monokee

Login once, run everywhere.

IAM and GDPR:

connections, implications

o p p o r t u n i t i e s

TABLE OF CONTENTS

INTRODUCTION

From 25 May 2018, **General Data Protection Regulation** (GDPR) has radically changed the way organisations are required to collect, store and process personal data.

The focal point is that any information through which we can identify a person must be protected during all stages of the process, in order to prevent possible data loss, *data breaches* and unlawful data processing.
GDPR implies a change of perspective in the relationship between people and organisations: users achieve now full control over the entire life-cycle of their personal data.

Nowadays, data protection goes beyond a physical defence of the enterprise perimeter, gradually moving toward a new strategy based on **digital identity protection** and **access management**.
Therefore, the question organisations need to answer is no longer "where" the information is physically located, but "**who**" has access to this information.

It is worth noting that GDPR does not provide guidance on "how" organisation should act to meet the requirements of articles from 5 to 32 related to access management and security of data processing, bringing out what some experts define as a "**technological gap**".

An answer to this gap is provided by **Identity and Access Management** platforms, which represent an excellent solution to ensure that information (among which stand out digital identities) is only accessible to authorised staff. In this way organisations can effectively comply with GDPR security requirements.

CHAPTER 1

IDENTITY and ACCESS MANAGEMENT AS A STRATEGIC RESPONSE TO GDPR

Considering the principal GDPR application areas, the implementation of an Identity and Access Management platform is strategic in a wide variety of frameworks:

PERSONAL DATA MANAGEMENT

Key principle of GDPR is personal data protection against unlawful or unauthorised processing.

A centralised Identity and Access Management platform, built on specific access policies and strengthened by **multi-factor authentication** mechanisms, ensures that **only authorised staff or roles have the possibility to access to certain information**. An IAM platform also ensures **traceability** of log-in data (who, when, to what information…), enabling a prompt management of access rights through **Identity Federation** mechanisms.

SECURITY OF PROCESSING

According to article 32 of GDPR, Data controller and Data processor "*shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk*".

In particular, must be fulfilled "*the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services*" and "*the ability to restore the availability and access to personal data in a timely manner in the event of physical or technical incident*".
Is also central the requirement to define *"a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing*".
It is worth recalling that these security requirements shall be applied to all personal data processing within the organisation, not only to those occurred after 25 May 2018.

In accordance with GDPR requirements, an effective IAM platform **reduces the risk of data loss, data breaches and unauthorised access**. At the same time, in case of data breach, it ensures **a timely detection of personal data violations.**

According to articles 6, 25 and 32 of GDPR, is important to include mechanisms of **pseudonymisation** of audit events and forms of **encryption** of personal data, in order to implement technical and organisational measures ensuring a risk-adjusted level of security.

INFORMED CONSENT

According to article of 4 of GDPR, **consent** of data subject is "*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by statement of by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*".

When an organisation needs the consent of data subjects should be aware that this indication must be:

- **FREELY GIVEN**: consent means giving people genuine choice and control over how organisation uses their data. People must be able to refuse consent and to withdraw it easily at any time;
- **SPECIFIC**: the consent must be referred to a specific data processing or to a limited category of data;
- **INFORMED**: users must be provided with all necessary information to form their own opinion regarding the possibility to give or refuse consent. This information must be available before any data processing;
- **UNAMBIGUOUS**: consent requires either a statement or a clear affirmative act.

The ideal solution would be collecting the so-called **GRANULAR CONSENT**, asking to users a specific consent for each type of data the organisation intends to process. In this way, data subjects can precisely verify the extent of data processing for each area.
This kind of approach simultaneously complies with two important legal requirements: from one hand, it informs data subjects about essential elements of the service offered, from the other, it asks for a specific consent for each of these.

Naturally, even if the consent meets all the above-mentioned requirements, this authorisation does not permit illicit or unlawful data processing. If the extent of the processing is excessive or disproportionate, even if the data subject has given his or her consent, Data controller and Data processor are violating GDPR requirements.

In any case, according to article of 7 of GDPR, if data processing requires informed consent, Data controller must be able to **demonstrate** that data subject has expressed his or her consent to data processing.
Moreover, organisation must be prepared to manage any **request for revocation or amendment** from users, who can also ask for the backup of their data.

Personal data is therefore an information the organisation must be able to recover at any time.

Consent management is simplified with an effective IAM platform, because the majority of collected consents is **centrally registered and administrated** through user profiles.
Organisation can also access to a **list of collected consents**, in addition to the possibility to download **audit reports** to monitor given or denied consents.

