Microsoft

Data Governance for GDPR Compliance: Principles, Processes, and Practices

Table of contents

A data governance plan, supported by effective technology, is a driving force to help document the basis for lawful processing.

Executive Summary

An effective data governance strategy forms the foundation of an organization's approach to protecting the privacy of personal data under the General Data Protection Regulation (GDPR), the new data privacy law by the European Union. Data is a valuable corporate resource, but under the GDPR personal data collected by an organization that pertains to customers, potential customers, employees, and others comes with significant responsibilities.

The GDPR strengthens existing rights and provides for rights for individuals who are in the EU to control the collection, storage, processing, and use of their personal data. Although the text of the regulation doesn't use the word governance, it lays out specific requirements for organizations that control and process such data, which fall under the umbrella of data governance.

A data governance plan, supported by effective technology, is a driving force to help document the basis for lawful processing, and define policies, roles, and responsibilities for the access, management, security, and use of personal data. Today's organizations are data-centric; they accumulate enormous amounts of information in many different formats. Software applications, systems, and databases like customer relationship management and enterprise resource planning systems contain personal information about customers, potential customers, employees, members, and other individuals.

This paper addresses data governance from concept to implementation.

01 What is data governance?

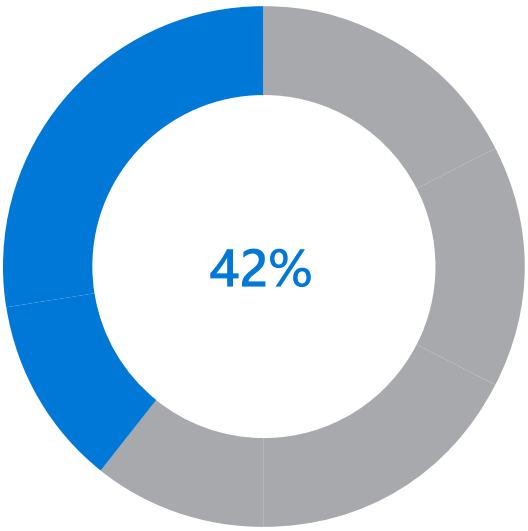
Data governance refers to an overarching strategy that encompasses the policies, processes (including technologies), and people involved in managing and protecting data. Data governance drives risk assessment, which drives the compliance effort, which in turn develops the governance program. The three--governance, risk assessment, and compliance--must work hand-in-hand for effective management and protection of data.

Data governance is a means of creating policies related to data, including how and where it is stored and sent, who has access to it and to what level, and what actions can be performed on the data, by whom, when, using what methods, and under what circumstances.

An effective data governance program must be both proactive and reactive. It is designed to protect the data and prevent any unauthorized access or exposure, but also contains a response plan that can be put in place quickly if an incident occurs.

Note: "Data governance" and "data management" are sometimes used interchangeably, and the two overlap in many areas. However, governance is only one of multiple elements in a data management model.[1]

[1] Data ManagementAssociation International. Data Management Body of Knowledge



Growth in digital data from 2010 to 2020

Why data governance matters

The amount of data that organizations collect and process is exploding. IDC Research predicted that the volume of digital data will expand at a compound annual growth rate of 42 percent over the decade of 2010 to 2020.[2] This growth is being driven by an ever increasing number of sources, and the data being generated now is more complex than ever.

As the amount of data in your organization increases, so do the demands on your organization to be compliant with legal and regulatory requirements to quickly find, keep and protect data. Spending days to find the specific protected data is not only expensive, it's not an option.

As your business grows, staying compliant in a sea of evolving global regulations adds new layers of complexity. Policy makers are rapidly adopting new international standards, and security and privacy concerns dominate in an ever-changing global business and social landscape. This is a challenge for any organization, large, medium, or small. Microsoft products and services can help you to address these challenges.

[2] EETimes. Digital Data Storage is Undergoing Mind-Boggling Growth

How data governance facilitates compliance efforts

A data governance program applies to many different types of data. Data can be classifed in many different ways. Effective data governance involves classifying data according to security requirements. The data that is collected, used, and stored by most organizations can be divided into a number of different categories based on the required security level.

