Accountability and Demonstrating Compliance

In addition to Article 5(2), Article 24(1) of the GDPR also requires a data controller to demonstrate that data processing activities comply with the GDPR's requirements. Together, Articles 5 and 24 form the concept of accountability under the GDPR, which is a key element of the regulation.

Meeting the accountability requirement means doing more than just establishing data protection policies and procedures. Accountability requires a data controller to be able to demonstrate compliance with the GDPR by showing the supervisory authority and individuals how the data controller complies, on an ongoing basis, through evidence of:

Internal policies and processes that comply with the GDPR's requirements.

The implementation of the policies and processes into the organization's activities.

Effective internal compliance measures.

External controls.

The obligation to demonstrate compliance replaces the obligation to notify local data protection authorities of processing activities, which was a requirement under the EU Directive and its local implementing laws in several EU member states. The effect of the GDPR's accountability principle is that organizations subject to the legislation must implement a formal data protection compliance program. For more on developing a privacy compliance program.

Complying with the accountability principle requires the data controller to:

Establish a data protection compliance program and privacy governance structure

Implement and maintain privacy controls on an ongoing basis

Embed ongoing privacy measures into corporate policies and day-to-day activities, throughout the organization and within each business unit that processes personal data

Leverage technology to require or ensure compliance

Maintain documentation of the privacy measures implemented and records of compliance

Train employees on privacy and data protection matters

Regularly test the privacy measures implemented

Use the results of testing, other audits, or metrics to demonstrate both existing and continuous compliance improvement efforts

Failure to comply with the accountability principle may result in fines of up to EUR20 million or 4% of the organization's total worldwide annual revenue for the preceding financial year, whichever is higher (Article 83(5), GDPR). Demonstrating compliance may help reduce the data controller's or data processor's risk of liability including administrative fines.

Obligations Requiring a Demonstration of Compliance

The GDPR imposes many different obligations on data controllers, and sometimes data processors, that either explicitly or implicitly, require the data controller or data processor to demonstrate compliance with the GDPR's requirements including:

Establishing and maintaining a comprehensive data protection compliance program and appointing individuals responsible for overall data protection matters as part of the program, including, but not limited to:

an EU representative; and

a data protection officer

Embedding privacy measures into policies and operations, including, implementing appropriate technical and organizational measures.

Complying with processing obligations and documenting compliance including:

determining and documenting a lawful basis for each instance of processing personal data

maintaining a record of data processing activities

providing data subjects with a GDPR-compliant privacy notice

satisfying specific requirements when relying on data subject consent

satisfying specific requirements when processing special categories of personal data

honoring data subject rights, including rights relating to automated decision making and profiling and

complying with cross-border data transfer restrictions and maintaining compliant data transfer mechanisms

Delivering ongoing data protection training through formalized training and communication efforts

Making explicit arrangements with joint data controllers

Taking certain steps when engaging data processors and managing third-party relationships

Privacy Governance Structure

Establishing and maintaining a comprehensive data protection compliance program is a helpful and demonstrable way to implement the GDPR's requirements and support continuous compliance. Formalizing a privacy governance structure is a good foundation on which to build the larger data protection compliance program. A privacy governance structure may include, among other things:

Establishing a privacy office and assigning responsibility for implementing and maintaining a privacy compliance program to a privacy officer or other individuals in the organization.

Educating senior management about the GDPR's requirements and the impact of non-compliance.

Identifying key stakeholders.

Developing a privacy framework.

Designating roles with specific responsibilities and tasks.

Establishing reporting lines and regular communication between the privacy office and internal stakeholders.

As part of establishing a privacy governance structure, under certain circumstances, the GDPR requires data controllers and data processors to appoint:

An EU representative

A data protection officer

EU Representative

Data controllers and data processors not established in the EU must, subject to limited exceptions:

Designate, in writing, a representative in the EU.

The representative must be:

established in an EU member state where the organization's data subjects are located; and

addressed by supervisory authorities and data subjects on all issues relating to data processing, in addition

to or instead of the data controller or data processor.

(Article 27(1), GDPR.)

Document Appointment of EU Representative

Documenting the appointment of the EU representative may help demonstrate compliance with Article 27(1) of the GDPR. Examples of documentation include:

A written designation of a representative in the EU to act on behalf of the data controller or data processor.

Identification of the EU representative, including contact details, in a privacy notice, on a website, or via another mechanism to ensure data subjects are informed.

Data Protection Officers

A data controller or data processor must appoint a data protection officer when:

A public authority or body, except for courts acting in their judicial capacity, carries out the data processing.

