Morgan Lewis | White Paper

THE eDATA GUIDE TO THE GDPR

May 2018

www.morganlewis.com

With the General Data Protection Regulation (GDPR),[1] the European Union has taken a significant step to strengthen the fundamental rights of its citizens in the digital age.

Designed to replace the 1995 EU Data Protection Directive (DPD), the GDPR will go into effect on May 25, 2018, ushering in an era of increased protection and control for individuals, as well as standardized regulations—and penalties—for impacted organizations. The GDPR seeks to enhance and enforce EU citizens' right to privacy while harmonizing and simplifying data privacy rules to help facilitate commerce. Generally speaking, the GDPR has increased scope compared to the DPD, extending its reach to organizations beyond the EU's borders.

Knowing what the GDPR requires and how to satisfy its obligations will be crucial for the smooth operation of any business selling goods or services to data subjects in the countries bound together by the EU.

WHO IS SUBJECT TO THE GDPR?

One of the key changes to EU privacy law brought by the GDPR is its expanded territorial scope. According to Article 3 of the GDPR, **an organization is subject to regulation any time it processes personal data of an individual residing in the EU**.

Organizations handling personal data belonging to EU data subjects are in most cases either **data controllers** or **data processors**. Under the GDPR, liability now extends to data processors—not just controllers as was the case under the DPD.

Data Controllers[2]

A data controller is an entity that determines the purpose and means of processing data.[3] Data controllers are charged with implementing privacy by design, including the integration of effective technical and organizational measures to meet GDPR requirements and protect the rights of data subjects. Most organizations with personnel and customers are data controllers.

Data Processors[4]

Typically, a data processor is an entity that is responsible for obtaining, recording, holding, or carrying out any operation or set of operations on data on behalf of a data controller. Organizations that store, process, and manage data for a data controller (e.g., payroll companies, tax advisors, and cloud-based service providers) are data processors.

Organizations Outside the EU

Two activities under the GDPR apply to organizations outside the EU—offering goods and services or analyzing specific people or behavior (e.g., tracking movement). Although extraterritorial application will most likely affect all organizations doing business with any customers resident in the EU, it can be tricky for international organizations to determine what constitutes the offering of goods and services in the EU. Instructive for such organizations are answers to some basic questions:

- Do you interact with customers in local languages?

[1] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

[2] Articles 24–27.

[3] United Kingdom Information Commissioner's Office (ICO)

[4] Articles 28–30.

- Can customers pay for your products or services in euros?
- Does your website have a local top-level domain such as .de?
- Does your website feature EU customer testimonials about your products or services?

Organizations should take care not to construe the requirement to offer goods or services too narrowly. As the GDPR is EU law, it will be interpreted by the EU courts in a purposeful rather than a literal manner and with regard to the objectives of the GDPR to ensure high standards of data protection for data subjects.

That said, some commentators have noted that companies with only minimal or incidental EU contacts should pay close attention to GDPR compliance, but also be aware that EU authorities have limited ability to act against organizations with no presence or assets in the EU, as exercising the long arm of EU law beyond EU borders could prove quite cumbersome.

GENERAL PRINCIPLES

In many ways, the GDPR takes the principles established in 1995 by the EU Data Protection Directive and strengthens them, including in the areas of transparency, limitation of scope (collection, use, and storage time), security, and accuracy. The GDPR also adds some new elements to data privacy law, including a more robust accountability requirement.