The GDPR focuses on *personal data*. It also addresses special categories of personal data, also referred to as *sensitive data*. This is personal data that contains information about the data subject's racial or ethnic origins, political opinions, religious or philosophical beliefs, physical or mental health, sex life, genetic and biometric data, or membership in a trade union. It also includes information regarding criminal history and criminal court proceedings against a data subject.

Additional specific conditions must be met for the processing of these special categories of personal data.

Personal data is protected by the GDPR. Its disclosure could subject the data subject to substantial risk of loss of privacy as well as criminal victimization (e.g., identity theft). All personal data should be protected by the highest levels of security.

An important goal of a data governance program is to protect the needs of data stakeholders--individuals or groups who could affect or be affected by the data. These include those who create data, those who use data, and those who set rules and requirements for data. The focus in this paper is on protecting the privacy, confidentiality, and integrity of the personal data of EU citizens to help comply with the GDPR.

Steps to establish a data governance program

Processes and technologies can differ from one organization to another, as do implementation details, but the basic steps to establish a data governance program are the same:

Assign

Determine who will develop, implement, and manage the data governance program and the roles, responsibilities, and scope of authority of each, and the permissions required for each role to carry out its responsibilities.

Plan

Identify your requirements based on regulatory and legal mandates, business best practices, and organizational policies.

Decide

Establish rules to help meet those requirements.

Implement

Put in place policies, procedures, and processes (automated and/or manual) to enforce the rules.

Monitor

Track the status of rule enforcement on an ongoing basis.

Assess

Evaluate the success of your data governance program and make changes when necessary to increase its effectiveness.

The assignment of roles is one of the most important elements of data governance.

All organizations that deal with important data of any kind need a data governance plan, but in the context of GDPR compliance, there are some very specific requirements that fall under data governance. We will address those specifics in Part Two.

The assignment of roles is one of the most important elements of data governance; as with any task, choosing the right person for the job can make the difference between success and failure. We will discuss the roles and responsibilities associated with data governance in Part Three.

Each of the steps can include multiple parts. For example, implementation will involve research to determine the appropriate technologies for rule enforcement, and then testing of those products and services to ensure that they are adequate, and then integration into your organization's environment. We will discuss those sub-steps in more detail in Part Four.

Make data governance easier

Organizations today perform the steps discussed above manually, but the future of data governance will take the burden off of individuals in the organization and leverage machine learning to automate many of the processes and bring the information overload under control.

An intelligent, secure, enterprise-grade cloud that can be trusted lightens the overhead for administrators and users alike and allows you to focus more on your business and less on the details of compliance.

Microsoft cloud services empower you to find relevant information quickly and make informed decisions through automation. By leveraging these data insights, organizations can stay compliant and reduce risk. You keep what's important, and leave behind what's redundant, obsolete, or trivial automatically, so that the high-value content that is important to your business is efficiently protected for as long as you need it to be.

Shared responsibility for data governance in the cloud

Cloud computing can make data governance easier by giving organizations one centralized location for storing their data instead of having it spread across many different storage media. In addition, top cloud providers have the resources and expertise to apply the strongest available security measures. Microsoft implements advanced data protection and security features in its cloud services to safeguard data and privacy.

Storing and processing data in the cloud also creates a model of shared responsibility [3] for security and compliance in general and for data governance in particular. Cloud providers must implement and be accountable for measures to control physical access to data that is stored in and moves to and from their data centers, access to subscriptions, and physical resource management and tracking. The division of responsibilities differs depending on the cloud model (IaaS, PaaS, or SaaS).

[3] Shared Responsibilities for Cloud Computing

Microsoft applies best practices to the operation of its cloud services and provides customers with options and tools for securing the virtual machines, applications, and data that they run and store in the cloud. Because documentation is an important element in compliance, Microsoft provides customers with information regarding how their data is handled and protected in the cloud, as well as tools for applying additional security measures, such as enabling encryption in those cases where it isn't applied by default.