The core activities of the data controller or data processor consist of:

the regular and systematic monitoring of data subjects on a large scale; or

large-scale processing of special categories of personal data or personal data relating to criminal convictions and offenses.

(Article 37(1), GDPR.)

The data protection officer must:

Be professionally qualified and have expert knowledge of data protection law and practices (Article 37(5), GDPR).

Be involved in all matters relating to data protection (Article 38(1), GDPR).

Report to the highest level of management within the data controller or data processor (Article 38(3), GDPR).

The GDPR requires data protection officers to carry out certain tasks including, but not limited to:

Advising the data controller or data processor and employees of their obligations under the GDPR and other applicable data protection laws, including providing training to employees involved in personal data processing (Article 39(1)(a) and (b), GDPR).

Monitoring compliance with the GDPR, other applicable laws, and the data controller's or data processor's policies and procedures relating to data protection (Article 39(1)(b), GDPR).

Advising on data protection impact assessments (Article 39(1)(c), GDPR).

Cooperating with supervisory authorities and acting as the point of contact on issues relating to data processing (Article 39(1)(d), GDPR).

The data controller or data processor must publish the contact details of the data protection officer and provide these details to the relevant supervisory authority (Article 37(7), GDPR).

Although the GDPR does not require every organization to appoint a data protection officer, organizations may voluntarily choose to appoint one to head and manage their privacy governance structure.

Document Appointment and Responsibilities of the Data Protection Officer

Documentation to help demonstrate compliance with requirements relating to data protection officers under Articles 37, 38, and 39 of the GDPR includes, but is not limited to, records demonstrating:

That the data controller or data processor appointed a data protection officer and provided the data protection officer's contact details to the relevant supervisory authority.

The data protection officer's qualifications, such as resumes and certifications.

The data protection officer's responsibilities such as job descriptions or similar mandates, or any service contract with the data protection officer, if applicable.

The reporting structure such as an organizational chart, showing that the data protection officer reports to the highest level of management.

Communication between the data protection officer and management on data protection matters.

The data protection officer's involvement in the data privacy impact assessment process such as providing advice and monitoring the performance of these assessments.

The content of data protection training programs and evidence that employees completed these trainings.

That the data protection officer regularly monitors changes to applicable law and privacy and data protection practices to ensure continued compliance.

Embed Data Protection into Operations

To comply with the GDPR and demonstrate compliance with its requirements, the data controller must embed data protection measures into corporate policies and procedures and day-to-day activities throughout the organization. This means implementing internal policies and procedures, including an organizational level data protection policy, on handling personal data, which should include, but not be limited to, policies and procedures on:

Collection and use of special categories of personal data or personal data relating to criminal convictions and offenses

Collection and use of personal data about children and minors, including obtaining parental consent

Secondary uses of personal data

Obtaining valid consent

Maintaining data quality.

Anonymizing or pseudonymizing data

Processing personal data by automated means

Personal data retention and secure destruction.

Security breach management

Using personal data for direct marketing.

Using personal data in research.

Information security including the specific security measures implemented

Data controllers must not only maintain internal policies and procedures, but must ensure that it integrates data protection measures into the organization's practices and that employees follow the policies and procedures in their day-to-day activities. To help ensure that policies and procedures are fully integrated and followed organizations should implement regular training and use testing, audits, and other documented mechanisms to measure and demonstrate compliance.

The GDPR also requires data protection by design and by default as part of integrating data protection into the organization on an ongoing basis.

Data Protection by Design and by Default

The GDPR requires data controllers to integrate data protection into their systems and product designs to ensure the inclusion of appropriate technical and organizational GDPR compliance measures into personal data processing means (Article 25(1), GDPR).

Data controllers must also implement "privacy by default" measures to ensure that, by default, they only process the personal data necessary for each specific business purpose (Article 25(2), GDPR). The European Data Protection Supervisor published a preliminary opinion on privacy by design (Opinion 5/2018).

Conducting Regular Training to Integrate Policies and Procedures

One of a data protection officer's responsibilities is to advise employees of their obligations under the GDPR and other applicable data protection laws, including providing training to employees involved in personal data processing (Article 39(1)(a) and (b), GDPR).

Training is not an explicit GDPR obligation for organizations that are not required to appoint a data protection officer. However, to embed data protection into the organization's operations and daily activities effectively, the organization should still implement regular data protection training. Demonstrating compliance without effective and ongoing employee training programs on the organization's policies and procedures including how the organization integrates those policies into its actual practices becomes difficult.

Organizations should:

Implement a regular training program, including specialized training based on an employee's job function.

Implement a policy on when and how the organization conducts data protection training and refresher training courses and consider adding data protection training to the data controller's or data processor's core annual training curriculum.