The GDPR establishes principles to address the following areas:

- Processing of personal data
- Lawfulness of processing
- Conditions for consent
- Conditions applicable to child consent in relation to information society services
- Processing of special categories of "sensitive" personal data (race, ethnicity, political leanings, religion, trade union membership, health data, biometric data, and sex life)
- Processing of personal data related to criminal convictions
- Processing that does not require identification

The requirement for a lawful basis for processing data existed prior to the enactment of the GDPR. However, the GDPR places greater importance on accountability and transparency. Seven guidelines are helpful in establishing the proper conditions for processing personal data in compliance with the GDPR:

1. Personal data must be processed lawfully, fairly, and transparently

Data controllers and processors must determine the lawful basis before any processing can begin. Scenarios that form a lawful basis for processing include the following:

- **Consent**: The data subject has given the data controller and processor clear consent to process personal data for an identified purpose.
- **Contract**: Processing is required for a contract between the processor/controller and the data subject, or because the data subject has asked for specific steps to be taken prior to entering the contract.
- **Legal obligation**: Processing is required to comply with a law (this excludes contractual obligations).
- **Vital interests**: Processing is required to protect a person's life.

- **Public task**: Processing is needed for data processor/controller to undertake a task in the public interest, or the controller is exercising its public authority.
- **Legitimate interests**: Processing is needed for a legitimate interest of the data controller or a third party.

Here is a partial list of information that must be given to data subjects as part of a privacy notice when their data is collected[5]:

- Identity and contact information of your organization
- Purpose for which your organization intends to use the data
- Legal justification for processing
- Length of time the data will be preserved
- Identity of potential recipients
- Any potential for the data to be transferred to a party outside the EU
- Right of the data subject to lodge a complaint with a Data Protection Authority
- Right of the data subject to withdraw consent at any time

It is advisable to document the lawful basis and include it in your privacy notice, if applicable. Please note, under the GDPR, it is difficult to change an existing lawful basis for processing, so it is best to make an effort to identify the correct basis the first time around.

The standard for consent has been heightened under the GDPR. Data subjects must have a genuine choice and control when being asked for consent. Data subjects should opt-in with a clear and specific statement; consent cannot be by default. Consent requests should be distinct and kept away from other terms and conditions. Whenever possible, provision of a service should not depend on consent to process data. According to the Article 29 Working Party[6] Guidelines on Consent under Regulation 2016/679 (WP 29 Consent Guidelines), "if consent is bundled up as a non-negotiable part of terms and conditions it is presumed not to have been freely given."

The WP 29 Consent Guidelines suggest that, at a minimum, the following should be provided to a data subject when informed consent is sought:

- Controller's identity (if further transfer to additional controllers is anticipated, those controllers also should be named)
- Purpose of each of the processing operations for which consent is sought
- Type of data that will be collected and used
- Existence of the right to withdraw consent
- Information about the use of the data for decisions based solely on automated processing, including profiling such as targeted advertising, in accordance with Article 22(2)[7]

[5] For a full list of information requirements, see Chapter III, Section 2, Article 13 of the GDPR.

[6] The Article 29 Working Party was defined by the original DPD and tasked with interpreting various elements of the directive. It will be known as the European Data Protection Board (EDPB) under GDPR but serve a similar function.

[7] Article 22(2) states that if the automatic determination is necessary for the entering or performance of a contract with the data subject, is controlled by appropriate member state–defined guidelines, or is permitted through explicit consent, the right not to be subject to these types of decisions shall not apply.

- If the consent relates to transfers, the possible risks of data transfers to third countries in the absence of an adequacy decision (this includes the United States), and appropriate safeguards

Consent requests should name any third-party controllers that will rely on the consent, and withdrawal of consent should be easy and without detriment. Finally, consents should be reviewed regularly to ensure that the stated basis and purposes have not changed. If consent is too difficult to achieve, look to one of the other lawful bases.[8]

2. Lawful processing requires a specific purpose

Purpose limitation is a core principle of the GDPR. As such, the privacy notice should include the purpose of the processing. Should that purpose change over time, you may be able to continue processing under the original lawful basis if the new purpose is compatible with the original. However, collected data cannot be used for anything other than the stated purpose.

3. Minimize personal data collected so that you collect only the personal data necessary to fulfill the purpose (data minimization)

If a need for personal data to be transferred outside the EU has been established, it is critical to design safeguards around the use of that data, including data minimization. Through data minimization, data controllers and processors limit the amount of personal data collected and transferred. Redactions, search terms, and data restrictions are effective data minimization tools to consider.

