# AVVERA

BUSINESS COMPLIANCE

# NEW CHALLENGES
## FOR THE COMPANY BOARD

The introduction of stricter provisions on Administrative Liability of Corporations, Anti-Money Laundering, Data Protection and Health and Safety on the working place determined an extension of the obligations burdening on companies and a widening of the management's liability perimeter.

Criminal and administrative penalties, in some cases very punitive, require the adoption of new organizational models and of strategies of risks reduction able to protect the management, as well as the economical assets and the reputation of the company.

The extent of the processes, departments, and systems involved requires an innovative and more integrated approach as to the traditional legal consultancy.
Avvera's team is made of integrated professionals - lawyers, psychologists, process experts, IT and HR specialists - able to analyse the specific aspects of your company, to design a customized solution and provide your company with risk management systems allowing you to keep on operating with serenity and agility, in compliance with the laws.

## OUR COMMITTMENT:

# PROTECTING YOUR COMPANY'S MANAGEMENT AND VALUE

Avvera's mission is providing companies with the consultancy and operational support they need to manage the corporation operational and legal risks.
Its commitment is helping companies to develop an effective risk reduction system with an innovative approach, able to include all compliance actions within a wider and integrated strategy of Governance, Risk Management, and Compliance.

Our contribution isn't confined to providing the management with models, tools and formal procedures able to protect the company and the figures having responsibility roles, but extends to all levels of your company in order to ensure, with a direct and practical support, the effectiveness of the adopted measures, the meeting of deadlines and the correctness of fulfilments.

# OUR SERVICES

## COMPLIANCE WITH THE PROVISIONS

**Specialized consultancy**
Avvera operates on the whole national territory with an expert team that takes care specifically of Compliance and Management Systems.
The team is made up of figures with advanced multidisciplinary skills: lawyers, managerial engineers, organizational consultants, HR consultants, psychologists expert in the working environment, IT engineers, security experts, safety auditors, specialists in health and safety on the working place.
The services are structured as integrated modules of an iterative process in continuous improvement - Avvera's Enterprise Compliance Lifecycle Management - divided into six stages:

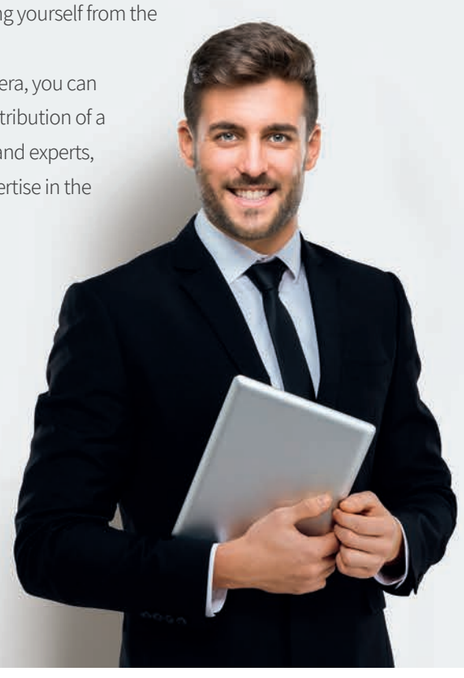
- **Risk Assessment**
- **Implementation**
- **Training**
- **Previous control**
- **Effectiveness analysis**
- **Audit & Due diligence**

**Operational Support**
Avvera helps you also to carry out the operational tasks, supporting your inner structures or directly taking care of the regulatory fulfilments.

## DPO OUTSOURCING

**The new figure of DPO**
Among the novelties introduced by the new EU Regulation no. 2016/679, there's the appointment of the DPO (Data Protection Officer), key figure to ensure the correct operation of the Personal Data Management System.
For some companies, the appointment of the Data Protection Officer is compulsory, while for others it can represent a suitable voluntary choice.

**Why should you choose a DPO by Avvera?**
The DPO can also be an external subject, having the needed requirements. Avvera offers you the possibility of outsourcing the figure and the tasks of the DPO, freeing yourself from the duties provided.
By relying on Avvera, you can count on the contribution of a team of lawyers and experts, with specific expertise in the field.



## DIGITAL TRANSFORMATION

**Compliance of digital projects**
The digitalization of business processes and the provision of services with a high technological content require an implementation in compliance with the provisions in force – both Italian and European -, the technical regulations issued and the provisions by the relevant authorities, in particular by AGID – Agency for Digital Italy – and by the Data Protection Authority.
Avvera's contribution allows to innovate the approach to business or the methods to carry out the services without forgetting the compliance needs.

