEA IKE

Project co-funded by the European Union, the European Regional Development Fund (ERDF) and National Funds of Greece and Italy

# About course

This module deals with two concepts:

- the Personal Data Protection Regulation (GDPR)
- the Safety and Health at Work.

**LEARNING OBJECTIVES** of the Module is the understanding by the potential entrepreneur of the following:

- The European General Data Protection Regulation (GDPR),
- Safety and Health at Work (SHW) regulations
- How to apply them for the smooth & safe operation of a business.

**EXPECTED RESULTS** of the Module are the Understanding by the Entrepreneur of the need to apply the rules of GDPR and SHW as well as to whom they should be addressed for their correct application in their business.

# Content

1. GDPR - DEFINITIONS & BASIC CONCEPTS
2. GDPR IMPLEMENTATION METHODOLOGY
3. RIGHTS & OBLIGATIONS
4. LEGAL FRAMEWORK & CERTIFICATIONS
5. PRACTICAL CONFORMITY MEASURES
6. RESPONSIBLE FOR IMPLEMENTATION AND CONTROL OF GDPR MEASURES
7. SHW- DEFINITIONS & BASIC CONCEPTS
8. RISK FACTORS AT WORK
9. EXISTING LEGAL FRAMEWORK & CERTIFICATIONS
10. RESPONSIBLE FOR IMPLEMENTATION AND CONTROL OF SHW MEASURES
11. BASIC PRINCIPLES OF OCCUPATIONAL RISK ASSESSMENT
12. WORKING TIME ORGANIZATION

SECTION A - Compliance of companies with  
the new Privacy Regulation (GDPR)- Directive  
(EU) 2016/680

# 1. GDPR - DEFINITIONS & BASIC PRINCIPLES

Potential entrepreneurs should be aware of the following terms:

- **EUROPEAN GENERAL REGULATION:** The Regulations have binding legal force in all Member States and enter into force on a fixed date in all Member States
- **EUROPEAN DIRECTIVE:** The Directives set out certain results to be achieved, but each Member State is free to decide how to transpose the Directives into national law.
  - The General Data Protection Regulation (GDPR) was implemented from 25/5/2018 in Greece
- **OTHER PERSONAL DATA:** Data such as identification data (name, age, physical characteristics, marital status, work status, etc.)
- **EASY PERSONAL DATA:** Data such as (racial/ethnic origin, political opinions, religious/philosophical beliefs, health status, erotic direction, participation in related groups of the above)

The basic principles of the GDPR are the following::

- The General Regulation on the Protection of Personal Data GDPR applies to every Public and Private enterprise and Organization that collects, processes or manages personal data.
- The GDPR does not concern data of legal entities (companies, etc.) unless it is a Sole Proprietorship or Sole Proprietorship.
- A Company must apply the Regulation when collecting and / or processing personal data of customers, employees and external partners.

# 1. GDPR - DEFINITIONS & BASIC PRINCIPLES

## What data are considered personal?

- Personal data are information relating to an identified or identifiable person in life.
- Personal data that have become anonymous, encrypted or for which aliases have been used, but which can be used to re-identity an individual, remain personal data and fall within the scope of gdpr.
- GDPR protects personal data regardless of the technology used to process it. It is technologically neutral and applies to both automated and manual processing. It also doesn't matter how data is stored in digital or print format.

## Examples of personal data

First and last name, home address, e-mail address, e.g. last name@company.com, card ID number, location data (e.g. location data function on a mobile phone), internet protocol (IP) address, cookie ID, data held by a hospital or doctor, which could be a symbol that identifies only one person.

## What data are NOT considered personal;

- Personal data that have become anonymous so that the person is not identifiable are no longer considered personal data.
- For the data to be truly anonymous, anonymization must be irreversible

## Examples of data that are NOT considered personal

Company registry number, e-mail address of the type information@company.com, anonymous data

# 1. GDPR - DEFINITIONS & BASIC PRINCIPLES

The following specific categories of personal data are considered 'sensitive' and receive special protection in accordance with GDPR

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- participation in a trade union
- processing genetic data biometric data for the purpose of the undisputed identification of a natural person;
- health sex life or sexual orientation.

The **Data Processing Officer** (DPO) is responsible for determining the processing ratio (Processing Policy) and must be able to demonstrate at all times that it applies the GDPR Regulation.

The main task of the **Data Protection Officer** (DPO) is to inform and advise the Data Processing Officer or the processor and the employees who process personal data, for their obligations arising from the data protection regulation.

Additionally:

- Monitors compliance with the GDPR, oversees the policy implemented by the Data Processing Officer and suggests practices and solutions when requested
- Trains the staff and management of the company on GDPR issues
- Collaborates with the supervisory "Personal Data Protection Authority"
- Acts as a point of contact for the supervisory authority on processing issues

## 2. GDPR APPLICATION METHODOLOGY

But how does the regulation apply to a company? It is prudent for the Property and the Management of each business to follow a Methodology in order to be sure that the procedures of the business are in accordance with the Regulation.

### Methodology of application of GDPR Regulation in a company (1)

- Preparation – Mapping of current situation (identify areas where the company already meets the requirements and areas that need additional control mechanisms)
  - **Recording of managers per department.** The departments of the company are identified, the data as well as the managers are recorded per department and per file. The log is recorded in the data processing register.
  - **Recording of available human resources per department** made available to the Head of Protection. Establishment of a representative working group in relation to the existing data and the organizational units that process them.
  - **Recording and mapping of Personal Data collected,** processed and distributed by the company. Recording by processing, file and type of data stored and circulated. Capture of personal data flow (DATA FLOW MAP) by category, in order to create the Archives of the Processing Activities, as required by the Regulation and to have a complete record of the management of personal data. Determining the type of processing, sources of origin, data retention time.
  - **Determination of Legal Basis - correctness check.** The Legal Basis on which the data processing is based is determined, the correctness, completeness and validity, the recording and documentation and the manner of notification to the subjects are examined.
  - **Mapping the installed information system.** Control, evaluation, recording of information system and network infrastructures and operating procedures.
  - **Documentation Recording.** Mapping of the existing documentation, concerning the security of personal data, examination of its completeness and security.