At the point of collection, only data that is necessary should be collected. However, even after data is collected, data controllers and processors should regularly reevaluate whether it is necessary to continue storing or processing each piece of datum. In some instances, data can be pseudonymized. If used, for example, for market analysis purposes, the data need not be linked to information that makes it possible to identify a particular person. Data controller and processor employees should be trained in how to practice data minimization in their day-to-day operations. Only those specific employees with a need to access the personal data should be allowed access, and that access should end when the specific purpose is achieved.

Periodic audits or exercises are a good way to remind employees of the need to delete data that is no longer needed. Further, data controllers and processors should contractually obligate their third-party vendors to process data in compliance with the principle of data minimization, including disclosure to the controller or processor of any practices that involve indefinite storage or duplication of personal data provided to them. The implementation and execution of record retention policies is a critical piece in achieving this goal.

4. Collected data must be accurate and up to date, and if not, it must be corrected

Any inaccuracies must be corrected or removed promptly. Data controllers and processors should build into their systems mechanisms for maintaining the accuracy of data and allowing data subjects to request correction. Controllers and processors should make verification easy for data subjects. One way to achieve this is by reminding data subjects to verify their personal details when they log into the data controller's website. Data subjects who do not come into regular contact with the data controller or processor's website can be segmented based on risk: Focus first on achieving accuracy for data subjects

[8] For additional information about consent requirements under the GDPR, please see the Article 29 Data Protection Working Party Guidelines on Consent under Regulation 2016/679 (November 28, 2017).

who are active clients, next on inactive clients with occasional activity within the past year, and finally on legacy data subjects with no interaction in the past year. When a request to correct data is received, it is good practice to note on the system that the data subject has challenged the accuracy of the data, and the reason for the challenge.

5. Data should not be used beyond its original purpose

If a processor or controller seeks an additional use for collected data beyond what was stated at collection, a new legitimate basis for processing must be obtained. Data subjects must be informed of the specific purpose for which their data is being processed.[9] If data has been collected on the basis of a legitimate interest, a contract, or a vital interest, it can be used for another purpose, taking into consideration the link between the original purpose and the new/upcoming purpose. If data has been collected on the basis of consent or pursuant to a legal requirement, no further processing is permitted absent new consent or a new legal basis.

6. Store personal data for no longer than necessary for the purpose it was collected

Data controllers and processors should establish procedures for destroying data once it is no longer needed for its intended purpose. The amount of data collected should be adequate, relevant, and limited to what is necessary for the purpose, pursuant to the principle of data minimization. Data should be kept for the shortest time possible, taking into account the reason the data was processed and any legal requirements to preserve the data.

7. Install appropriate safeguards to ensure security and confidentiality of data

European privacy legislation has always required data controllers to take adequate security measures to ensure the confidentiality and integrity of data. The GDPR goes a step further and specifically recommends pseudonymization and encryption of data as two possible mechanisms to ensure that data remains secure and confidential. Data controllers and processors should take a risk-based approach to security, assessing the risk that an individual's privacy will be compromised and the ensuing harm that could be caused to that individual.

The specific security safeguards used by a data controller or processor can vary according to the data type and risk. Rather than try to list all the specific security tools, the GDPR requires that data controllers and processors take into account "the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms" of data subjects when implementing appropriate technical and organizational security measures.[10] Data controllers and processors should consider various types of encryption, password requirements, and backup procedures to ensure a level of security appropriate to the risk. We can expect additional guidance from trade and data security organizations to provide additional clarity on specific safeguards appropriate to GDPR compliance.

The GDPR requires that data protection principles be considered at the product and system development stage—well before any personal data is actually processed. This is addressed by the GDPR's Data Protection by Design and Default[11] model, which is closely related to the concept of Privacy by Design. Thinking about data protection principles at the development stage is necessary to better ensure that personal data is protected throughout its life cycle.