DATA MINIMIZATION

"**Data minimization**" is a fundamental principle of GDPR, referred to the practice of liming the collection of personal data to that which is directly relevant and necessary to perform essential processes.

Through an IAM platform, organisations dispose of a **centralised control over accesses and authorisations**, by establishing **periods of time and quantity of information to which grant the access** and managing the elimination of information connected to accounts no longer used.
Moreover, a properly integrated IAM platform has the capacity to give information about the access to the applications, knowing who has the access to what data.
Organisation need to give great importance to the concept of "**Access Recertification**", according to which it is necessary to regularly recheck access rights in order to grant that users possess the correct level of authorisation, **monitoring status changes** and eliminating in a timely manner potential "**ghost accounts**".

SEGREGATION OF DUTIES AND LEAST PRIVILEGE

In conformity with the concept of Data minimization there are two more principles to which an IAM platform permits to comply. The first is the concept of **Segregation of Duties,** which requires more than one person to complete a task concerning data processing.
The second is the concept of **Least Privilege**, which implies a restriction of access rights to only those absolutely required to perform authorised activities, according to the roles.

Access policies should be kept to a minimum but, on the contrary, security should be ensured at the maximum levels, especially with regard to **authentication** systems.

Along this line, to centralise the access to a variety of applications, organisations can adopt a **Single Sign On** technology, through which they can unify and organise log-in procedures.

In order to strengthen security in a Single Sign On context, **Strong Authentication** techniques are increasingly used, by combining ease of access and data protection. One of these techniques is the **Multi-factor authentication**, which requires more than one method of authentication to verify user's identity.

All the above-mentioned concepts can be enclosed in two essential principles of GDPR:

PRIVACY BY DESIGN:

privacy principles must be taken into account throughout the whole engineering process, following a risk-based approach.

ACCOUNTABILITY:

controllers are responsible for and should be able to demonstrate their compliance with the GDPR data processing principles.

CHAPTER 2

IDENTITY and ACCESS MANAGEMENT AS "PROOF OF COMPLIANCE"

According to the concept of **accountability**, Data controller is responsible for determining the impact that data processing can have on data subjects' rights and freedoms. At the same time, Data controller shall demonstrate that risk evaluations, as well as technical and organisational measures, are the result of considered choices that can be documented.

The so-called "***proofs of compliance"*** represent a key principle of GDPR perspective. An Identity and Access Management platform, integrated with ***Analytics & Intelligence*** features, gives the Data controller reporting capabilities on identity and access governance within the organisation, during the whole users' life cycle.

The analysis tool highlights evolution trends for accesses and the rights connected to *entitlements*, ensuring a timely detection of suspicious events according to a *risk-driven approach.*
In this way, an IAM platform can provide more information about users and their access privileges, through advanced analytics.

An IAM platform, integrated with ***Analytics & Intelligence*** features, provides many benefits:

EASY AND TIMELY RISK DETECTION (Risk Analysis)

Through the traceability of events, it is possible to monitor activities considered to be at risk, whether done by administrators or users, such as violations of the principle of Segregation of Duties, password changes, direct assignations, failed authentications…

TRACKING EVENTS AND ANALYSING TRENDS (Audit Event Analysis)

Analytics & Intelligence features provide a detailed auditing of IAM platforms, analysing data from different data sources according to different insight levels and representing data though risk-oriented dashboards, which can be customised to the specific needs of the organisation.
Starting from the detection of Key Risk Indicators (KRIs), it is possible to track their trend allowing organisations to notice atypical behaviours.

TRACKING SUSPICIOUS PRACTICES

The audit analysis feature allows organisations to track audit events and find the root cause of practices that can be considered unusual or outside a normal use of IAM platforms.
In this way, after understanding the origin of the anomaly, it is possible to adopt preventive security measures in order to avoid irreversible damages (for example by modifying access policies).

IMPROVING AND ACCELERATING DECISION-MAKING PROCESSES

The possibility to have up-to-date reports, statistics and trends leads organisations to an optimization of decision-making processes.
Analytics & Intelligence tools provide a business-oriented perspective, which can lead decision makers to an improvement of administrative and governance processes.
Moreover, the possibility to filter audit events according to different criteria (for example date, category, type…) accelerates the decision-making process, making it more accurate.

OPTIMISING COSTS

The possibility to monitor access trends and log-in gives important information about the use of applications connected to an IAM platform. This feature enables to verify if the costs which have been incurred correspond to applications usage.