Consider implementing regular bulletins and other mechanisms to deliver updates and reminders on data protection matters to the entire staff.

Implement a process to record when employees complete the required training.

Enforce the requirement to complete data protection training.

Using Codes of Conduct and Certifications to Demonstrate Compliance

The GDPR approves the use of codes of conduct (Article 40, GDPR) and certifications (Article 42, GDPR) to help demonstrate compliance with certain GDPR obligations. Participating in certification programs or adhering to established codes may help demonstrate compliance with requirements under the following GDPR Articles:

Responsibilities of the controller (Article 24, GDPR). A data controller may use adherence to approved codes of conduct or certification programs to demonstrate compliance with its obligations to implement appropriate technical and organizational measures to ensure processing complies with the GDPR's requirements.

Data protection by design and by default (Article 25, GDPR). Adherence to an approved certification program helps demonstrate that an organization integrated data protection into its data processing by design and by default.

Processor (Article 28, GDPR). Adherence by a data processor to a code of conduct or certification program

helps demonstrate that the processor provides sufficient guarantees that it implements appropriate technical and organizational measures to ensure processing complies with the GDPR's requirements.

Security of processing (Article 32, GDPR). Adherence to a code of conduct or certification program helps demonstrate the implementation of technical and organizational measures that ensure a level of security appropriate to the risk.

Data protection impact assessment (Article 35, GDPR). Adherence to a code of conduct is considered in assessing the impact of the processing operations performed by the data controller or data processor.

Transfers subject to appropriate safeguards (Article 46(2), GDPR). Adherence to a code of conduct or participation in an approved certification program can provide appropriate safeguards to support personal data transfers outside of the EU.

The Article 29 Working Party (now the European Data Protection Board (EDPB)) issued guidelines for accrediting certification bodies under the GDPR (WP261, adopted on 6 February 2018).

The EDPB has also adopted the Article 29 Working Party's draft guidelines on certification and identifying certification criteria under Articles 42 and 43 of the GDPR.

The European Commission has encouraged the use of codes of conduct and certification programs to legalize cross-border data transfers. Codes of conduct have been submitted to the Article 29 Working Party (now the EDPB) for cloud infrastructure service providers and for Health applications.

Using Technical and Organizational Measures to Demonstrate Compliance

Data controllers must implement appropriate technical and organizational measures to ensure:

That processing complies with the GDPR's requirements (Article 24(1), GDPR).

A level of security that is appropriate to the risk (Article 32(1), GDPR).

When assessing the appropriate level of security, the data controller or data processor should consider the risks presented by processing the personal data, including the risks associated with accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data (Article 32(2), GDPR).

To determine whether measures are appropriate, the data controller or data processor should conduct a risk assessment and consider the nature, scope, context, and purposes of processing, as well as the likelihood and severity of the risks to the data subjects' rights. As part of implementing appropriate measures, the GDPR requires data protection by design and by default and data protection impact assessments under certain circumstances.

Data Protection Impact Assessments

The GDPR requires a data protection impact assessment under certain circumstances, including where the processing is likely to result in a high risk to the rights and freedoms of data subjects (Article 35, GDPR). This applies when the data controller implements new programs, systems, or processes, or when the data controller makes changes to programs, systems, or processes. The GDPR specifically requires data protection impact assessments when the data controller engages in:

Automated processing, including profiling, that produces legal or other significant effects for a data subject.

Large scale processing of special categories of personal data (Article 9) and processing personal data relating to criminal convictions and offenses (Article 10).

Large scale, systematic monitoring of a publicly accessible area.

(Article 35(3), GDPR.)

Supervisory authorities may specify additional types of processing that require a data protection impact assessment or exclude processing types from the data protection impact assessment requirement, so data controllers should always check with the relevant supervisory authority.

When a data protection impact assessment indicates that processing would result in a high risk to data subjects, the data controller must consult with the relevant supervisory authority (Article 36, GDPR). For more information on data protection by design and by default, and on conducting data protection impact assessments.

Document Risk Assessments and Technical and Organizational Measures
Documentation to help demonstrate compliance with the obligation to assess risk and implement technical and organizational measures appropriate to the risk, includes:

Policies or procedures requiring the incorporation of data protection mechanisms into the technical specifications of IT systems, networks, processing operations, and business practices.

Data protection impact assessment templates specifying the assessment information required by Article 35(7).