Guiding principles for data governance

There is more to data governance than processes and practices. It's important to keep in mind the guiding principles on which data governance is founded. These include:

- **Integrity**
- **Transparency**
- **Auditability**
- **Accountability**
- **Stewardship**
- **Standardization**
- **Change management**[4]

[4] The Data Governance Institute. Goals and Principles for Data Governance

Data management policies and standards should be based on these principles, and are impacted by a multiplicity of factors, such as business goals and strategies, IT objectives and strategies, data types and uses, and last but not least, regulatory requirements.

The remainder of this paper will focus on data governance as it applies to GDPR requirements.

02 GDPR data governance implications

The term “data governance” doesn’t appear anywhere in the text of the GDPR articles, yet data governance best practices are at the heart of its mandate to protect the privacy of personal data. An effective, well-documented data governance strategy helps organizations achieve and maintain GDPR compliance by establishing clear policies, procedures, and processes for managing and securing data, including personal data.

The GDPR was adopted in April 2016 with a two-year grace period; enforcement begins in May 2018. It supersedes EU Directive 95/46/EC, commonly referred to as the Data Protection Directive. As a regulation, rather than a directive, it is a binding legislative act[5] that applies across the EU. In contrast, a directive only sets out goals; it is up to the individual countries to define their own laws to achieve those goals, resulting in variable regulatory requirements from country to country.

The GDPR updates, clarifies, and expands upon the concepts that were addressed in the directive. In Article 3, the GDPR expands the territorial scope of the law to apply to the processing of personal data by organizations established in the EU regardless of whether it takes place within the EU. It also applies to controllers and processors without a presence in the EU who offer goods and services to individuals in the EU or monitor their behavior (such as tracking individuals online to create profiles via website cookies).

Data governance, as it pertains to the GDPR, is a means of protecting the privacy of personal data. At the same time the GDPR expands the territorial scope, it also expands the definition of what is considered "personal data" under the regulation. The new definition includes *any data that can be used to directly or indirectly identify a person (data subject)*.

[5] European Union Regulations, Directives and other acts

A "data subject" is an identified or identifiable natural person. A natural person is generally defined as an individual human being; this does not include a corporation or other legal entity that may be considered a "person[6]" for legal purposes.

"Any data" in the context of this definition refers to (but is not limited to) information such as names, addresses, email addresses, IP addresses, identification numbers, biometric identifiers (fingerprints, iris patterns, DNA), physical or physiological attributes, occupation, location, medical/health information, or even website cookies.

GDPR Recital 30 addresses online identifiers that include "devices, applications, tools, and protocols, such as internet protocol addresses, cookie identifiers, or other identifiers such as radio frequency identification tags." When these leave traces that can be combined with other unique identifiers to create profiles of natural persons and identify them, they may fall under the definition of personal data.

[6] Merriam-Webster Law Dictionary

GDPR principles for processing

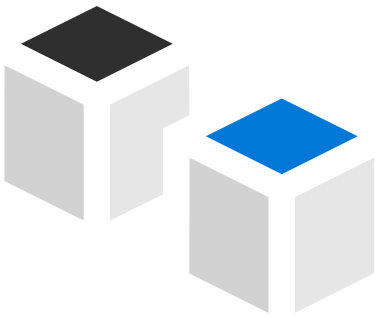
In Article 5, the GDPR lays out basic principles for the processing of personal data, and subsequent articles prescribe specific requirements in keeping with those principles. The principles are aimed at ensuring that personal data is collected lawfully, is accurate, is properly secured, and is limited in purpose, use, and duration of storage.

The GDPR principles align closely with the more generally accepted guiding principles for data governance that were discussed in Part One of this paper.

GDPR requirements and data governance

The GDPR requirements lay out specific instructions regarding how personal data is to be collected, processed, used, and stored in keeping with the principles discussed above. These requirements can be divided into four broad categories that also form the basis for an effective data governance plan:

- Data discovery (identification and classification of personal data)
- Data management (including response to the requests of data subjects)
- Data protection (all aspects of securing personal data)
- Reporting (documentation of activities and conditions pertaining to personal data)



Data discovery and management

The ability to quickly find data and manage it effectively and efficiently are cornerstones of data governance. Chapter 3 (Articles 12-23) of the GDPR addresses the rights of data subjects. These rights include a data subject's right to access their personal data and details regarding associated processing activities, as well as a means to submit requests for data rectification, erasure, and the export of that personal data.