---

[9] Article 29 Working Party Opinion 03/2013 on purpose limitation.

[10] Article 32(1).

[11] Article 25.

RIGHTS OF THE DATA SUBJECT

Under the GDPR, all EU citizens now have privacy rights that previously existed piecemeal only in some EU countries, such as the right to be forgotten (right of erasure). The GDPR contains new rights as well, including the right to data portability, which allows data subjects to demand access to their data in an easily accessible format. These newly enumerated rights include the following:

Right to Be Informed

Data controllers must provide clear, concise, and more specific information to data subjects about what is done with their personal data, compared to requirements under the DPD. Information must be proactively provided in an easy-to-access and understandable way. Methods for providing privacy information include the following:

- Dashboards that help people manage how their data is used
- Just-in-time notices that deliver targeted privacy information at the time of collection
- Icons—small but prominent symbols indicating that a particular type of processing is occurring
- Mobile phone pop-ups and voice alerts

It can be effective to combine several of the above approaches. Additionally, it is recommended that data controllers place privacy information on their websites and make individuals aware that the information is there. At least some privacy information must be provided at the time personal data is obtained. A data map can provide a great resource to help a data controller understand what personal data it has, and where.[12]

Right of Access

Data subjects have the right to access their personal data and supplementary information free of charge (in most cases) so that they are aware and able to verify the lawfulness of data processing.[13] Requests that are manifestly unfounded or excessively repetitive can be partially or wholly refused (depending on the circumstances), but the requestor must be given an explanation in compliance with the GDPR requirements. The GDPR recommends, as a best practice, that privacy information be provided to data subjects via a secure network allowing the data subjects direct access to their private information.[14]

Right to Rectification

This is the right to have inaccurate or incomplete personal data corrected or completed. Even though a data controller may have taken earlier steps to ensure accuracy, the right to rectification requires a reevaluation of accuracy upon a data subject's request. The more important the information being corrected is, the greater the effort required on the part of the data controller. When data is corrected, the corrections must be communicated to each recipient (including data processors) when possible.[15]

[12] Articles 12–14 and Recitals 58 and 60–62.

[13] Recital 63.

[14] Articles 12 and 15 and Recital 63.

[15] Articles 5, 12, 16, and 19.

Right to Erasure

The right to erasure, or right to be forgotten, gives data subjects the right to request that their data be erased.[16] The right of erasure can apply when

- personal data is no longer needed for its original purpose;
- the data subject withdraws consent, and there is no other lawful basis for processing;
- the data subject objects to the legitimate interest that forms the basis for processing, and there is no other legitimate interest to do so; or
- the data has been processed unlawfully.

The right to erasure does not apply when processing is necessary for any of the following:

- Exercise of the right of freedom of expression
- Compliance with a legal obligation
- Performance of a task carried out in the public interest such as in the areas of preventive medicine or public health
- Archiving in the public interest
- Establishment or defense of a legal claim[17]

Right to Restrict Processing

Data subjects have the right to restrict or suppress the processing of their personal data in limited circumstances, including the following:[18]

- Data controller is verifying the accuracy of personal data after the data subject contests the accuracy of his/her personal data
- Data has been unlawfully processed
- Data processor or controller no longer needs the personal information but the data subject wants the data to continue to be preserved for a legal claim
- Data subject has objected to processing of his/her data under Article 21(1)[19] and the data controller is determining whose interests prevail[20]

Right to Data Portability

The right to data portability allows data subjects to retrieve and reuse their personal data for their own purposes across different platforms. This portability allows data subjects to control who uses their data and where it is used, and to choose the best application for this. If the data subject wishes to use a different service or application, the data requested should be easily transferrable to the preferred controller or processor.

The information must be provided in a machine-readable, commonly used format. The right of data portability applies only when the lawful basis for processing is consent or for the performance of a

[16] Article 17.