Completed data protection impact assessments, audits, or other risk assessments which include:

identification of risks, including high-risk data processing;

risk mitigation plans;

identification of the lawful basis for processing personal data;

verification that data processing complies with the GDPR;

evidence that the organization integrated necessary safeguards into systems, networks, and processing operations;

evidence that the organization reviewed processing activities and risks considering changes to programs, systems, or processes; and

confirmation that the organization made updates after program, system, or process changes affecting data protection risk.

Documentation showing consultation with the relevant supervisory authority in the case of high-risk processing.

Documentation that the data controller sought the data protection officer's advice during the data protection impact assessment process.

Evidence of regular security measure testing and an evaluation of those measures' effectiveness.

Detailed data privacy requirements for third parties that receive or access personal data such as data processors, including contracts with third parties. For more on steps to take when transferring personal data to a data processor.

Security Breach Management
The GDPR establishes new personal data breach notification requirements that require data controllers to:

Notify the relevant supervisory authority without undue delay and no later than 72 hours after any breach of personal data that poses a risk of harm (Article 33, GDPR).

Notify the data subject without undue delay if the personal data breach poses a risk of harm, subject to certain limited exceptions (Article 34 and Recital 86, GDPR).

The GDPR also specifies the notice's required contents to supervisory authorities (Article 33(3), GDPR) and data subjects (Article 34 (2), GDPR). Data subject notices must also comply with the data subject communication requirements in Article 12. The data controller must also document any personal data

breaches (Article 33(5), GDPR).

Implement a Security Breach Management Plan and Document Incidents

Documentation to help demonstrate compliance with the GDPR's personal data breach notification requirements includes, but is not limited to:

A security breach response plan including a protocol for notifying regulators, law enforcement, other agencies, and data subjects.

Identification of a security breach response team.

Template breach notification letters that comply with Articles 33 (Notification of a personal data breach to the supervisory authority), 34 (Communication of a personal data breach to the data subject), and 12 (Transparent information, communication and modalities for the exercise of the rights of the data subject).

A log for recording security incidents and security breaches, including a summary of the incident, its effects, and the responsive action taken.

Details of the analysis used to determine whether a security breach poses a high enough risk to require notification.

Document Compliance with Processing Requirements

Lawfulness of Processing
A data controller must have a lawful basis for processing personal data. Processing is lawful under Article 6 of the GDPR if one of the following applies:

The data subject consents to the processing.

The processing is necessary for:

performing a contract with the data subject;

complying with a legal obligation;

protecting the vital interests of the data subject;

performing a task carried out in the public interest; or

pursuing the legitimate interests of the data controller or a third party, except where the data subject's interests or fundamental rights and freedoms override the data controller's interests.

(Article 6(1), GDPR.)

A data controller generally cannot use personal data for a different purpose than the one it collected the personal data for, unless the secondary use purpose is compatible with the original purpose of use. Article 6(4) specifies how to determine when further processing for a different purpose than the data controller originally collected the personal data for is consistent with the original processing purpose. For more information on processing personal data under the GDPR.

Document a Lawful Basis for Processing Personal Data

Documentation to help demonstrate a lawful basis for processing includes, but is not limited to:

A record specifying the lawful basis for processing personal data under Article 6.

Policies and procedures for obtaining valid data subject consent under the GDPR and a record of valid consents obtained.

Completed data protection impact assessments or other risk assessments for new processing operations or when making changes to processing operations.

Completed data protection impact assessments or other risk assessments detailing the analysis used to determine the lawful basis for processing.

Policies and procedures on determining whether secondary uses of personal data are compatible with the original purpose of use.

Policies and procedures on using personal data for secondary purposes different than the purposes originally notified to the data subject.

Record of Processing Activities

The GDPR establishes specific data processing recordkeeping requirements in Article 30. Data controllers and data processors must, subject to limited exceptions:

Maintain a written or electronic record of its data processing activities, including specific information for data controller activities (Article 30(1), GDPR) and for data processor activities (Article 30(2), GDPR).

Make the record available to the supervisory authority on request (Article 30(4), GDPR).

Maintain a Current Data Inventory of Processing Activities

To help demonstrate compliance with Article 30's recordkeeping requirements, data controllers, and if applicable a data controller's representative, should maintain a current and detailed data inventory of processing operations that includes the following information:

The name and contact details of:

the data controller;

any joint controllers, if applicable;

the data controller's representative, if applicable; and

the data protection officer, if applicable.

The purposes of data processing.

A description of the categories of data subjects and categories of personal data.

The categories of third-party data recipients including recipients in other countries.

For transfers to countries outside of the European Economic Area (EEA), identification of the country and the safeguards used to secure the transfer.

Storage periods for the different categories of personal data.

A general description of the technical and organizational security measures used to secure the personal data.

(Article 30(1), GDPR.)