Having informed the data subject of their rights at collection, an organization processing personal data will need to facilitate the exercise of these rights by providing a method to request enforcement of a data subject right, and processes and supporting technology to discover (identify) the personal data, and to manage and respond to these requests.

The right to data portability means controllers must provide a copy of the personal data to the data subject in a commonly used, machine-readable format. The data subject also has the right to transmit that data to another controller under certain circumstances. Data subjects have the right to object to the processing of their personal data, and to not be subject to a decision based solely on automated processing if the decision significantly affects the data subject.

One of the most important purposes of a data governance plan, for organizations that are subject to the GDPR, is the protection of these rights.

Data protection

Security is a critical component in data governance. Article 32 of the GDPR addresses the security of processing of personal data. It applies to both controllers and processors, and mandates that they "shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk."

This mandate specifically names pseudonymisation and encryption of personal data as measures that should be taken when appropriate, and on a much broader scale, further requires "the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services."

Recognizing that regardless of the level of security, incidents may occur, the article goes on to specify that security measures should include "the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident."

It is not enough to have security and incident response measures in place. It is also necessary to establish a process for regularly testing and evaluating the effectiveness of those technical and organizational measures.

Reporting and documentation

Documentation is a vital aspect of data governance. Under the GDPR, records must be retained to show that:

- Data was collected lawfully
- Consent (if applicable) was freely given
- Data subject's rights requests were appropriately managed
- Appropriate security measures were taken to protect personal data and respond to incidents
- Required notifications were made
- Data protection impact assessments (DPIAs) were carried out (when required)
- A data protection officer (DPO) were designated (when required)

Microsoft products and services that can help customers demonstrate compliance with these requirements will be discussed in more detail in Part Five.

Discover

Manage

Protect

Report

Defining roles and responsibilities under the GDPR

At the highest level, the GDPR recognizes two important roles that are assumed by organizations that deal with the personal data that falls under its regulations: controllers and processors. The GDPR differentiates between the two and assigns different responsibilities to each. Chapter 1, Article 4 provides precise definitions:

Controller: the natural or legal person, public authority, agency, or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Processor: a natural or legal person, public authority, agency, or other body that processes personal data on behalf of the controller.

The controller controls the processing of the personal data, whereas the processor performs the processing on the controller's behalf. The same organization can act as both controller and processor, or the two roles can belong to two separate organizations. In most cloud services relationships, the customer is the controller and the cloud services provider is the processor that carries out the processing on behalf of the customer.

The data protection directive did not impose specific and direct legal obligations on processors. The GDPR changes that and expands the scope of the requirements to include processors along with controllers.

Chapter 4 (Articles 24-43) lays out the responsibilities of controllers and processors in complying with the regulation, including security of processing and records of processing activities. Security measures implement and enforce the principles and policies of data governance, and tracking and recording document adherence to the data governance plan.

Controllers are specifically required to demonstrate compliance with the seven principles that are listed in Article 5 and discussed in the previous section. Controllers also must implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this regulation. Those measures shall be reviewed and updated where necessary.

The GDPR prohibits organizations from using third-party data processors unless those processors guarantee by contract their ability to implement the technical and organizational requirements of the GDPR. As a processor, Microsoft has extensive expertise in protecting data, championing privacy, and complying with complex regulations, and is committed to GDPR compliance. Microsoft makes available the contractual guarantees[7] required of processors by the GDPR, including assisting its customers in responding to data subject requests to correct, amend, or delete personal data, detecting and reporting personal data breaches, and helping its customers demonstrate compliance with the GDPR.

In devising a data governance plan, both controllers and processors should establish policies and assign responsibilities within their organizations for access, management, and use of personal data.

[7] Earning your trust with contractual commitments to the General Data Protection Regulation

Assigning roles and responsibilities within the organization

A successful data governance model in an enterprise environment requires the cooperation of many people working together across many business units and at many levels, from the senior leadership team down to the IT implementers and the users who create and access the data.