## 2. GDPR APPLICATION METHODOLOGY

But how does the regulation apply to a company? It is prudent for the Proprietor and the Management of each business to follow a Methodology in order to be sure that the procedures of the business are in accordance with the Regulation

### Methodology of application of GDPR Regulation in a company (2)

- Development of data protection policies & procedures
  - **Development of data collection, processing and data security policy.** Manual of data collection and processing policy procedures that may be part of the company's security policy.
  - **Writing a security policy.** The Security policy is a document of the Controller which describes the security objectives and the corresponding procedures to be followed. It includes: a) organizational security measures regarding the responsibilities of those involved in the management and processing of personal data, training, security incident management, personal data destruction, b) technical security measures regarding user management, identification, security, information system operation. (c) physical security measures, specifying the role of each person involved within the undertaking, the responsibilities, responsibilities and duties relating to security.
  - **Development of a security, data recovery and destruction plan.** Plan referring to the measures of protection, recovery and restoration of information systems and technological infrastructures in case of emergency.
  - **Design of a mechanism for detecting violations.** Checking an existing or implementing a new mechanism for detecting breaches (security Breaches) or simple security incidents (security incident) with automatic logging (Security log). It is part of the mandatory documentation and a prerequisite for the timely response to a report of violations.
  - **Event management planning.** The incident management plan is the document that states the procedures to be followed in case of security breach. It also describes the appropriate review process.
  - **Develop an action log.** Important record of documentation of compliance or progress made towards compliance with the requirements of the Regulation.

## 2. GDPR APPLICATION METHODOLOGY

Training BEFORE the company's compliance with the GDPR

- Information & training to all employees to understand the critical points of the regulation and contribute with suggestions, observations and ideas for compliance

Training AFTER the company's compliance with the GDPR Regulation

- Information & training to all employees about the system, application procedures by department/address, the notification process in case of loss of personal data

INTERNAL GDPR Compliance Assessment & Inspection

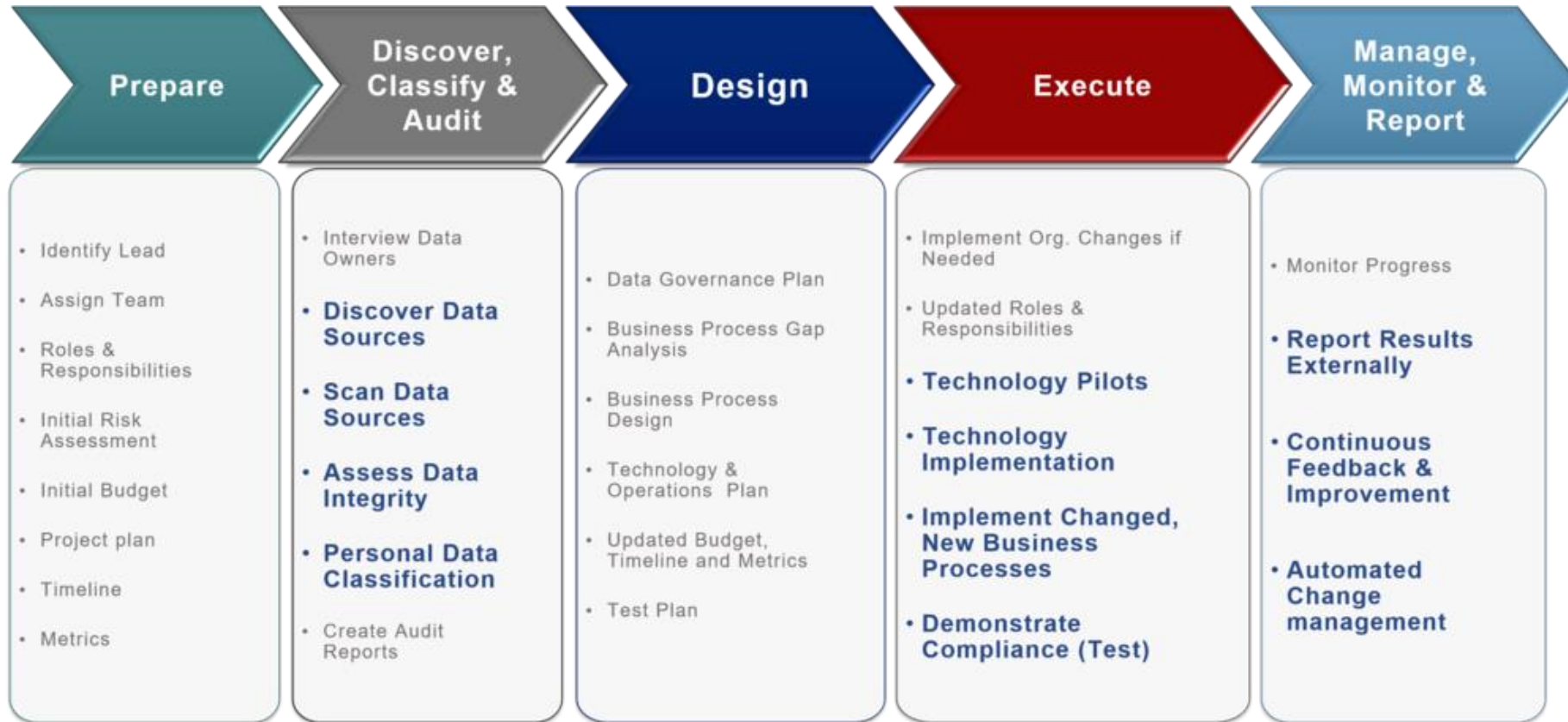
- Gdpr compliance inspection and evaluation to better ensure and adopt best practices is initially internal (by DPO and its team)