Intervention fields:

- **Digital preservation systems**
- **Electronic signature advanced systems**
- **Documents workflow systems**
- **Digital services: compulsory documents and manuals**

## COMPLIANCE COCKPIT

**Informative Dashboard**
Intactor is a software studied by Avvera to help the companies to manage and keep under control all activities aimed at mitigating the operational and legal risk of corporations. Intactor offers to companies, institutions, and organizations a set of advanced tools to manage and monitor the fulfilments and conformity actions on:

- **Eu Regulation 2016/679 and Legislative Decree 196/2003**
- **Administrative/Criminal Liability of Corporations (Legislative Decree 231/2001)**
- **ISO 27001**
- **Impact on the assets**

The solution provides the management with analytic and synthesis graphic dashboards allowing to assess the risk degree and to monitor the status of the fulfilments.
The integrated automatisms generate the activities provided and manage the relevant deadlines sending reminders and notifications to the relevant functions.
The system, compatible with all IT environments, is completely customizable depending on the company's specificities.

# OUR TESTIMONIALS:
# MORE THAN
# 400 ACTIVE CUSTOMERS

## BANKS, INSTITUTIONS, INDUSTRIAL GROUPS, DISTRIBUTION AND SERVICES COMPANIES, BOTH NATIONAL AND INTERNATIONAL

We cooperate with institutions, great groups, medium-sized enterprises, and organizations of any size.
Among our customers, you can find important realities operating in the following fields:

- Automotive
- Insurance companies
- Banks & finance companies
- Building & Constructions
- Energy & Utilities
- Great distribution & Retail
- Food industries
- Chemical industries
- Pharmaceutical industries
- Information Technology
- Mechanical production
- Logistics & Transports
- Luxury & Fashion
- Raw materials
- Media & Publishing
- Hospitality & Catering
- Health services
- On-line services
- Telecommunications
- Textile & clothing
- University
- Travels & Tourism

## OUR MODEL

# ENTERPRISE COMPLIANCE LIFECYCLE MANAGEMENT

The compliance is a continuous process that develops with time. Avvera's Enterprise Compliance Lifecycle Management is a set of integrated services that allows to minimize the operational risks, keeping the company always in line with the legal requirements. The approach is modular: the company can entrust Avvera with the management of the whole cycle or of one or more operations.


**Risk Assessment**
Risk assessment with formal verification of the organizational and management model and of all existing relevant documents.

**Implementation**
Taking charge of all operational activities needed to comply with the regulations in force.

**Training**
Training on-site or through an e-learning platform to teach the collaborators suitable and aware behaviours.

**Previous control**
Strict collaboration with the company's inner functions while exercising the required effectiveness assessment, in the management of deadlines and updating of documents and procedures.

**Effectiveness assessment**
Substantial and effective verification of the Organization, Management, and Control Model adopted.

**Audit & Due diligence**
Formal verification of the Organization, Management, and Control Model adopted and of the documents submitted for its issuing and operation.

## OPERATING METHODS

**Risk detection and management**
Our Risk Management process allows us to detect, subject by subject, what company area, function or person is subject to the risk as to specific offences or violations:

- We examine the activities and processes that can expose you to the risk
- We evaluate the risk in terms of seriousness and probability
- We analyse with what provisions, procedures, IT or physical measures the risk is prevented
- We define the new risk management plan

**Compliance**
Once the Risk Management Plan has been designed, we decide together with you the actions to be taken: from the improvement of the company governance instruments (articles of association, delegations of the board of directors, etc.) up to the issuing of the working instructions for the executive tasks.

- We collaborate with your organizational functions in the implementation of the procedures and controls and we support them while carrying out the legal fulfilments.
- We train and sensitize your collaborators so that their behaviour is aware and compliant
- We check that their behaviour effectively converts into an operational practice.

**Monitoring e reporting**
We monitor the status and the evolution of the system through periodic controls, solving the problems that could emerge with time.
We provide the management with periodic feedback allowing a wise and aware management.

## WHY SHOULD YOU CHOOSE US?

**We study tailored solutions**
Each company is a system with several inner and outer variables. We can analyse and understand the difference of each customer and adapt a general and abstract system of rules to the specific reality with the minimum impact on the existing one.

**We provide a complete support**
We don't limit ourselves to showing you the solution, but we collaborate with you even from the operational point of view, integrating your inner controls and taking charge of the bureaucratic and administrative tasks.

**We know all dimensions of the matter and its impacts on the organization**
Our team is constituted by professionals with multidisciplinary expertise and years of experience on the field.