An IAM platform, integrated with ***Analytics & Intelligence*** features, allows organisations to mitigate one of the major security concerns of top management, which is poor threat visibility, since they do not dispose of a complete and up-to-date risk reporting.

Moreover, for large enterprises will become more and more complicated the management of thousands of users, each of which has its own role and access privileges to keep track of.

This fact significantly increases security risks, as well as organisational deficiencies, data loss and failure to comply with regulatory standards.

The integration of an IAM platform with *Analytics & Intelligence* features grants organisations a double advantage in terms of Security and Compliance.

The possibility to have audit reports and statistics is compliant with GDPR concept of **accountability**, allowing Data controller to demonstrate that the organisation has implemented from the beginning appropriate security measures against the risk of data breaches.

However, it is necessary to highlight the fact that the concept of accountability must go hand in hand with the principle of **Privacy by design**. The compliance with data protection regulation must be granted also during the implementation of *Analytics and Intelligence* features, which can not be design in contravention of GDPR requirements.

From this perspective, it is important to make preventive choices on many issues: collection of consents (following the provision of a privacy policy), mechanisms of data pseudonymization, the period for which personal data will be stored, within a Policy Document.

CHAPTER 3

ADDITIONAL LEGAL ELEMENTS WORTH CONSIDERING TO BE GDPR COMPLIANT

TERRITORIAL SCOPE (article 3 of GDPR)

According to article 3 of GDPR, "*this Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not*."

Moreover, the Regulation *"applies to the processing of personal data of data subjects who are in the Union, where the processing activities are related to:*

a) *the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or*
b) *the monitoring of their behaviour as far as their behaviour takes place within the Union."*

Lastly, "*the Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law*."

LAWFULNESS OF PROCESSING AND DEFINITION OF ROLES (articles 4 and 6 of GDPR)

A primary need is the identification of **roles,** by defining from the beginning who perform the role of Data controller and Data processor. The definition of roles, supported by the required documentation, allows a clear identification of levels of **responsibility in case of data breach.**

Data controller: is "*the natural or legal person, public authority, agency or other body which, alone or jointly with others, **determines the purposes and means** of the processing of personal data*."

Data processor: is "*a natural or legal person, public authority agency or other body which **processes personal data on behalf of the controller***."

DATA PROTECTION IMPACT ASSESSMENT (article 35 of GDPR)

According to article 35 of GDPR, "*where a type of processing in particular using **new technologies**, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a **high risk to the rights and freedoms** of natural persons, the controller shall, prior to the processing, carry out an **assessment of the impact** of the envisage processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks."*

Data Protection Impact Assessment (DPIA), besides being a GDPR requirement, represents an important element in terms of **accountability**, because it helps Data controller to demonstrate that appropriate measures have been implemented in order to comply with GDPR.

DPIA is part of the responsibility of Data controller, must be executed before data processing and constantly reviewed.

DATA PROTECTION OFFICER (articles 37, 38, 39 of GDPR)

GDPR has introduced the *Data Protection Officer (DPO)* position, which is designated by Data controller and Data processor in a number of cases:

a) the processing is carried out by a public authority or body;

b) the core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale;

c) the core activities consist of processing on a large scale of special categories of data (sensitive data, health-related data, data revealing racial or ethnic origin, sexual orientation, genetic or biometric data).

Data Protection Officer is an **expert advisor** who supports Data controller and Data processor monitoring compliance with GDPR.
DPO is responsible for overseeing organisation's data protection strategy, conducting audits to ensure compliance and addressing proactively potential issues.

More in detail, DPO's responsibilities include the following:

a) conducting regular assessments and audits to ensure GDPR compliance;

b) cooperating with Data controller and Data processor, if necessary, carrying out DPIA and maintaining records of processing activities;

c) ensuring that controllers and data subjects are informed about their data protection rights, obligations and responsibilities;

d) serving as the point of contact between organisation and GDPR Supervisory Authorities;

e) training staff involved in data protection.

Data Protection Officer is an integral part of the organisation but should be able to perform his or her duties **independently** and **autonomously.**
In fact**,** DPO must protect personal data regardless of organisation's interests.
In a condition of absence of conflict of interests, Data controller and Data processor shall ensure that DPO does not receive instructions regarding the exercise of his/her tasks.
For this reason, usually organisations hire externally the DPO, because it is difficult to ensure independence within an employer-employee relationship.

RECORDS OF PROCESSING ACTIVITIES (article 30 of GDPR)

An important requirement of GDPR, settled up by article 30, is the obligation to keep **Records of processing activities**.
Data controller shall produce this record in a **written form** and make it **available to the supervisory authority** on request.