EXTERNAL GDPR Compliance Assessment & Inspection

- The inspection and conformity assessment of the entire system by external Certified inspectors (legal, organisational & technical) in order for the company to be certified with the GDPR SEAL

# 2. GDPR APPLICATION METHODOLOGY

Methodology for the application of the GDPR Regulation



# 3. RIGHTS & OBLIGATIONS

## Rights of The Original Owners of Personal Data

1. Right to **information** and **access** to data: Clearer information when collecting data for processing and the right to access it. Data owners have the right to receive clear and comprehensible information about who processes their personal data and why. They can also ask all companies to have access themselves and find out exactly what information the companies hold about them.
2. Right to **correct** / **complete** the data: The data owner may request from the Business Processor to correct or complete inaccurate data.
3. Right to **restrict processing**: The owner may request the refusal to process the data under certain conditions e.g. for "profiling" or for marketing.
4. Right to **object** to the **processing**: If not observed for a specific legal and declared purpose.
5. Right to be **forgotten**: When the processing and preservation of personal data is no longer desired, there is a right to request their deletion from the companies' databases.
6. Right to **compensation** by going to court: If the data owner suffers damage eg theft of his data by hacker cyber attacks against companies.
7. Right to data **portability**: The data owner can request to obtain his data in a structured form from a Processor and pass it on to another Processor.

## 3. RIGHTS & OBLIGATIONS

### Basic obligations for Data Processing Officers (DPOs)

- 1. Responsibility:** The controller has the responsibility to prove that it takes all appropriate organizational and technical measures to protect personal data and that it complies with the GDPR Regulation.
- 2. Data protection by design:** The Regulation requires the implementation of products and services (electronic and non-electronic) that during their initial design create friendly conditions for the protection of your data. For example, online social networking services should allow you to choose settings that will best protect your personal data.
- 3. Data protection by default:** The Regulation requires the implementation of appropriate technical and organizational measures to ensure that, by definition, only the data necessary for the purpose of processing are processed.
- 4. Processing security:** The controller and the processor must implement appropriate technical and organizational measures in order to ensure the appropriate level of security.
- 5. Reporting of data breaches:** The controller has an obligation, as soon as he / she realizes a breach, to inform within 72 hours, the competent supervisory authorities and you, as long as the breach puts you in serious danger.

## 3. RIGHTS & OBLIGATIONS

- 6. Impact assessment and prior consultation:** When processing may pose a high risk to human rights, in particular because it is systematic, large-scale, specific data categories and based on the use of new technologies, the controller should conduct an impact assessment on the Data protection impact assessment. When, on the basis of the impact assessment carried out and despite the provision of protection measures, there is still a high risk of processing, the controller is obliged to consult the supervisory authority in advance.
- 7. Data Protection Officer (DPO):** Provides, under certain conditions, the definition of "data protection officer" who has guarantees of independence and monitors compliance with the law, being at the same time the point of contact with the supervisory authority.
- 8. Codes of conduct:** The development of codes of conduct by controllers is encouraged and submitted to the supervisory authority for approval. In case of trans-European activity, the opinion of the European Data Protection Council is also sought.
- 9. Certification:** The introduction of certification mechanisms, seals and data protection marks to prove compliance with the Regulation or to demonstrate the provision of appropriate guarantees during processing is encouraged.

# 3. RIGHTS & OBLIGATIONS

## Basic obligations for the Data Protection Officer (DPO)

1. The Data Protection Officer (DPO) is required in the following cases:
  - The processing of data is carried out by a **public authority or public body** (including natural or legal persons under public or private law exercising public authority). Courts are excluded when acting under their jurisdiction.
  - Regular and systematic **monitoring of data subjects on a large scale** (eg insurance or banking services, telephone or internet services, provision of security services, all forms of monitoring and "profiling" on the Internet, such as for behavioral advertising purposes).
  - **Large-scale processing of specific categories** of data (eg in the context of the provision of health services by hospitals) or personal data relating to criminal convictions and offenses.
  - **Therefore, small businesses that do NOT collect large amounts of data are NOT required to hire / designate a DPO**
2. Each organization can designate a DPO. Even in cases where **the DPO designation is not mandatory**, such voluntary actions are encouraged. When an organization designates a DPO on a voluntary basis, the same requirements will apply in relation to its definition, position and tasks as if the definition were mandatory
3. The Data Protection Officer (DPO) **facilitates the compliance** of the Data Processing Officer (DPO) and the processor with the provisions of the GDPR and mediates between the various stakeholders (eg supervisors, data subjects).