[17] Articles 6, 9, 12, and 17, and Recitals 65 and 66.

[18] Article 18.

[19] Article 21(1) defines the right of data subjects to object to the use of private information, as illustrated further in this document.

[20] Articles 18 and 19, and Recital 67.

contract, and the processing is electronic, not paper. The right of portability refers only to data provided by the data subject (e.g., gender, name, web usage, location data) and does not apply to data the controller or processor created about the data subject (e.g., a user profile based on the provided data).[21]

Right to Object

Data subjects have the right to object to processing based on legitimate interests or for the purpose of carrying out a task in the public interest, as well as for direct marketing or processing for scientific research. If a data subject objects to processing, data controllers and processors using data for performance of a legal task or the data controller's legitimate interest must stop processing the data absent a demonstration of compelling, legitimate grounds for processing that outweigh the interests of the data subject or show that the processing is for the establishment or defense of a legal claim. Data subjects must be informed of their right to object in initial communications and in the data controller's privacy notice.[22]

SECURITY AND BREACH

Security of Processing

Complying with the GDPR will require the adoption of policies and technical measures to ensure that data is protected and that organizations are able to cope with data breaches. The GDPR calls for data controllers and processers to embrace "the principles of data protection by design and data protection by default."

Controllers and processers should consider the right to data protection as they design systems that process personal data. Such systems should integrate the latest reliable technology and use multiple methods of protecting personal data. If a data breach occurs, protocols should be in place to communicate the breach to the necessary parties and to take steps to minimize its impact.[23]

The data controller and processor must have security measures in place to match the risk to the data subject. The more sensitive the personal data, the greater the security and organizational measures should be. Controllers and processors should conduct an assessment to determine the level of security needed prior to designing a processing system that accounts for the risks that processing may create. The assessment should consider the risks of accidental or unlawful destruction or alteration, unauthorized disclosure, or access to personal data.

Measures that may be taken to ensure the proper level of security include the following:

- Minimize the personal data to be processed
- Pseudonymize personal data
- Encrypt personal data
- Create processes/systems to ensure the ability to preserve the ongoing confidentiality, integrity, availability, and resilience of systems
- Create processes/systems to ensure the ability to restore data in a timely manner in case of incident
- Establish processes for testing security measures

[21] Articles 13 and 20, and Recital 68.

[22] Articles 12 and 21, and Recitals 69 and 70.

[23] Article 25.

- Ensure that natural persons with access to personal data do so only upon instruction from the controller[24]
- Create and adhere to a code of compliance[25] and gain certification according to the mechanism described in Article 42[26]

Data Protection Impact Assessment and Prior Consultation

If processing is likely to be high risk, the controller must conduct a data protection impact assessment (DPIA).[27] Factors that should be considered when determining whether processing is high risk and a DPIA required include the following:

- Processing involves evaluation or scoring (e.g., screening against a credit reference database)
- Automated decisionmaking will occur that has legal-like effect
- Systematic monitoring is in place (e.g., CCTV)
- Sensitive data or data of a highly personal nature (e.g., ethnicity, sexual orientation) is stored
- Data is to be processed on a large scale (large number of subjects or great volume)
- Processing matches or combines datasets
- Data concerns vulnerable data subjects (e.g., children or employees)
- Processing involves innovative use or application of new technological or organizational solutions
- Processing in itself "prevents data subjects from exercising a right or using a service or a contract"[28]

In addition, compliance with Article 40 code of conduct and other corporate rules must be taken into account when assessing the impact of processing. The Article 29 Working Party considers any combination of at least two of the above factors to be high risk, however, any one factor can constitute high risk. If a controller determines that high-risk processing cannot be mitigated, it must consult with the applicable supervisory authority (see Supervision and Authority below for more on supervisory authorities).