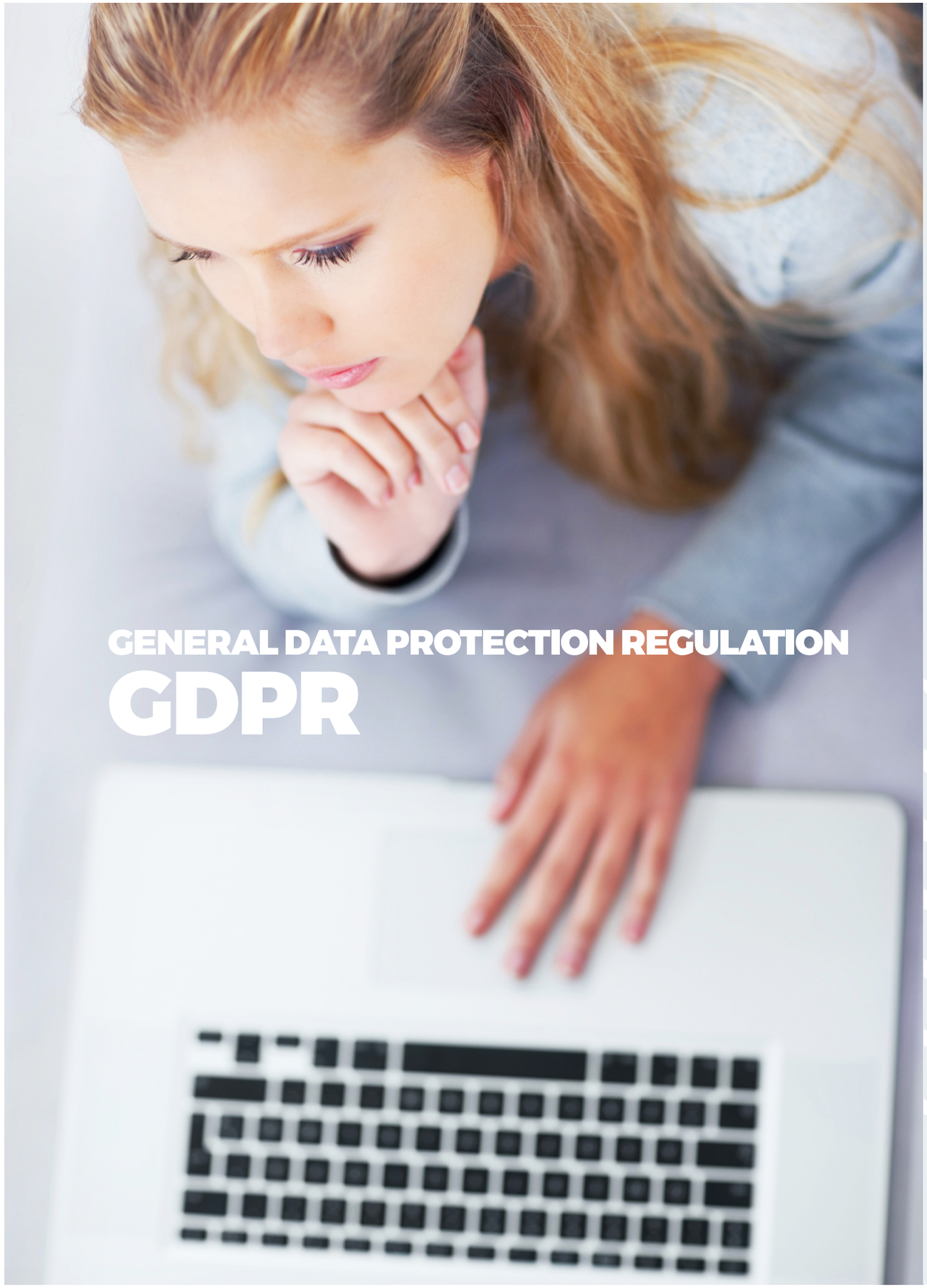
**We favour pragmatism**
We adopt a pragmatic approach, aiming at the results. Our customers appreciate us for our expertise, availability and for the certainty that we'll keep our word.

# REGULATORY COMPLIANCE

Nowadays, companies - as well as private and public bodies - have a primary role in economy and society and the legislator regulates the organizational aspects and activities in a more and more incisive way.

The regulations on personal data protection, health and safety on the working place, anti-money laundering and corporation liability show that the provisions have become stricter and refer to a wider and wider spectrum of functions and responsibilities.

The actions of companies are always controlled by the shareholders, the community, and the control bodies. Therefore, it's not surprising that the compliance with the regulations drew the management's attention, occupying a determining role in the containment of the operational and legal risk and taking a strategic importance for the protection of the company value.