### 3. RIGHTS & OBLIGATIONS

4. Its role is **advisory (not decisive)** and it does not bear **personal responsibility** for the non-compliance of the company / organization and its employees with the GDPR Regulation.
5. Be the first **point of contact** for supervisors and data subjects (employees, customers, etc.).
6. To **cooperate** with the supervisory authority and to represent the company / organization
7. The **contact details** of the Data Protection Officer (DPO) must be made public in order to ensure seamless communication with data subjects.
8. In addition, **information concerning the definition** of DPO must be notified to the supervisory authority.
9. Monitor **internal compliance** with the Regulation and other data protection provisions (eg identification and management of processing activities, staff training, internal audits)



# 4. LEGAL BACKGROUND & CERTIFICATIONS

- GDPR legislation
  - European General Data Protection Regulation (GDPR)  
<https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016L0680&from=EL>
  - National Law 4624/2019 "Personal Data Protection Authority, implementing measures of Regulation (EU) 2016/679 of the European Parliament ....»  
<http://www.et.gr/index.php/anazitisi-fek> find Gazette 137/A/29-8-2019
- Certification for GDPR
  - Certification is **optional**, voluntary and available through a transparent process,
  - It does not limit the liability of the person responsible or the executor for compliance with the GDPR,
  - It shall not prejudice the duties and responsibilities of the supervisory authorities.
  - The Personal Data Protection Authority encourages its introduction because it enables the improvement of transparency by allowing data subjects to quickly assess the level of data protection of the relevant products and services
  - Certification shall be granted by certification bodies which have previously been accredited to:
    - have an appropriate level of expertise in relation to the protection of personal data, and
    - have informed the competent supervisory authority.
  - The maximum period for granting certification shall be **three years** and may be renewed under the same conditions, provided that the relevant criteria are still met.

## 4. LEGAL BACKGROUND & CERTIFICATIONS

- DPO Certification
  - The DPO shall be appointed in particular **on the basis of its experience** in the field of data protection law and practices, as well as on the basis of its ability to carry out its tasks;
  - The **necessary level of experience** should be determined according to the **data processing operations** performed and the protection required by the personal data being processed.
  - At the same time, the DPO must have **knowledge of the field of activity of the organization** or body in which it works but also of **information technologies and data security**.
  - The Regulation does **not impose a mandatory requirement** for DPO certification, nor does it even encourage certification on an optional basis.
- In any case, Certifications for DPO and GDPR in general, must be issued by **Certification Bodies** (Companies / Individuals) that have been previously **accredited** by the National Accreditation System (ESYD).

# 5. PRACTICAL COMPLIANCE MEASURES

Here are some practical steps for small businesses to Comply with the Regulation

## Passwords

- Use strong security passwords
  - At least 8 characters, with mandatory use of lowercase and uppercase letters, numbers and symbols
- Different passwords per application
- Frequent password changes

## USE Antivirus software

- Regularly update the software to deal with new threats
- Regular file checks
- File encryption

## Business Software Update

- Compatibility testing between critical applications
- Enable automatic updating of critical applications
- Installing new versions of critical applications

## PRECAUTIONS in the face of suspicious attachments of incoming emails

- Sender check
  - Intersection with the sender to send an attachment
- Enable file extension display in general
- Check for suspicious attachments through Antivirus software

## BACK-up

- On the cloud
- On hard drives
- In documents (whenever allowed)

## PERSONAL CONFORMITY

- Security awareness
- Use of (web) seminars
- Information on the tools and technologies used
- Simulations in cyber-attack scenarios (if possible)

## 6. Responsible for the Implementation & Control of GDPR Measures

- The application of the GDPR regulation to the Companies that collect, process or manage personal data is done by the Data Processing Officer (DPO) under the advisory guidance of the Data Protection Officer (DPO)
- An employee can be appointed to work as a Data Processing Officer or DPO, alternatively an outsider. Especially the role of DPO is:
  - To represent the Processing Officer or the Executor of the Processing (of the enterprise) vis-à-vis the authorities
  - Advise the Management of the Company in matters of personal data protection
  - To suggest directly to the Company Management the appropriate data protection policies considering them as a valuable asset of the Organization
- The implementation of the GDPR is monitored in every EU country by national authorities

## SECTION B – Safety and Hygiene at Work

# 7. SHW - DEFINITIONS & BASIC PRINCIPLES

What do the following terms mean?

- **HAZARD:** Any source, condition or activity potentially causing human injury or illness or a combination of these
- **DANGER:** A combination of the likelihood of a dangerous event or exposure / s and the severity of the injury or illness that may result from them.
- **WORK ACCIDENT:** Defines the external impact, unintentional and sudden event, which causes physical injury to an employee. The demarcation against occupational disease is the "sudden", while towards self-injury the "unintentional".
- **NEAR ACCIDENT:** An event, ie an event related to work where there was no injury or occupational disease or death is characterized as a near accident

What is Safety and Health at Work?

✓ By Occupational Safety & Health, we mean maintaining such conditions at work, which ensure the **health** and **well-being** of employees.

✓ Good health at work contributes to better **public health** in general, but also to improving the **productivity** and **competitiveness** of a business.

✓ On the contrary, any health and safety problems at work have high **costs** for both the victim and the company, but also for the **social security system**.

✓ Therefore, it is necessary to ensure **pleasant** and **safe** working conditions for employees and to take care of their general well-being.

✓ It benefits both **employers** and **employees**, but also **society** at large.

# 8. RISK FACTORS AT WORK

## Common Risk Factors

**The microclimate of the workplace.** The climate in the workplace (often referred to as the "microclimate") is greatly influenced by general climatic conditions. In hot weather, job performance falls if the climatic conditions prevailing in the workplace are not regulated.



**Improper Workplace Temperature** causes additional fatigue and potential health hazards. It is regulated by installing air conditioners or shading outdoors.



**Improper degree of humidity in the workplace.** It creates intolerable working conditions and discomfort in the workers' breathing, as well as exhaustion. It is fought with dehumidification systems and frequent and adequate ventilation of the space.