Record of processing activities shall contain all of the following information:

- the **name** and **contact detail** of Data controller, Data processor and, where applicable, Data protection officer (DPO);
- the **purpose** of the processing;
- a description of the **categories of data subjects** and of the **categories of personal data**;
- where applicable, **transfers** of personal data to third country or an international organisation;
- where possible, the envisage **time limits for erasure** of the different categories of data;
- where possible, a general description of the **technical and organisational security measures** implemented.

Record of processing activities is not a general obligation: according to fifth paragraph of this article, the obligation "*shall not apply to an enterprise or an organisation employing fewer than 250 persons, unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 1*0."

Aside from being an obligation, Record of processing activities is an **internal control tool** and a way to demonstrate organisation's compliance with GDPR, documenting its data processing and enhancing internal awareness of risks associated.

RIGHT TO BE FORGOTTEN (article 17 of GDPR)

According to article 17 of GDPR, "*the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay.*"

Among the rights data subjects have gained with GDPR, significant is the **Right to erasure**, better known as **Right to be forgotten**, which introduces the possibility for individuals to have personal data erased.
If a valid erasure request is received and no exemption applies, organisation will have to ensure erasure from backup systems as well.

More in detail, according to article 17 of GDPR, data subjects have the right to obtain the erasure of personal data which are no longer necessary in relation to the purposes for which they were collected or processed, when he or she withdraws the consent on which the processing is based, or when personal data have been unlawfully processed.
In order to strengthen this concept in the online environment, Data controller are required to inform Data processors in order to cancel all links referring to personal data for which erasure has been requested.

Article 17 of GDPR specifies that Right to be forgotten includes **few limitations**. Freedom of expression and information, reasons of public interest, scientific, historical or statistical purposes shall allow the conservation of data regardless of any erasure request.

NOTIFICATION OF A PERSONAL DATA BREACH (articles 33 and 34 of GDPR)

According to article 33 of GDPR, in case of a personal data breach, Data controller shall **notify it to the supervisory authority** without undue delay and, where feasible, **not later than 72 hours** after having become aware of it.

With Resolution nr. 157 30 July 2019, the Supervisory Authority has introduced a **new Notification Form**, through which it requires Data controller to collect a range of information about violations, making more burdensome the notification process.
More in detail, in addition to the details of the subject who is notifying and of Data controller, it is necessary to specify the degree of severity of the violation and its possible consequences. Moreover, it is necessary to document the countermeasures organisation has applied to limit the impact of the violation and the strategy implemented to prevent the reoccurrence of the problem. In another section of the form, Data controller shall specify if the data breach has been communicated to data subjects.

In this regard, according to article 34 of GDPR: "*when the personal data breach is likely to result in a high risk to the rights and freedoms of natural person, the controller shall communicate the personal data breach to the data subject without undue delay".*

Three are the exceptions to this communication:

1. the controller has implemented appropriate technical and organisational protection measures to the personal data affected by data breach (**encrypting techniques** are fundamental);
2. the controller has taken subsequent measures which ensure that the risk to rights and freedoms is no longer likely to materialise;
3. the communication involves disproportionate effort (in such a case it will be replaced by a public communication).

The recent additional cost connected to data breach notification should be considered in a twofold approach: from one hand, it allows data controller to become aware of the extent of the violation occurred, from the other, it allows him to assess the necessity of communicate (or not) the violation to data subjects.

The notification process is supported by the obligation to keep a **Register of personal data breaches**.
This document is under the responsibility of Data controller and provides a double function: it allows Data controller to monitor all data breaches occurred within the organisation and enables Supervisory Authority to verify compliance with reporting requirement.

Fines up to

€ 20 millions

or up to

4 % of global turnover.

CHAPTER 4

GDPR REQUIREMENTS FOR NEW IT PROJECTS

After the entry into force of GDPR, in accordance with the principles of *privacy by design* and *privacy by default*, Data controllers and Data processors should take into account privacy concerns from the early stages of projects' implementation, in particular in case of automated processing of personal information.

Among general principles we find:

- EXPLICIT FUNCTIONAL REQUIREMENTS: they represent functional needs IT service must comply with, in order to generate value for users;
- IMPLICIT FUNCTIONAL REQUIREMENTS: they represent functional needs underlying the service offered, including user profiling rules, access rights and privileges;
- NON-FUNCTIONAL REQUIREMENTS: they include organisational and technical features the service must comply with;
- QUALITY AND SECURITY REQUIREMENTS: in accordance with ITIL model, they include what acts as "guarantee" for the service offered, representing its quality. Among the most important requirements emerge availability, capacity, reliability and security of the service.