Data processors have a similar obligation under Article 30(2). Data processors, and if applicable a data processor's representative, should maintain a current and detailed data inventory of processing operations that includes the following information:

The name and contact details of:

the data processor or data processors;

each data controller that the processor acts on behalf of;

the controller's or processor's representative, if applicable; and

the data protection officer, if applicable.

The categories of data processing that the data processor carries out on behalf of each data controller.

For transfers to countries outside of the EEA, identification of the country and the safeguards used to secure the transfer.

A general description of the technical and organizational security measures used to secure the personal data.

(Article 30(2), GDPR.)

Privacy Notice Requirements

A data controller uses a privacy notice to provide data subjects with certain information about its data processing activities. Information provided to data subjects must be:

Concise.

Transparent.

Intelligible.

Easily accessible.

In clear and plain language.

A data controller can provide the required information:

In writing.

Electronically if appropriate.

Orally in some cases.

(Article 12(1), GDPR.)

To help ensure fair and transparent processing, data controllers must:

Provide specific information to data subjects at the time of data collection when collecting data directly from them (Articles 13(1) and (2), GDPR)

Provide specific information to data subjects when collecting data from third parties (Articles 14(1) and (2), GDPR)

Satisfy specific timing requirements for providing the privacy notice when collecting personal data from a party other than the data subject (Article 14(3), GDPR).

Provide additional information to the data subject if the data controller intends to use personal data for a different purpose than originally notified to the data subject (Articles 13(3) and 14(4), GDPR)

Data subjects have the right to object to processing based on certain grounds under Article 21 of the GDPR Data controllers should also notify data subjects if they carry out processing for one of these purposes and of the right to object to the processing, including processing done:

For the performance of a task in the public interest under Article 6(1)(e) (Article 21(1), GDPR).

For the purposes of the legitimate interests pursued by the data controller or a third party, except where the data subject's interests or fundamental rights or freedoms override these interests under Article 6(1)(f) (Article 21(1), GDPR).

For direct marketing purposes (Article 21(3), GDPR).

For scientific or historical research purposes or statistical purposes under Article 89(1) (Article 21(6), GDPR).

Maintain Compliant Privacy Notices

Documentation to help demonstrate compliance with the privacy notice requirements includes, but is not limited to:

Policies and procedures describing when and how the data controller provides privacy notices to data subjects when collecting personal data directly from data subjects or from third parties.

Copies of dated privacy notices provided to data subjects when data is collected directly from data subjects or from third parties, which satisfy the various notification requirements established in Articles 12, 13, and 14 of the GDPR.

Policies and procedures on using personal data for secondary purposes different than the purposes originally notified to the data subject.

Policies and procedures on data subject rights, such as the right to object to processing.

Consent Requirements

Data subject consent is one of several legal bases for processing personal data under Article 6(1). The data controller must satisfy certain requirements when relying on consent to process personal data, including a requirement that the data controller demonstrate that it obtained the data subject's consent. The GDPR requires that consent be:

Freely given, specific, and informed.

Unambiguous and take the form of an affirmative action or statement.

Explicit for certain types of data processing, including, but not limited to, sensitive personal data processing and cross-border data transfers.

Presented in a manner clearly distinguishable from other matters, in an intelligible and easily accessible form.

Provided in clear and plain language.

When the data controller collects personal data from a child under the age of 16, Article 8 requires the data controller to:

Obtain consent from the child's parent.

Take reasonable steps to verify that the parent consented.

Member states may lower this age requirement, provided the revised age requirement does not fall below 13 years.

Maintain a Method of Obtaining Valid Data Subject Consent

Documentation to help demonstrate compliance with the GDPR's requirements for valid consent includes, but is not limited to:

Policies and procedures for obtaining consent that comply with the GDPR's requirements for valid consent. For more information on valid consent under the GDPR.

Policies and procedures on obtaining and verifying parental consent.

Copies of dated privacy notices which satisfy the various notification requirements established in Articles 12, 13, and 14 of the GDPR and that notify of the right to withdraw consent when the data controller bases processing on consent. For more on the GDPR's privacy notice content requirements.

Archives of past, publicly posted privacy notices, along with their effective dates.

Copies of compliant consent forms, including written and web-based forms that use check boxes, buttons, or other methods to obtain consent.

Copies of signed and dated written and electronic consent forms.

Policies and procedures to respond to a data subject's withdrawal of consent. For more information on complying with data subject rights.

Policies and procedures to ensure that personal data is only used in accordance with the consent obtained.

Policies and procedures on using personal data for secondary purposes different than the purposes originally notified to the data subject.

Policies and procedures on obtaining consent for secondary use purposes.