**Inadequate lighting of the workplace.** Inadequate lighting causes strain on the optic nerves. It is fought by ensuring the existence of natural light. If it is not possible with the use of technical lighting of good quality and correctly placed as well as the use of bright paint colors of the walls indoors.

# 8. RISK FACTORS AT WORK

## Common Risk Factors



**Workplace or outdoor environment noise.** Noise is characterized by sound that is unpleasant and unpredictable. In recent years, noise levels have increased. Machines that have become more efficient and faster have also increased noise levels. Noise reduction can be achieved by using sound insulation and in special cases by using headphones - earmuffs.



**Chance of fire.** The start of fire can result from negligence of a natural person or from material failure e.g. creating sparks in electrical appliances, leakage of flammable gases, etc. It is treated with fire safety measures, fire extinguishers, sprinklers, fireproof uniforms, etc. provided in the fire protection study.



**Existence of chemicals.** The increase in the use of chemicals has inevitably led to an increase in the risks arising from them, both for employees and for populations close to companies that use chemicals as well as for the environment in general. They are treated with Personal Protection Measures: masks, gloves, wellies, etc. but also with special materials to limit the expansion of chemicals.



# 8. RISK FACTORS AT WORK

## Common Risk Factors



**Any biological substances used or produced.** Bacteria, viruses, fungi and parasites are present in many workplaces. These organisms are usually invisible, which means that the dangers they pose may not be perceived. They are controlled with special disinfection facilities and Personal Protection Measures.



**Ergonomics of staff workstations.** It is affected by the improper design of workplaces (insufficient space, lighting, ventilation, abnormal and painful posture, etc.). The correct distances and other factors are assessed through a special study that removes obstacles. In addition to the defined work stations, respectively there is an important issue of ergonomics in the technical tasks of the staff e.g. when removing items.



Those of the aforementioned **Risk Factors** that exist in the company, should be examined in detail and taken into account in the **Risk Assessment Study**.

# 9. Existing Legal Framework & Certifications

## National Legal Framework

The basic legal framework in Greece is included in the framework law L.3850 / 2010 "Ratification of the Code of laws for the health and safety of workers" whose main points include:

### **Obligations of Employers**

- to ensure the safety and health of workers in all aspects of work, in particular on the basis of the general principles of prevention & protection through appropriate equipment, free of charge for workers
- assess occupational hazards, even when selecting different types of equipment and arranging workplaces, and establish protection and prevention services
- to record and report work-related accidents
- to organize first aid, fire safety, evacuation of workers in case of danger and to take measures in case of serious and immediate danger
- ensure that every worker is adequately and professionally trained in occupational safety and health
- inform employees, consult them and facilitate their involvement in all matters relating to occupational safety and health

### **Obligations of Employees**

- make proper use of machinery and other means, personal protective equipment and security systems
- identify any working conditions that present a serious and immediate danger, and any defects in the protection systems
- contribute to meeting the health care requirements imposed and to facilitate the employer to ensure that the working environment and conditions are safe and secure

# 9. Existing Legal Framework & Certifications

## European Legal Framework

The European legal framework is based on Council Directive 89/391 / EEC “Measures to improve the safety and health of workers at work” whose main points include:

### ➤ Obligations for Employers

- are obliged to ensure the health and safety of their employees. This includes risk assessment and avoidance, developing a coherent safety policy and providing appropriate training to staff
- appoint a person responsible for risk prevention at work
- take the necessary precautionary measures regarding first aid, fire safety and evacuation of premises
- assess the risks that specific employees may face and ensure that the necessary safeguards are implemented
- provide employees and / or their agents with all relevant information regarding potential health and safety hazards and measures taken to prevent them
- advise employees and / or their representatives and include them in all discussions about health and safety at work
- ensure that every worker is provided with adequate safety and health training in relation to his or her job

### Other key points

- Every employee is responsible, as much as possible, for the care of his own health and safety as well as that of his colleagues.
- Special protection should be provided to workers who may be sensitive to potential hazards in the workplace

All the Governments of the member states of the European Union have the obligation to harmonize their legislative frameworks with the Community Directive 89/391 / EEC.

# 9. Existing Legal Framework & Certifications

## Certifications in Safety & Hygiene at Work

- The standard ISO 45001 - Occupational Health & Safety, was published in March 2018 by the International Organization for Standardization.
- It replaced the UK standard BS OHSAS 18001 which was widely adopted internationally.
- Greek standard ELOT 1801: 2008 is in line with BS OHSAS 18001.

Some of the benefits of implementing and certifying a Health and Safety at Work Management System in a business can be summarized as follows::

1. Alignment with the current legal framework and regulations
2. Commitment to continuous improvement of measures
3. Providing protection and prevention services to reduce and eliminate occupational accidents and occupational diseases
4. Identifying occupational risks arising from the way the company operates and minimizing them
5. Improving working conditions and increasing employee efficiency, leading to increased production and business viability

# 9. Existing Legal Framework & Certifications

## Certifications in Safety & Hygiene at Work

6. Creating a safe working environment for employees, partners and visitors of the company
7. Reduction of operating costs as it is considered an investment
8. Improving the business image
9. Use of the certificate as a tool for compliance with laws, regulations, regulations, but also standards and specifications on issues related to the health and safety of employees
10. Ability to deal with emergencies
11. Use of the certificate as a marketing tool