REGULATORY COMPLIANCE

# GDPR

The new European regulation is aimed at harmonizing the different national provisions to favour the circulation of the European citizens' data in a safe and protected way. With the issuing of the GDPR, companies have to face a regulatory impact that requires a different approach as to the past. The new regulation emphasizes the essential objectives and the accountability principle, attributing to the company wider margins of autonomy but giving it heavier responsibilities.

In spring 2016, the new EU Regulation 2016/679 (General Data Protection Regulation) has been published on the Official Gazette of the European Union, abrogating and replacing the Directive 95/46/EC on the protection of personal data and their free circulation.

The purpose of the European legislator is unifying and strengthening within the Member Countries the processes, procedures and standards for the collection, management, and protection of personal data inside and outside the borders of the EU.

The Regulation entered into force 20 days after its publication on the Official Gazette and became definitively applicable in a direct way in all EU Countries since the 25th of May 2018, without the need of acknowledgement acts by each country.

The national legislator, however, intervened with a Legislative Decree (101/2018) with the purpose of harmonizing the previous Data Protection Code with the new EU Regulation.

The Regulation creates rights and duties for people and can therefore be enforced before national judges.

**Objectives of the compliance action:**

- **Evaluating the size of the risks and the effects consequent on the data breach**
- **Activating continuous processes, measures and controls aimed at mitigating the risk and at complying with the regulatory obligations**
- **Detecting the inner/outer figures to which to entrust responsibilities and supervisory tasks**
- **Ensuring the Data Subject rights, inclusive of the right to be forgotten and the data portability**
- **Reducing the risk of pecuniary sanctions or legal actions**
- **Manage in a rational, sustainable, and effective way the regulatory obligations**

## Main compliance fields

**Revision of the Organizational Model**
Reformulation of delegations, tasks, and inner functions: the figure of the inner Data Processor isn't present anymore, but the organizational need to assign tasks and functions to different hierarchical levels already present inside the company is still in force.

**Introduction of the Data Protection Officer (DPO)**
Its task is supervising the correct application of the regulation, carrying out inspections and consultations and being the contact point with the management and the Data Protection Authority.

**Information notice and consents**
The Data Subject has the right to receive the information in a transparent way and the request of consent in a distinguishable and unconditioned way. The Data Controller is obliged to demonstrate that it obtained the consent.

**Accountability**
The cases when it's necessary to ask an authorization or contact the Data Protection Authority considerably reduced. The Data Controller has more powers to decide autonomously, with the awareness that such powers are balanced by very important administrative sanctions.

**Data Protection**
Obligation to implement personal data protection measures (e. g. pseudonymisation and encryption) to ensure a security level suited to the risks among which destruction, loss, undue modification, unauthorized access.

**Privacy by design / by default**
Obligation to implement suitable measures during the planning stage (by design) or by default based on the criticality of the data processed.

**Data Breach Notification**
Obligation to communicate possible data breaches without undue delay and within 72 hours to the relevant authority (and, in the presence of specific conditions, obligation to notify the breach also to the Data Subjects).

**Records of processing activities**
Obligation of keeping a record of the processing activities on the personal data containing, among other information, the purposes, categories of Data Subjects and processing operations, as well as the description of the security measures adopted.

**Data Protection Impact Assessment (DPIA)**
Obligation to carry out a previous assessment of the impact deriving from the processing operations on the personal data protection, including an assessment of the risks and security measures.

**Data Transfer**
Obligation to verify the existence of the conditions provided by the regulation before transferring the personal data to a third country or an international

# GDPR

## The new role of the DPO

The regulation provides the introduction of a new high-profile figure characterized by a wide autonomy and independence, with the task of supervising the correct application of the regulation.
The role can be covered by an inner or external resource, on condition that it has the needed expertise and has no responsibility roles that could represent a conflict of interests.

Avvera offers companies the possibility to entrust to an external qualified figure, counting on the know-how of a team made up of specialized experts.

## The compliance process proposed by Avvera

**Awareness**
- Identification of the main gaps.
- Execution of the compliance program to the GDPR based on the results of the Risk Assessment.

organization.