A record of any consents obtained for secondary use purposes.

Processing Special Categories of Personal Data

The GDPR prohibits processing special categories of personal data unless a lawful justification for processing applies. Special categories of personal data include:

Racial or ethnic origin.

Political opinions.

Religious or philosophical beliefs.

Trade union membership.

Genetic data.

Biometric data.

Data concerning health or sex life.

Sexual orientation.

(Article 9(1), GDPR.)

The prohibition on processing special categories of personal data does not apply when:

The data subject consents to the processing.

The processing is necessary for:

carrying out the data controller's rights in the field of employment law, social security, and social protection;

protecting the vital interests of the data subject when the data controller cannot obtain consent;

establishing, exercising, or defending legal claims;

reasons of substantial public interest;

purposes of preventive or occupational medicine to assess the working capacity of a data subject, medical diagnosis, or for the provision of health or social care or treatment;

reasons of public interest in the area of public health;

archiving in the public interest; or

scientific, historical research, or statistical purposes.

The processing relates to the legitimate activities of certain non-profit organizations.

The processing relates to personal data made public by the data subject.

(Article 9(2), GDPR.)

The GDPR also limits the processing of personal data relating to criminal convictions and offenses to certain circumstances, including when applicable law authorizes the processing and provides for appropriate safeguards for the rights and freedoms of data subjects (Article 10, GDPR). For more on processing special categories of personal data.

Document Procedures for Processing Special Categories of Personal Data

Documentation to help demonstrate compliance with the requirements relating to processing special categories of personal data includes, but is not limited to:

Documentation specifying the grounds for processing special categories of personal data through data protection impact assessments or other mechanisms, including evidence of the analysis used to determine the processing's lawful basis.

Policies and procedures on the collection and use of special categories of personal data.

Copies of privacy notices that comply with Articles 12, 13, and 14.

Policies and procedures for obtaining valid consent under the GDPR.

Copies of compliant consent forms.

Copies of signed consent forms that demonstrate explicit consent to process special categories of personal data.

Policies and procedures to ensure that personal data is only used in accordance with the consent obtained.

Policies and procedures to respond to a data subject's withdrawal of consent.

Data Subject Rights

The GDPR provides data subjects with several rights, including, but not limited to the right to:

Receive a privacy notice containing certain information about the processing activities (Articles 12 to 14, GDPR).

Confirm whether the data controller processes personal data about the data subject and the right to access the personal data processed and obtain certain information about the processing activities (Article 15, GDPR).

Correct inaccurate personal data (Article 16, GDPR).

Have personal data erased under certain circumstances (Article 17, GDPR).

Restrict the processing of personal data under certain circumstances (Article 18, GDPR).

Receive a copy of the personal data the data controller holds under certain circumstances and transfer the personal data to another data controller (Article 20, GDPR).

Object to processing under Article 21 that is:

done for the performance of a task in the public interest under Article 6(1)(e) (Article 21(1), GDPR);

done for the purposes of the data controller or a third party pursuing its legitimate interests under Article 6(1)(f) (Article 21(1), GDPR);

for direct marketing purposes (Article 21(3), GDPR); or

done for scientific or historical research purposes or statistical purposes under certain circumstances (Article 21(6), GDPR).

Not be subject to a decision based solely on automated data processing, including profiling, where the

decision has a legal or other significant affect, subject to certain limited exceptions, including:

where the data subject explicitly consents;

where the automated data processing and decision-making is necessary for the performance of a contract with the data subject; or

where an applicable law that also requires measures to protect data subjects' rights authorizes the automated data processing and decision-making.

(Article 22(2), GDPR.)

The data controller also must notify each recipient of personal data, for example, third-party data processors, of any correction or erasure requests or restrictions on processing so that the third party can carry out the request (Article 19, GDPR).

EU member states can create additional restrictions on the scope of data subject rights and impose additional obligations on data controllers if they comply with the provisions of Article 23 (Restrictions) of the GDPR. For more information.

Documentation Demonstrating Compliance with Data Subject Rights

Documentation to help demonstrate compliance with data subject rights includes, but is not limited to:

Copies of privacy notices that comply with Articles 12 (Transparent information, communication and modalities for the exercise of the rights of the data subject), 13 (Information to be provided where personal data are collected from the data subject), and 14 (Information to be provided where personal data have not been obtained from the data subject).