### **Important**

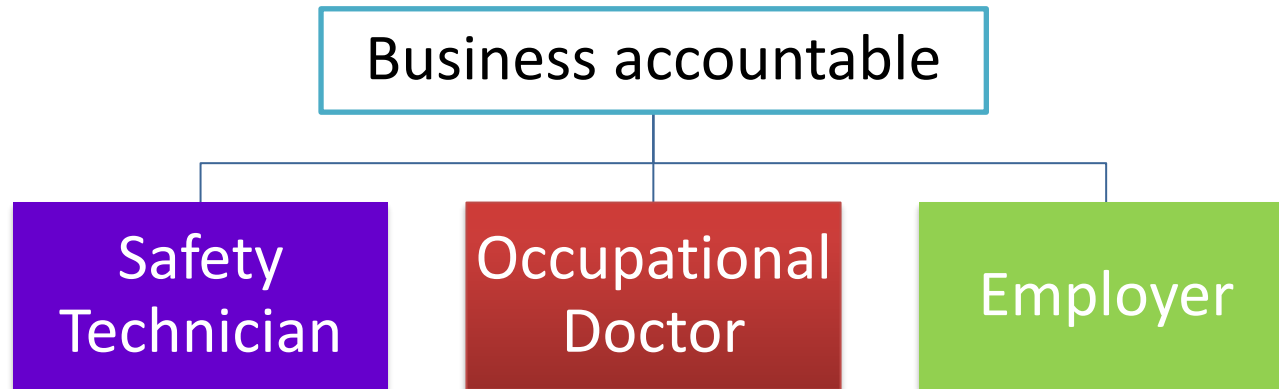


Obtaining and applying the procedures of an ELOT / ISO certificate is not a requirement of the law!



## 10. Responsible for the Implementation & Control of SHW Measures

Like any regulation, the rules of Safety and Health at Work are applied and supervised by specific, competent, natural persons defined by law.



As "Responsible", there are considered the people who are responsible for the planning and observance of the Safety and Hygiene measures of the Company.

# 10. Responsible for the Implementation & Control of SHW Measures

## Safety Technician

1. Required in every company that employs at least 1 employee.
2. The hours of his presence in the company depend on its degree of risk (A-High, B-Medium, C-Low) and the number of employees in it. \*
3. It can be an employee, an external partner, or even the owner, under certain conditions. Must be declared to the Labor Inspectorate.
4. He is responsible for the preparation & control of the Risk Assessment and the definition of measures to eliminate (or reduce) it.
5. Provides tips and advice, either in writing or orally, on ensuring employee safety and prevention to avoid accidents at work.
6. He has the obligation to record the written instructions in a special book of the company. This book is bookmarked and should be considered by the labor inspectorate. The employer is obliged to sign that he was aware of the suggestions that have been registered in this book.
7. Advises on issues related to the design, planning, construction and maintenance of facilities.
8. Selects and controls the effectiveness of personal protective equipment.
9. Shapes positions and arranges the work environment.
10. Informs the employer of any omissions in the hygiene and safety measures.
11. Informs employees about any risks arising from their profession.
12. Advises employees on occupational risk prevention measures.
13. Schedules training seminars and safety & hygiene exercises in collaboration with the Management and other bodies e.g. Fire Service.

## 10. Responsible for the Implementation & Control of SHW Measures

### Occupational Doctor

1. Required in companies with a staff of more than 50 people
2. The hours of his presence in the company depend on its degree of risk (A-High, B-Medium, C-Low) and the number of employees in it.
3. It must be declared to the Labor Inspection Body where the dates and times of its presence in the company are mentioned.
4. Visits every point of the company that employs staff and conducts inspections in all areas and workplaces in relation to occupational health and safety and the prevention of accidents at work.
5. Prepares and / or updates the individual medical file of each employee.
6. Issues certificates of suitability of employees.
7. Explains the need for the proper use of personal protective equipment.
8. Investigates the causes of occupational diseases, analyzes and evaluates the results of research and proposes measures to prevent these diseases.
9. Informs employees about how to deal with emergencies that may affect their health.
10. Takes care of the medical examinations and records the results in the individual medical file of the employee.
11. Enters his suggestions in the special Instruction Book of the installation. The person in charge of the installation is informed by signature of the instructions recorded in this book.
12. Maintains Medical Confidentiality in favor of the employee.



## 10. Responsible for the Implementation & Control of SHW Measures

### Employer

1. Ensures the safety and health of employees in all aspects of work and takes measures to ensure the health and safety of third parties.
2. Uses the services of a security technician regardless of the number of employees and the activity of the company.
3. Uses the services of an occupational physician, in companies with 50 or more employees.
4. Has at its disposal a written assessment of occupational hazards to safety and health including those involving groups of workers exposed to particular hazards (OCCUPATIONAL RISK ASSESSMENT STUDY).
5. Has the obligation to report the Occupational Accident.

## 10. Responsible for the Implementation & Control of SHW Measures

The application of the above rules as they apply to each type of business depending on the risk and the size of the staff, is controlled by the State.

### Control Officers

Responsible Ministry for Occupational Safety & Health is usually the Ministry of Labor and Social Affairs and specifically:

- the General Directorate of Occupational Conditions and Hygiene
- the Labor Inspection Body

Responsibilities of a Labor Inspection Body can be:

1. To control all companies / holdings for the observance and implementation of the provisions of the labor legislation.
2. Carry out inspections, measurements, sampling and surveys to determine whether the provisions of labor law are complied with.
3. To investigate the causes of fatal and serious occupational accidents and occupational diseases.
4. To examine the submitted complaints and requests of employees. It is noted that complaints are submitted in writing or orally, by name or anonymously.
5. To impose administrative sanctions on violators or to appeal to the court for the imposition of criminal sanctions.
6. To intervene conciliatively to resolve individual or collective labor disputes.
7. The Labor Inspectors can enter freely around the clock in all workplaces.