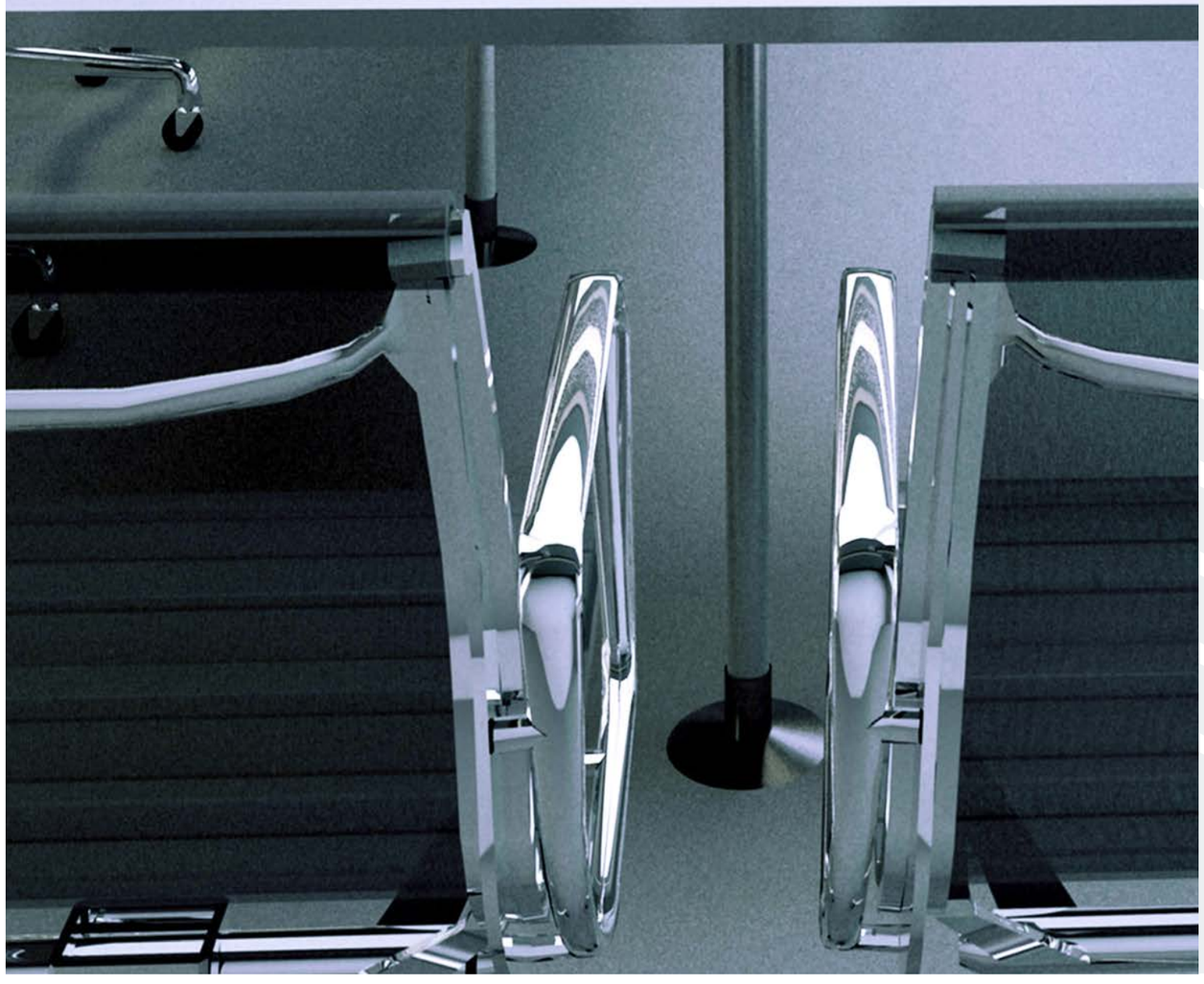
**Start up**
- Definition of the activities' perimeter of the compliance program to the GDPR.
- Approval of the estimates and budget.

**Resolution**
- Definition of a compliance integrated program with identification/prioritization of interventions.

**Compliance**
- Institution of the DPO and of the reference processes, with adjustment of the organizational assets and relevant information flows and procedures.
- Implementation of the Privacy by design/default, definition of an escalation process in case of data breach, through the adoption of operational procedures.
- Training of the people who process personal data.

**Optimization**
- Optimization of processes based on the data breaches.
- Strengthening of the security measures on personal data.

# CORPORATE GOVERNANCE AND LIABILITY 231/2001



REGULATORY COMPLIANCE

## 231/2001

With the introduction of Legislative Decree 231/2001, companies, institutions, and associations are liable from an administrative point of view for the offences committed in their interest and to their advantage by subjects in top positions or people operating under their direction. The impact of the pecuniary sanctions, of disqualifications and the consequent reputational damage can compromise the stakeholders' trust and negatively affect the value of the company.

The Legislative Decree no. 231 of 8th June 2001 introduced in Italy the corporate liability for the offences committed by the staff, both in top positions and subordinate, in the interest or to the advantage of the company. The risk of incurring sanctions is high and can entail both pecuniary sanctions and disqualifications.