Policies and procedures on responding to data subject access and other requests in a timely and appropriate manner in compliance with Chapter III of the GDPR (Rights of the Data Subject). Policies and procedures should ensure, among other things, that:

communications with the data subject are concise, transparent, intelligible, easily accessible, and in clear and plain language;

the data controller provides information to the data subject on any action taken in response to a request within one month of receiving the request, unless the data controller extends the period to respond under Article 12(3); and

when the data controller does not act in response to a data subject request, the data controller notifies the data subject within one month of receiving the request of the reasons why.

Response letters or response forms to access and other types of requests. For standard data controller response letters.

Forms to collect additional information where necessary for preparing data subject request responses

Evidence of a mechanism provided to data subjects for updating or correcting their personal data.

An inventory or log for recording data subject requests and for tracking responses

Guidance on assessing requests to object to or restrict data processing under Articles 18 and 21 and requests for erasure under Article 17 of the GDPR.

Procedures to ensure that personal data are used only in accordance with any objections to or restrictions on processing.

Policies and procedures on the use of automated decision making including when use is acceptable.

Procedures for reviewing data processing conducted wholly or partially by automated means to ensure compliance with Article 22 of the GDPR.

A data inventory identifying automated data processing and the legal justification for the processing.

For automated data processing, procedures allowing the data subject to:

obtain human intervention by the data controller in the decision-making process;

express a point of view on any decision made through automated processing; and

contest the decision.

Data Transfers

Data controllers and data processors transferring personal data outside of the EU must comply with certain requirements for data transfers established in Chapter V of the GDPR (Transfer of Personal Data to Third Countries or International Organisations). Data controllers and data processors can base transfers outside of the EU on any of the following:

A determination by the European Commission that the recipient country provides an adequate level of protection (Article 45, GDPR).

Where the data controller or data processor provides appropriate safeguards, and provided data subjects can enforce their legal rights and have effective legal remedies (Article 46, GDPR). Data controllers and data processors can provide appropriate safeguards, without the approval of a supervisory authority, through:

a legally binding and enforceable instrument between public authorities or bodies;

binding corporate rules (Article 47, GDPR)

standard data protection clauses adopted by the European Commission;

standard data protection clauses adopted by a supervisory authority and approved by the European Commission;

an approved code of conduct under Article 40, together with the recipient data controller's or data processor's commitment to apply appropriate safeguards; or

an approved certification program under Article 42, together with the recipient data controller's or data processor's commitment to apply appropriate safeguards.

(Article 46(2), GDPR.)

Data controllers and data processors can also provide appropriate safeguards, with approval from the supervisory authority, through:

contractual clauses between the data controller or data processor and the data controller, data processor, or recipient in the non-EU country; or

provisions inserted into administrative arrangements between public authorities or bodies that include enforceable data subject rights.

(Article 46(3), GDPR.)

In the absence of an adequacy decision or appropriate safeguards, Article 49 permits the cross-border transfer of personal data when the data subject explicitly consents.

Article 49 also permits the cross-border transfer of personal data in the absence of an adequacy decision or appropriate safeguards when the transfer is necessary for:

the performance of a contract;

important reasons of public interest;

the establishment, exercise, or defense of legal claims;

protecting the vital interests of the data subject and the data subject is incapable of giving consent; or

under limited circumstances, pursuing the legitimate interests of the data controller and the data subject's interests or rights and freedoms do not override those legitimate interests.

(Article 49(1), GDPR.)

Implement and Document Compliant Data Transfer Mechanisms

Documentation to help demonstrate compliance with the GDPR's cross-border transfer requirements includes, but is not limited to:

A data inventory of processing activities identifying cross-border data transfers and the specific transfer mechanism relied on for each transfer.

Identification of any specific adequacy decision relied on to support the transfer.

Copies of valid consent forms relied on to support the transfer. The forms must include information on the possible transfer related privacy risks from the absence of an adequacy decision or appropriate safeguards. For more on consent under the GDPR.

When relying on other derogations under Article 49 besides consent:

identification of the specific transfer basis, such as to perform a contract or for the establishment, exercise, or defense of legal claims; or

a record of the assessment balancing the data controller's legitimate interests against the data subject's rights and freedoms.

When relying on other appropriate safeguards:

documentation of compliance with the EU-US Privacy Shield Framework for transfers from the EU to the US and the Swiss-US Privacy Shield Framework for transfers from Switzerland to the US (for more on the EU-US and Swiss-US Privacy Shield Frameworks

approved binding corporate rules and related documentation

data transfer agreements incorporating standard data protection clauses

documentation of compliance with an approved code of conduct or certification program; or

documented approval from the relevant supervisory authority.

Joint Controllers

The GDPR specifies that two or more data controllers that jointly determine the purposes and means of data processing are considered joint controllers (Article 26, GDPR). Joint controllers must:

Determine which data controller is responsible for certain obligations under the GDPR.