## 10. Responsible for the Implementation & Control of SHW Measures

### Books to keep in a business (low risk):

1. Special book, which must be paginated and considered by the locally competent Labor Inspectorate and in which the written instructions to the employer of the Safety Technician and the Occupational Physician (if any) will be recorded.
2. Special accident book in which the causes and the description of the accidents will be written in detail as well as the days of the employees' absence from work
3. Special book that will be registered signed by the person in charge, who did the maintenance or inspection of the security systems, the maintenance date and the relevant remarks.
4. Occupational Risk Assessment Study.

# 11. Basic Principles of Occupational Risk Assessment

## Occupational Risk Assessment

- According to the relevant legislation, every employer must have at his disposal a written Occupational Risk Assessment for the Work Environment of his Company.
- The work environment can include physical, chemical, biological, ergonomic and psychological harmful factors, which are also the causes of occupational risk.
- The above factors must be identified, recorded, evaluated in terms of their impact on employee health.
- The effect of these factors must be zeroed through the measures suggested by the Safety Technician and the Occupational Doctor.
- Τα ανωτέρω υλοποιούνται μέσω της μεθοδολογίας που ονομάζεται:

**"Assessment and Prevention of Occupational Risks in the Working Environment"**

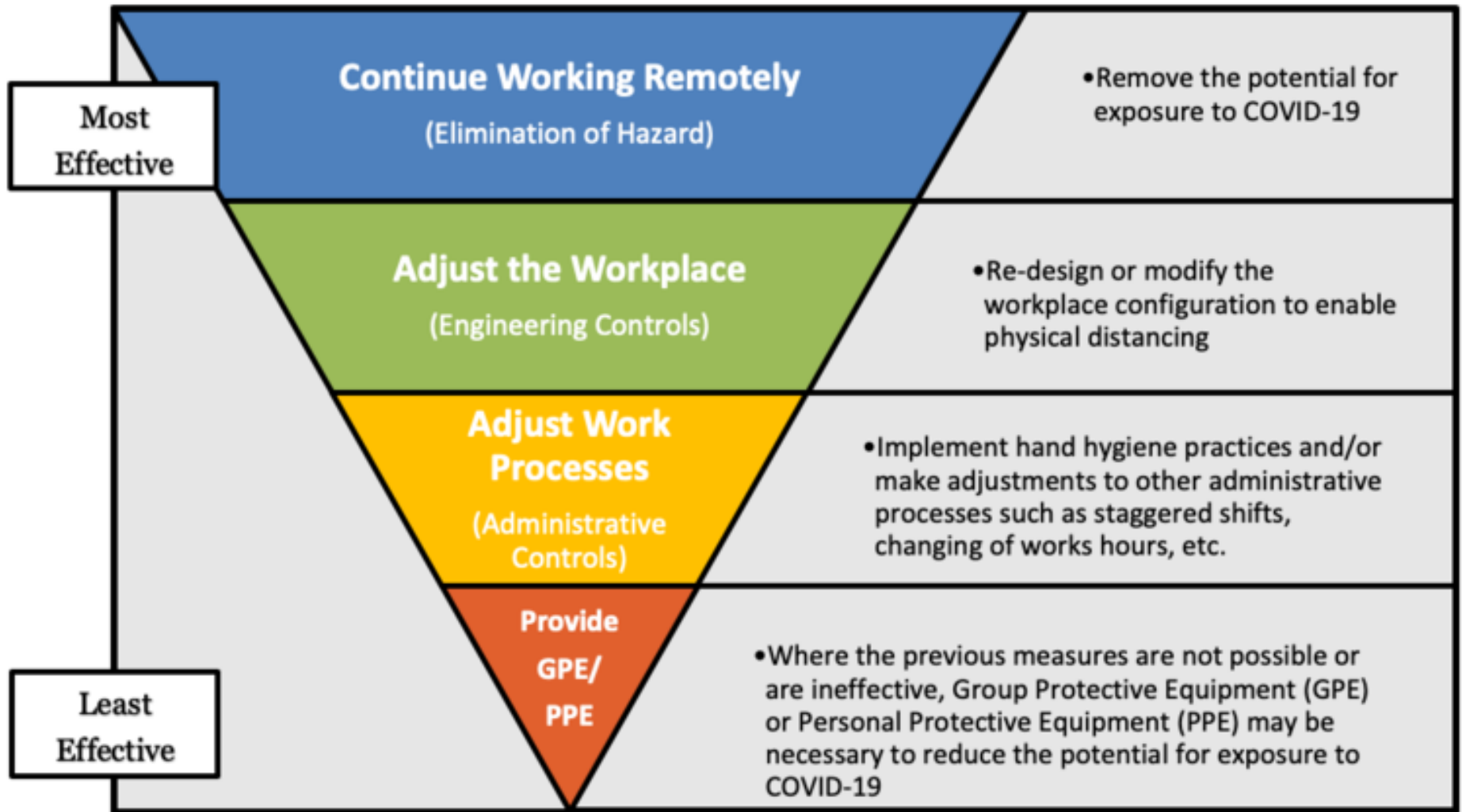
# 11. Basic Principles of Occupational Risk Assessment

## Occupational Risk Assessment Methodology (Flow Chart)

- There is no set way for the risk assessment to be carried out, however care must be taken to ensure that all relevant sources of risk are examined with a view to **eliminating** or, if not practically possible, **reducing** the level of risk and minimizing the number of exposed workers.
  