Companies are asked to adopt effective and efficacious organizational and management models, able to prevent the offences to be committed. Each company shall carry out a suitable risk assessment on the commission of each offence and adopt specific regulations, procedures, codes of conduct and training courses for the staff and for those who act in its interest. The decree provides also the compulsory institution of an inner supervisory body equipped with autonomous powers of initiative and control.

**Purposes of the compliance action:**

- **Preventing the development of wrong practices and illegal behaviours inside the company organization**
- **Ensuring the protection of the employees that report illegal acts (whistleblowing)**
- **Reducing the risk of pecuniary sanctions or disqualifications**
- **Preventing damages to the company's properties and reputation**
- **Protecting the reputational assets and the stakeholders' trust**
- **Preserving the value for shareholders**
- **Managing in a rational, sustainable, and effective way the regulatory obligations**

# PREVENTION AND FIGHT AGAINST MONEY LAUNDERING 231/2007

## REGULATORY COMPLIANCE

## 231/2007

The Legislative Decree no. 231 of 21st November 2007 acknowledges the European regulation to prevent money laundering and financing of terrorism. The decree, deeply modified by Legislative Decree 90/2017, regulates the prevention and fight of money laundering, that the subjects are obliged to carry out through the introduction of facilities aimed at ensuring the knowledge of the risk, the full knowledge of the customer and the detection of the suspicious operations.

The legislative Decree 90/2017, published in July 2017, deeply modified the Legislative Decree 231/2007. In particular, the regulation is based on a system of obligations inspired to the following essential assumptions:

- suitable assessment of customers with whom relationships are established or operations are carried out (customer due diligence),
- identification of the real owner,
- preservation and protection of documents, data, and information useful to prevent, detect or ascertain possible activities of money laundering or financing of the terrorism,
- notification of suspicious operations.

Among the recipients of all or some obligations, more than banks and money brokers, insurance companies or brokers operating in the branches specified by article 2, paragraph 1 of the Private Insurances Code, there are professional accountants, auditors, lawyers, notaries, money changers, salerooms, gold operators, cash-carrying and storing service, online game operators and so on.

**Purposes of the compliance action:**

- **Preventing the company or the professionals to be involved in the commission in the offences of money laundering and financing of terrorism**
- **Reducing the risk of criminal and administrative penalties**
- **Protecting the company's assets and reputation**
- **Preserving the stakeholders' trust**
- **Managing in a rational, sustainable, and effective way the regulatory obligations**

# HEALTH AND SAFETY ON THE WORKING PLACE
# 81/2008

REGULATORY COMPLIANCE

## 81/2008

The decree provides the actions and controls that companies should take to protect the workers from possible physical and psychological injuries consequent to inappropriate operational methods and working environments. The employer shall carry out a careful assessment of the critical factors present in the company, in order to take all compulsory initiatives aimed at the elimination and containment of the risk, such as the adjustment of structures, systems and equipment, the health control, the workers' training, as well as the revision of processes and procedures. The deficiency and lack of such provisions expose the company to very risky civil and criminal liabilities.

The Legislative Decree no. 81 of 9th April 2008 is aimed at ensuring the uniformity of the workers' protection on the national territory through the compliance with essential security levels and applies to "all sectors of activity – both private and public – and to all types of risk". The Decree encourages each company to a continuous improvement through the adoption of the Security Management System.

The regulation affects the organization, the production processes and systems of the company and confirms a very risky civil and criminal liability system. The action of compliance with the regulation and the following management of the fulfilments have to start from a correct detection of the employer and adopt – where possible – an effective delegation of responsibilities, thanks to all instruments provided by the decree.

**Purposes of the compliance action:**

- **Preventing occupational diseases and accidents on the working place**
- **Improving the workers' security and wellbeing**
- **Reducing the legal and operational risk**
- **Reducing the risk of administrative sanctions**
- **Managing in a rational, sustainable, and effective way the regulatory obligations**

# MANAGEMENT SYSTEMS

Management systems are useful instruments to improve the inner processes, to regulate the organizational behaviours and to ensure to customers, partners, and institutions a quality service based on certified methods. They are based on active control procedures able to regulate the processes and trigger corrective actions and preventive measures. The requirements that a company should meet to implement a Quality Management System and preserve it with time involve the company at several levels with a direct impact on several departments and on a wide company population.

# QUALITY MANAGEMENT SYSTEM
# ISO/9001

MANAGEMENT SYSTEMS

## ISO 9001

ISO 9001 is the quality management system that helps companies to identify the possible improvements that could be made to each and any process and to the operation of the “company machine”. The system facilitates the continuous monitoring of quality and the quick activation of corrective actions to achieve the quality objectives defined during the strategic planning. The company can therefore meet new efficiency targets and obtain significant saving, offering the customers a more careful and in continuous improvement service.