Specify their duties by an arrangement which should:

include a point of contact for data subjects;

reflect the data controllers' roles vis-à-vis the data subjects;

be made available to data subjects; and

allow data subjects to exercise their rights against each of the data controllers.

Document Arrangements with Joint Controllers

Documentation to help demonstrate compliance with Article 26 (Joint controllers) includes, but is not limited to:

Details of the arrangement between joint controllers specifying each data controller's obligations.

A privacy notice that includes details on the joint controller relationship and a contact point for data subjects.

Policies and procedures on responding to data subject access or other requests.

Data Processors

Article 28 of the GDPR establishes specific obligations and requirements for engaging data processors. It only permits transfers to data processors when the data processor provides sufficient guarantees that it has implemented appropriate technical and organizational measures to protect personal data in accordance with the GDPR.

Data processor relationships must be governed by a contract or other legal act under applicable law that binds the data processor. Article 28(2) states that the data processor must have written authorization from the data controller before engaging another data processor. Also, Article 28(3) specifies certain terms that a data controller should include in any contracts with data processors.

For more on engaging data processors and data processor obligations under the GDPR.

Implement Procedures for Engaging Data Processors

Documentation to help demonstrate compliance with Article 28 (Processors) includes, but is not limited to:

Policies and procedures for conducting due diligence on potential data processors, including screening questionnaires.

Completed due diligence reports or data processor risk assessments.

Data protection requirements for data processors.

Policies and procedures for engaging data processors and executing contracts.

Privacy and security clauses for insertion into data processor contracts.

Executed contracts with third parties that comply with Article 28 or include standard contractual clauses approved by the European Commission or other supervisory authority.

Evidence of the data processor's adherence to an approved code of conduct referred to in Article 40. For more information on approved codes of conduct.

Using Testing and Auditing to Demonstrate Compliance

Organizations must do more than implement internal policies and procedures that comply with the GDPR's requirements. Organizations must also:

Ensure that mechanisms put the policies and procedures into effect in the day-to-day activities of the organization.

Implement recurring means, such as testing and audits, to measure the effectiveness of the mechanisms and privacy measures.

Maintain evidence of regular testing of privacy measures and an evaluation of those measures.

Be able to prove to the relevant data protection authority through audit results and other metrics that it meets its obligations under the GDPR and that data processing complies with the GDPR's requirements.

Accountability for Data Processors

The accountability principle under Articles 5 and 24 expressly applies to data controllers. However, in practice, the GDPR obligations imposed directly on data processors or indirectly passed on by the data controller also subject processors to certain accountability requirements. These obligations include, but are not limited to, an obligation to:

Process personal data only according to the data controller's instructions under Article 29.

Maintain a record of data processing activities that complies with Article 30(2).

Appoint a data protection officer under certain circumstances as specified in Article 37.

Implement appropriate technical and organizational measures in compliance with Article 32.

Have written data controller authorization before engaging subcontractors under Article 28(2) and pass obligations down to any data processors it engages via contract as specified in Article 28(4).

Notify the data controller of any security breach without undue delay in accordance with Article 33(2).

Appoint an EU representative when the data processor is not located in the EU, subject to certain limited exceptions under Article 27.

Only transfer personal data internationally in accordance with Article 44, which requires the data processor to have a compliant data transfer mechanism.

Make available to the data controller all information for the data controller to demonstrate compliance with its obligations under Article 28 (Processors), as set out in Article 28(3)(h).

Data processors can demonstrate compliance with these obligations by taking the same steps and maintaining the same types of documentation as data controllers. Data processors may also rely on codes of conduct and certification programs to demonstrate compliance with certain obligations.

Reducing Liability by Demonstrating Compliance

A data controller or data processor's ability to present evidence to regulators of its efforts to comply with the requirements of the GDPR may help reduce liability under Article 83 (General conditions for imposing administrative fines). In considering whether to impose an administrative fine and the amount of the fine, the GDPR instructs supervisory authorities to consider, among other factors:

The infringement's intentional or negligent character.

The controller's or processor's degree of responsibility when considering their implementation of technical and organizational measures under the Articles requiring data protection by design and by default (Article 25) and secure processing (Article 32).

(Article 83(2), GDPR.)

If a data controller or data processor demonstrates, for example, that it did not act intentionally in violating the GDPR and that it implemented technical and organizational measures appropriate to the risk, a supervisory authority may consider this in deciding whether to impose a fine, or it may reduce the fine imposed.

In addition, Article 82(3) (Right to compensation and liability) states that a data controller or data processor is exempt from liability if it proves that it was not responsible for the event resulting in damage.