- A suggested Occupational Risk Assessment procedure could include the following steps:
  - Discrete examination of each part of the working environment.
  - Identification of possible hazards of each department.
  - Recording of existing risk removal / mitigation measures.
  - Record the number of staff and their length of stay per department.
  - Recording of the work carried out in each specific department.
  - Examination of the way the staff involved work.
  - Risk assessment from the various tasks of the staff in each department.
  - Regular updating of the Occupational Risk Assessment

# 11. Basic Principles of Occupational Risk Assessment

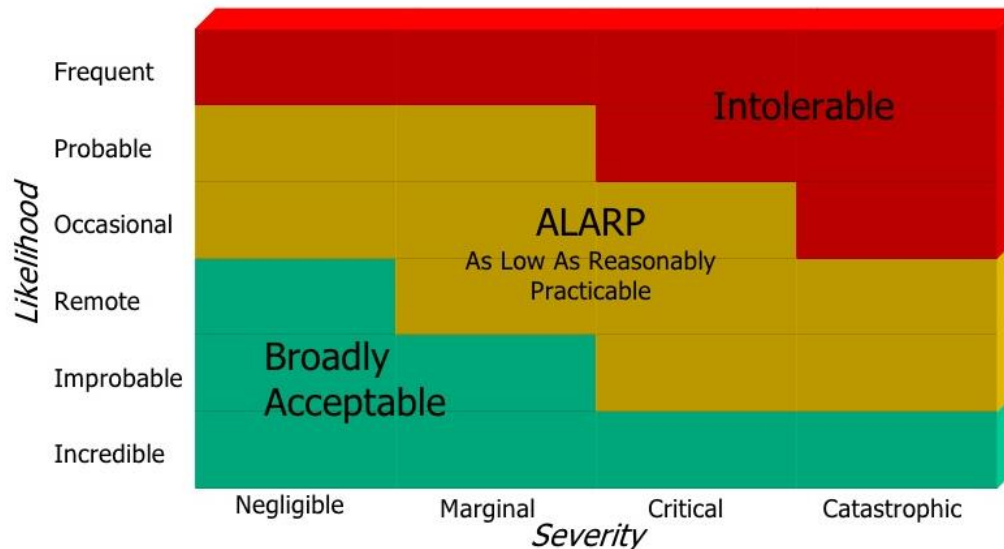
## Risk Assessment and Control for Covid-19 Prevention



# 11. Basic Principles of Occupational Risk Assessment

## Risk assessment (Diagram)

The Risk Assessment (Scale 1-5), as well as the respective proposed measures, they must take into account the possibility of an accident and its possible consequences.



Both the frequency of the accident and the consequence of the possible accident are distinguished on a scale from 1 -5. This type of grading means:

- 1 - 2: Area of acceptable risk. It does not mean that no measures are taken at all. The necessary measures are taken such as keeping distances, use of Personal Protection Measures, fire extinguishers, etc. (Blue)
- 3 - 4: Risk area that requires risk mitigation measures, as there is a significant risk and increased chances of accident. (Yellow)
- 5: Unacceptable risk area. In these cases, significant protection measures are imposed, even restrictive measures (prohibitions) to remove the degree of danger. (Red)

# 12. Organizing Working Time

## Legal & Conventional Hours

- **Working hours** are the total hours during which the employee provides his work to the employer, daily, weekly, regular, part-time, by law or contract.

The legislation provides as a legal schedule the **weekly work of 40 hours**, for the employees who are employed by any employer with a dependent employment relationship under private law.

Deviations from the **maximum legal hours** are allowed, both downwards (**reduced employment**) and upwards (exceeding the maximum legal hours) which is considered as **overtime** or **overworking (additional time)** and corresponds to a **higher hourly wage**. It must be provided in the Contract and is called **Contractual Hours**.

The determination of the employee's schedule (shifts, start and end during the day), and in general the organization of working time, is a **right of the employer** and is defined by the signing of the individual employment contract.

The employer's right to **change working hours** must not be abused otherwise it can be considered a detrimental change in working conditions.

The working hours of the employees and any modification must be declared to the competent Labor Inspection Body.



# 12. Organizing Working Time

## Overworking and Overtime

- **Overworking** occurs when we have exceeded 40 hours of weekly employment. For companies that operate 5-day and 8-hour, overtime is considered the additional employment of 5 hours per week (from 41st to 45th), while for companies that implement a system of 6-day employment (from 41st to 48th). These hours are paid with the paid hourly wage increased by 20%.
- **Overtime** exists when we have exceeded the maximum daily working hours, ie beyond 8 hours per day for 6 days, and beyond 9 hours per day for 5 days, employment. Overtime is paid with the paid hourly wage increased by 40%

Violations of the provisions on working hours and time limits of employment of employees, in their majority, are characterized as of high or very high importance and incur high fines.

# 12. Organizing Working Time

## Working Time Management - Advantages and Disadvantages

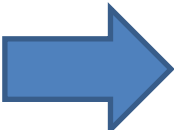
### **Advantages**

1. The company operates more efficiently as it adapts to the requirements of the market in which it operates.
2. In times of high demand, the company does not have to pay overtime and thus maintains its operating costs while increasing its sales revenue..

### **Disadvantages**

1. Increasing the daily working time by 2 hours overturns the rationale of eight-hour work.
2. Reducing or eliminating overtime will severely reduce employee income.
3. The flexibility introduced through the arrangement will favor the creation of part-time jobs at the expense of full-time jobs.

### **Conclusion**



The implementation of Working Time Management can improve the operational and financial performance of the Company, but also hides many risks for staff. If implemented, it should be done after mature thinking and taking into account the interests of all involved: employer and employee.