Depending on the organization and its size and structure, data governance roles and responsibilities will involve some or all of the following levels:

- Executive (Typically C-level Managers)
- Strategic (Data Governance Council)
- Tactical (Data Domain Stewards, Data Steward Coordinators)
- Operational (Operational Data Stewards; Includes Data Users)
- Support (Data Governance Partners; Includes IT, Information Security, Risk Management, and Compliance)

The list above is based on the Data Governance Roles and Responsibilities Pyramid[8]. In smaller organizations, roles may need to be combined, with one person or a group assuming multiple roles.

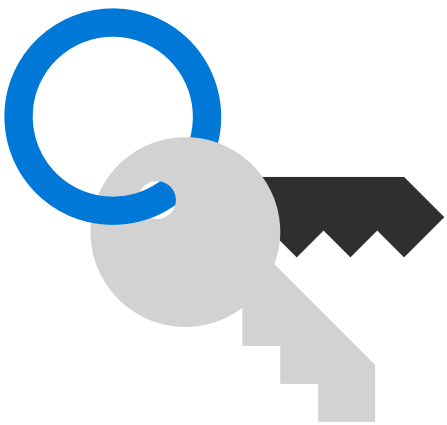
Executives at the top level of the organization have ultimate decision-making authority over the data governance program and appointment of the Data Governance Council members.

A Data Governance Council reports to the executive level and is responsible for coordinating and communicating data governance activities across organizational divisions.

IT and Security roles include data classification, technical handling of data, securing the infrastructure, and ensuring that projects follow data governance best practices.

Data Stewards include data custodians and data subject matter experts (SMEs). They are responsible for management of data and for documenting rules for data and communicating those rules to data stakeholders.

Additional roles, depending on the organization, may include data architects (who design the structure and organization of data) and data analysts (who research and analyzes problems with the data and data quality).



[8] CompleteSetofDataGovernanceRoles&Responsibilities

Data governance programs for small businesses will necessarily be structured differently. The internal organization is different from that of an enterprise, and budgets may be tighter so that there is less funding for formalizing a data governance program. Nonetheless, data governance is important regardless of business size.

Cloud services can help to enable small businesses to implement better data governance at lower cost, thanks to the shared responsibility model and the economies of scale that allow cloud providers such as Microsoft to offer management and security measures that would be too costly for small organizations to deploy on their own.

Assigning roles at the technological level

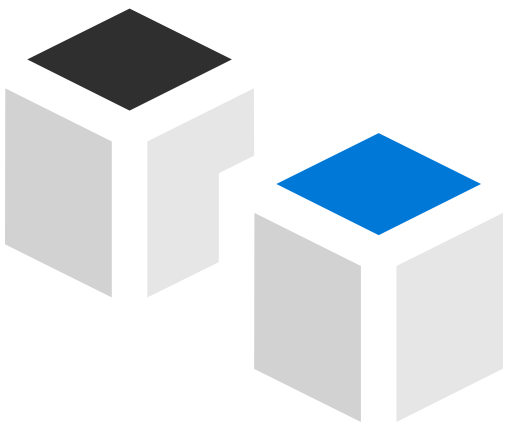
From the IT implementation perspective, the roles of users and groups of users can be leveraged as a means of controlling access to data and other network resources. Role-based access control (RBAC) regulates the ability of users in different roles to perform specific tasks. Roles are based on job description, responsibilities and level of authority. Permissions are assigned to each role, on a need-to-know or "principle of least privilege" basis.

The GDPR, in Article 25(2), imposes upon controllers the obligation to "implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed." It goes on to say that "In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons."

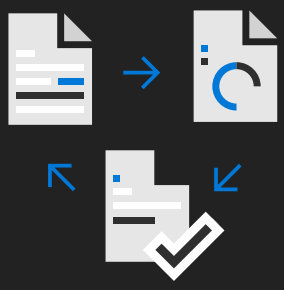
Microsoft products and services provide the means to technologically enable data governance by defining user roles for access, management, and use of personal data, and to apply and enforce policies based on roles. This will be discussed in more detail in Part Five.