It's worth noting that these requirements, related to *Business Analysis* standard, are totally in accordance with GDPR conditions, highlighting the complementarity between data protection and business organisation models.

Translating business requirements into GDPR requirements, emerge the following features which must be respected by Data controllers during data processing:

- AVAILABILITY: implies the ability to ensure that required data is always accessible where and when needed (even if disruption occurs);
- CONFIDENTIALITY: is a guarantee of reliable access to the information only by authorised people;
- INTEGRITY: is the assurance that the information is trustworthy, accurate and safeguarded from unauthorised amendments;
- ACCURACY: information should be correct, keep up to date and erase or rectified when inaccurate.
- COMPLIANCE: information should be presented in accordance with laws and regulations in force.

Moreover, organisations have to conduct two other reasonings regarding to data protection:

- RTO (Recovery Time Objective): is the maximum desired length of time allowed between an unexpected failure or disaster and the resumption of normal operations and service levels;
- RPO (Recovery Point Objective): expressed backward in time, is the point in time organisation can recover to in the event of a disaster. In other words, RPO can be expressed as the maximum amount of data organisation is willing to lose.

All the above-mentioned requirements, in the context of GDPR compliance, must be systematically addressed from the beginning of projects' implementation, in other words *by design.*

STEPS TO FOLLOW FOR THE IMPLEMENTATION OF A PROJECT GDPR COMPLIANT:

1. CONDUCT A RISK ANALYSIS:

- recognising potential risks (accidental or not) which can affect the expected result, building on the experience, good practices and other codified methodologies;
- quantifying the probability of occurrence of these events;
- quantifying the weight of the risk examined (by multiplying the impact by the probability of occurrence);
- producing a list of risks, from heaviest to lightest;
- deciding what actions can mitigate the probability and/or the impact of risks analysed, along with their cost;
- reconsidering risks on the basis of counter-measures planned.

2. SET THE EXTENT OF DATA PROCESSING: what kind of data are processed? What is the purpose of the processing? How long will data be stored? If the project is considering personal data, organisation has to be GDPR compliant.

3. PREPARE A PRIVACY POLICY DOCUMENT: after opportune analyses, this document should include a description of data collected, the purpose and the type of data undergoing processing, the storage time and the protection measures implemented.

4. COLLECT DATA AND CONSENTS: data collection must be made at the time of signing of the contract, along with informed consent with all GDPR requirements;

5. PROPERLY ARCHIVE CONTRACTS AND CONSENTS: it is necessary to apply appropriate measures in order to prevent unauthorised access to personal data. At the same time, only authorised staff has the possibility to insert new personal data.

6. APPLY ALL SECURITY MEASURES TO PERSONAL DATA: combine GDPR requirements with functional, non-functional and quality requirements of Business Analysis, toward a global and integrated security management. Organisation must also consider additional measures as Firewall systems, mechanisms of cryptography and pseudonymization, access policies, backup and restore settings, password management, quality control…

7. CONSTANTLY REVIEW AND IMPROVE: GDPR requires that these analyses are periodically repeated, in order to have an up-to-date risk evaluation and, consequently, preserve data protection over time.

CONCLUSION

In view of the analysis carried out above, it is quite clear that the process of compliance with GDPR requirements can represent a **strategy** to increase organisation's awareness and its **competitive advantage**, beyond a simple transposition of rules to avoid sanctions.

Moreover, GDPR requirements are extremely interdisciplinary, so they are in line with good practices and relevant international standards such as ITIL and COBIT frameworks, as well as standards related to information security management (ISO 27001), risk management (ISO 31000), business continuity (ISO 22301) and quality (ISO 9001).

GDPR compliance is therefore a first step, essential and crucial, capable of leading the organisation toward a better **understanding** of internal processes, risks, roles and data flows, ultimately increasing business security.

Being able to count on a solid Identity and Access Management platform, which in turn is GDPR compliant, represents a winning reply to Data Protection, guarantee of conformity and source of competitive advantage.

A risk-driven approach, supported by the integration of an IAM platform with Analytics & Intelligence features, allows decision makers to move from a consequential and repressive perspective to a **proactive and preventive** view of business security, fully in line with GDPR approach.

monokee

Login once, run everywhere.

CONTACT US


Via Zeni Fortunato, 8, Rovereto, TN


+39 049 2970297


monokee@monokee.it

monokee.com