The quality management system is the organizational and guarantee instrument of the “Quality Management” company process, planned in a specialized way with the purpose of stimulating the behaviour of everybody to take an “active role” as to the objectives defined by the General Direction.

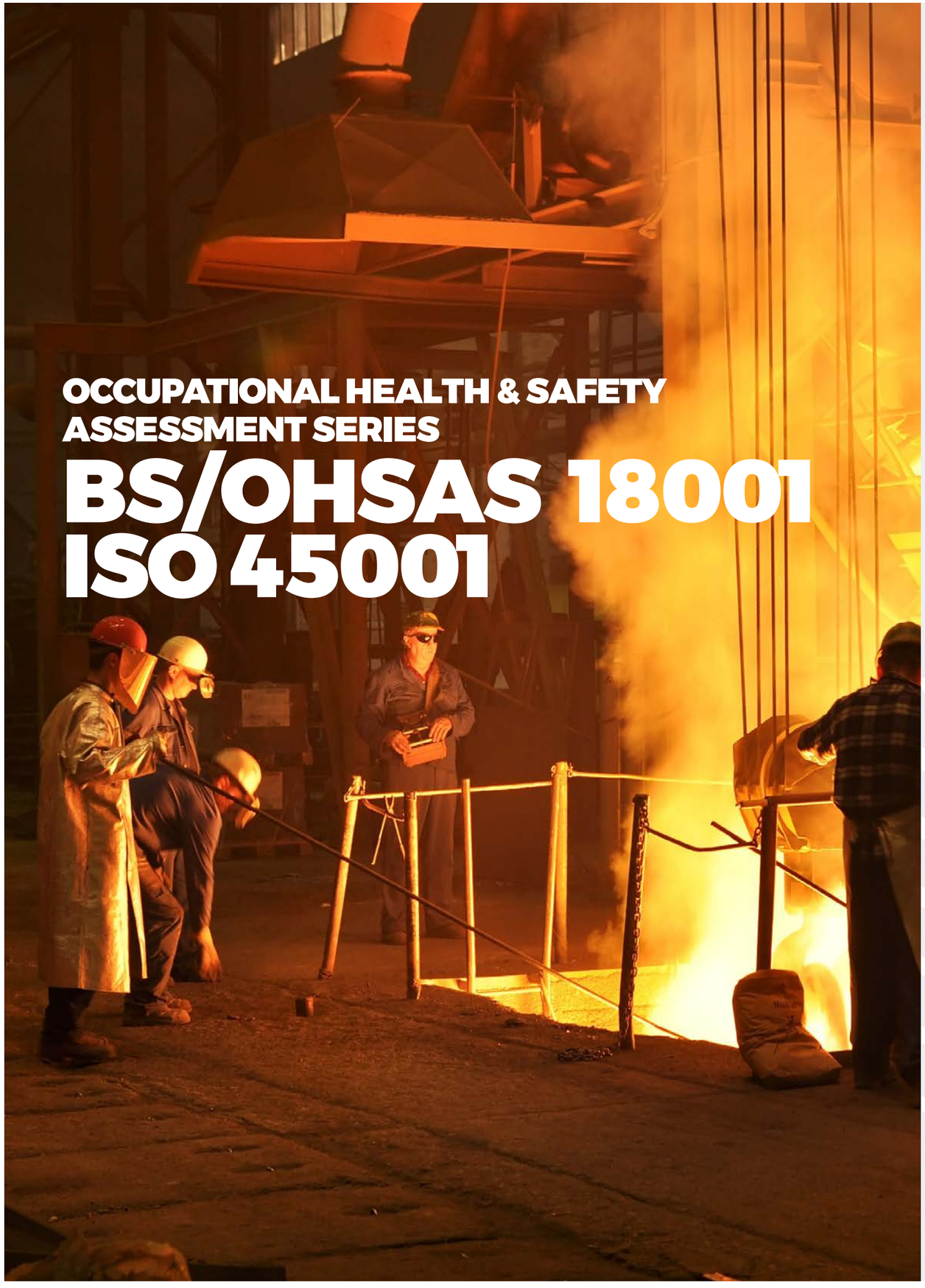
The UNI EN ISO 9001 standard is based on the principle of determination of the company “context” through the definition of the interested parties and the consequent assessment of “risks and improvement opportunities” keeping the continuous monitoring on the processes management.