03 Building blocks of a data governance program

Building a data governance program is based on a three-pronged approach; it involves policy, processes, and people. The effectiveness of the data governance program is dependent on the planning and thought that goes into the policies and processes, and the selection, education, and motivation of the people who are involved.



Policy



Process

People

Policy prioritizes the quality, integrity, and trustworthiness of data, and the confidentiality and privacy of personal data, as a business objective.

Processes ensure the enforcement of policies through standardized automated or manual procedures. This includes both the operations performed to accomplish a task (such as correcting an error in personal data in response to a data subject's request) and the technologies that are used to carry out the operations.

People, consisting of organizational leadership, IT and security implementers, data stakeholders, and stewards (all of the data governance roles within an organization that we discussed above), are the drivers of both policy and processes, and the technologies used to implement them.

For policies and processes to work, people must be engaged. Users disregard or actively circumvent policies that are difficult to understand or seem unreasonable, and resist using processes that are time-consuming, have a steep learning curve, or drastically change the way they work. Smooth adoption by the people who work with the data requires policies that make sense and have a clear benefit, and processes that are user-friendly.

Data governance policy and processes should address the following broad areas:

- Data acquisition
- Data discovery (identification and classification)
- Data ownership and accountability
- Data management (including management of metadata)
- Data access and usage
- Data protection (through file level, disk/volume level, and network level security)
- Documentation of all of the above

The policy-making phase should take all of these into account. Once all of the building blocks are in place and the framework for your data governance program has been built, you can move on to the implementation phase, where the processes for each stage of the data management and protection lifecycle are clearly defined.

04 Data governance implementation and technologies

Successful implementation of a data governance program is a team effort, joining the business experts, IT professionals, IT security, and compliance specialists to turn policies and procedures that exist only on paper into working processes.

The business team includes subject matter experts who understand how the data is used to accomplish the business objectives and goals, and who help develop the policies for its use. The IT team understands the technology that is used to store and process the data and that can be used to enforce the policies established on the business side. The security team understands the technologies that can be used to protect the data in a multilayered security strategy. The compliance team understands the regulatory requirements that drive the policies and how the technologies can assist in meeting them.

All parts of this triad must work together to get both the human processes and the technological tools into place that will enable data governance practice and enforcement.

When GDPR compliance becomes a driving force for data governance, it becomes even more important to get it right. Knowledgeable and dedicated teams of people lay the foundation for effective data governance, but successful implementation also depends on having the right technologies and tools to do the job.

The Microsoft Cloud, with a large investment in research, is taking some of the burden out of compliance processes and is now leading in compliance certifications and strong data privacy commitments.

Microsoft offers a number of technological solutions to help customers manage and fulfill GDPR mandated obligations to data subjects, whether the data is processed and stored in the Microsoft Cloud or in the customers' on-premises data centers.

These include features, functionalities, and tools for identifying, classifying, managing, and securing personal data, as well as tracking, monitoring, and reporting tools to help document measures taken to meet compliance requirements.

Data discovery: identification and classification

An important component in an effective data governance plan and the first step toward meeting many of the obligations identified in the GDPR is to identify personal data managed by the controlling organization, so appropriate measures can be taken to protect it and to facilitate Data Subject Rights requests.

The policies

A data classification policy prescribes how data is to be handled, based on the level of security/privacy it requires. The first step in determining what protections should be applied to a particular type of data is to determine its classification. Data classification policies assign levels and the extent to which data at each level is to be controlled and secured. Personal data, including special categories of personal data, must be labeled as such for easy identification.

The processes

A mature data classification process enables organizations to more effectively understand their use of personal data, as well as apply security measures and access rights based on sensitivity levels. The data discovery, identification, and classification processes use search methods to locate data of a certain type (in this case, personal data) and tagging or labeling it to make it easy to find, alter, and apply management and security operations to it.

Microsoft services and products provide features and functionalities that can be used to manage personal data and respond to data subjects' requests.

Data management and response to data subject requests

Data governance is based on sound data management policies and the means to enforce those policies. Data management includes the ability to not only locate and identify personal data but also the ability to correct inaccurate data, add to incomplete data, erase data, and restrict or discontinue the processing of data.

The GDPR gives data subjects the right to request such rectification, erasure, restriction, or discontinuation, and organizations need the technological tools to respond to those requests in a timely manner. The GDPR also provides data subjects with the right to request that a controller erase their personal data in certain circumstances.

Further, data subjects have the right to request and receive their personal data from controlling organizations in a "structured, commonly used and machine-readable format."

Microsoft services and products provide features and functionalities that can be used to manage personal data and respond to data subjects' requests.

Data protection and security

Protecting and securing data is an essential element of a data governance plan, and Microsoft services and products provide numerous built-in security mechanisms, as well as additional optional security features that can be enabled by the customer.

The GDPR states that organizations collecting or processing personal data must implement "appropriate technical and organizational measures" to implement data protection principles and to integrate the necessary safeguards into processing to meet GDPR requirements and protect the rights of data subjects. The GDPR specifically identifies encryption as one tool that may facilitate this requirement.

In addition, the requirements of the GDPR regarding the protection of personal data expect organizations to have implemented security controls to prevent, detect, and respond to vulnerabilities and personal data breaches.

The GDPR requires organizations to operate according to a "privacy by design and privacy by default" model. Microsoft has been building its services and products on such a model for many years, incorporating security features that help to protect data whether it is at rest or in transit across the network and giving customers control over the collection, use, and distribution of their data. Additional information on this topic can be found in the Microsoft Trust Center.

Reporting and documentation

Documentation is an essential element in both business and IT. Human memory is fallible; written records preserve an accurate account of an agreed-upon policy, procedural steps, or past actions that were taken including when, where, how, and by whom.

To achieve GDPR compliance, not only must you meet the regulation's requirements regarding management and protection of personal data, you must also be able to offer evidentiary documentation to prove that you did so. This includes records showing lawful basis for data collection and processing (and when consent is the basis, showing that it was obtained according to the requirements), as well as keeping records of processing operations performed on personal data and information documenting your security policies and procedures and configurations.

To demonstrate that data subject rights requests were appropriately managed, records must be retained illustrating the result of data subject rights requests. Additional records should contain not only the nature of the request (e.g., view, edit, etc.), but also the resolution of the request. These records should be available for regulatory authorities on request.

Microsoft services and products provide logging and auditing features and tools that allow organizations to track and record processing activities.

Summary

Meeting the data governance challenge

Managing information effectively to meet internal and external compliance requirements is more complex today than ever, due to the exponential growth in the amount of data coupled with new regulations, such as those imposed by the GDPR. For organizations that are impacted by the legislation, protecting the privacy of individuals is no longer just a good business practice; it's a legal obligation.

The solution begins with effective data governance, which traditionally involves many people acting in various roles at all levels of the organization. The future of data governance is the automation of more processes, taking the burden off of IT professionals and users and leaving them free to focus on the business. This reduces cost and increases efficiency.

Microsoft's products and services deliver intelligent information governance solutions that address identifying, classifying, managing, and protecting data, including personal data as defined by the GDPR. In today's data-driven business environment, your data governance framework is an essential element in your overall security and compliance strategy. Microsoft provides tools to help you meet the data privacy and security challenges that you face in achieving your compliance goals.

Appendix

Further reading and resources

This white paper provides an overview of data governance as it pertains to the GDPR, and how Microsoft services and products can help implement a data governance program. Data governance is a broad topic, and GDPR compliance is a complicated subject. The following resources offer a deeper look at various aspects of the GDPR and data governance.

GDPR legislation

Full text of the General Data Protection Regulation (PDF)
Final text of the GDPR including recitals, searchable

White papers

Enhance your GDPR compliance with the Microsoft cloud

How Microsoft Azure Can Help Organizations Become Compliant with the EU GDPR

Guide to enhancing privacy and addressing EU GDPR requirements with the Microsoft SQL platform

Websites

The Microsoft Trust Center provides resources on how Microsoft implements and supports security, privacy, compliance, and transparency in all our cloud products and services.

The Data Governance Institute provides vendor-neutral data governance best practices and guidance.