**Purposes:**

- **Organizational improvement**
- **Processes standardization**
- **Access to new customers and opportunities**

**Advantages:**

- **More effectiveness and productivity**
- **Encoded rational processes**
- **Better control**
- **Better customer service**
- **Increase of credibility and trust**



## OCCUPATIONAL HEALTH & SAFETY ASSESSMENT SERIES

# BS/OHSAS 18001 ISO 45001

MANAGEMENT SYSTEMS

## ISO 45001

ISO 45001 defines the minimum standards for the protection of the workers' health and wellbeing. The structure of the standard reintroduces the contents of the standards BS/OHSAS 18001 and 81/2008, widening them. ISO 45001 is a certifiable standard recognized at international level and is destined to replace the standard BS/OHSAS 18001 that will decay on 12th March 2021. ISO 45001 provides a reference framework to reduce the risks and improve the security through an iterative process of continuous improvement actively involving the whole organization, from the top management to the single worker.

BS/OHSAS 18001
Standard issued by the British Standard Institute specifying the requirements for a management system of the Health and Safety on the working place.

ISO 45001
It's a recent standard and it's the first international standard applicable to any organization that wants to realize a healthy and safety management system to eliminate or reduce the risks for workers and for all the figures that could be exposed to dangers on the working place associated with the activity carried out.

**Purposes:**

- **Prevention of accidents on the working place**
- **Improvement of the working conditions**
- **Compliance with the regulatory requirements**

**Advantages:**

- **Reduction of legal and operational risk**
- **Increased wellbeing of workers**
- **Less absences**
- **Reduction of the insurance costs**
- **Increase of credibility and trust**

ENVIRONMENT MANAGEMENT SYSTEM

# ISO 14001 - EMAS

MANAGEMENT SYSTEMS

## ISO 14001

The environmental management system ISO 14001 guides companies in the definition of processes, procedures, and controls able to reduce the negative impacts of the companies' activities on the environment, minimizing the pollution risks.
The standard, more than providing a more aware approach to the correct consumption of resources and to the environment protection, allows the company to have an ethic and responsible conduct, with positive effects to the relationships with the community and institutions.

ISO 14001
The standard UNI EN ISO 14001 is a voluntary international instrument, applicable to all types of companies, specifying the requirements of an environmental management system. The certification is issued by an accredited independent body that verifies the real commitment in minimizing the environmental impact of processes, products, and services.

EMAS
EMAS (Environmental Management and Audit Scheme) is a community system for the environmental ecomanagement and audit that recognizes at European level the achievement of excellent results in the environmental improvement. EMAS provides that the Environmental Management System of a company is implemented in compliance with the requirements of the ISO 14001 standard, section 4.

**Purposes**

- **Reduction of the environmental impact**
- **Prevention of pollution**
- **Compliance with the regulatory requirements**

**Advantages**

- **Better use of the natural resources**
- **Reduction of the legal and operational risk**
- **Increase of credibility and trust**
- **Improvement of the relationships with community and institutions**

# NFORMATION SECURITY MANAGEMENT SYSTEM ISO 27001

MANAGEMENT SYSTEMS

## ISO 27001

ISO 27001 defines a systematic approach for the implementation of a security management system able to ensure the integrity, confidentiality, and availability of information.
The standard provides a reference framework for the implementation of suitable organizational countermeasures, aimed at preventing the loss, exposure, or theft of sensitive and business information due to cyber intrusions, errors, and inner unauthorized accesses.

ISO/IEC 27001 is an international standard that defines the requirements of an Information Security Management System, in particular with reference to the physical, logical, and organizational security aspects (Information Security Management System - ISMS).
The purpose of the standard is protecting data and information from any threats, in order to ensure their integrity, confidentiality, and availability. Besides, the standard ISO 27001 includes the requirements to adopt a suitable Information Security Management System (SGSI), aimed at a correct employment of the company's sensitive data.

Purposes

- **Protection of the IT assets**
- **Compliance with the contractual and regulatory requirements**

Advantages

- **Reduction of the legal and operational risk associated with the data breach**
- **Organizational improvement**
- **Increase of credibility and trust**

AVVERA

BUSINESS COMPLIANCE

**AVVERA Srl**

MILANO
ROMA
UDINE
PESARO

Largo Umberto Boccioni 1
21040 Origgio VA
tel. 02 96515401
fax 02 96515499

www.avvera.it
info@avvera.it

**ISO 9001**
Cert.N. 9175.PITC

**ISO/IEC 27001**
Cert.N° 9194.PIT2

**ISO 45001**
Cert.N. 9192.AVRA

AVVRCP04022021EN

AVVERA