When creating a DPIA, a controller should seek out the advice of the data protection officer (the DPO's role is described further below), and if the processing is to be at least partly performed by a data processor, the processor should assist.[29] The controller also should seek the views of data subjects or their representatives regarding the intended processing. If the controller's decision differs from the views of the data subjects, it must document the reason. Similarly, if the controller does not seek the views of data subjects, it should also document the reasons for that decision.

---

[24] Article 32.

[25] Article 40.

[26] Article 42 provides details for certification by member states of a controller's or processor's compliance program, including affixing seals and labels to the documentation as well as keeping central logging of such certificates.

[27] Article 35.

[28] Recital 75.

[29] Article 36.

A DPIA is required to contain the following:

- Systematic description of the envisaged processing operations
- Description of the purposes for processing
- Assessment of the necessity and proportionality of the processing operations in relation to the purposes
- Assessment of the risks to the rights and freedoms of data subjects
- Measures envisaged to address the risks and to demonstrate compliance

The controller should periodically conduct a review to assess if processing is being performed in accordance with the DPIA, at least as often as when there is a change of the risk represented by processing operations.

Breach Notifications

If a personal data breach occurs, the controller or processer is required to notify the applicable supervisory authority in less than 72 hours unless it is "unlikely to result in a risk to the rights and freedoms of natural persons."[30] A processor, however, should always notify the controller. All breaches should be documented and include the details of the breach, its effect, and remedial actions taken. In cases where a supervisory authority is notified, additional information should include the following:

- Description of the nature of the personal data breach, including information about the number of people and records concerned
- Name and contact details of the data protection officer or other contact
- Likely consequences of the breach
- Description of the measures taken or proposed to be taken by the controller to address and mitigate the breach

In the event of a breach that is likely to result in high risk and impact natural persons, the controller must inform the affected data subject(s) without undue delay. The nature of the breach, steps taken, and potential consequences must be described in clear and plain language. However, this communication is not needed if any of the following exist:

- Controller has implemented appropriate protection measures—in particular, encryption of the data
- Controller has taken steps to ensure that the risk is unlikely to materialize
- Too much effort would be required to send individually, in which case the controller should use a public communication of equal effectiveness

If a breach has not been communicated to a data subject, and the supervisory authority has determined that the risk is high, the authority may require the controller to do so, absent one of the exceptions above. As such, data controllers and processors, as a part of their data security protocols, should establish mechanisms for prompt notification of the necessary parties. They also should attempt to identify, and integrate into their procedures, situations that would be potential exceptions to the need for notification.

[30] Article 33.

Role of the Data Protection Officer

A DPO is designated by a controller or processor to be responsible for data protection procedures and measures to ensure compliance with GDPR and other regulations. The controller and processer must appoint a DPO in the following circumstances:

- Processing is carried out by a public authority, except for courts or independent judicial authorities when acting in their judicial capacity
- Core activities of the controller or processor consist of processing operations that require regular and systematic monitoring of data subjects on a large scale
- Core activities of the controller or processor consist of processing on a large scale of sensitive data or data of a highly personal nature, or personal data relating to criminal background information[31]

In other cases, the controller or processor (or associations and other bodies representing categories of controllers or processors) may be required by EU or EU member state law to designate a DPO. They also may appoint one voluntarily. The DPO must possess the proper professional qualifications, in particular, expert knowledge of data protection laws and practices. The contact information of the DPO must be published and communicated to the applicable supervisory authority.

The DPO should be involved in all issues that relate to the protection of personal data.[32] The controller and processor should provide the resources necessary for the DPO to carry out his/her tasks, allow access to personal data and processing operations, and help the DPO maintain his/her expert knowledge. In addition, controllers or processors should take steps to ensure that the DPO remains independent. To remain independent, the DPO should not be instructed on how to perform his/her tasks, nor should the DPO be dismissed or penalized for performing such tasks. Additionally, the DPO should report directly to the highest management level, as an employee or contractor. DPOs may fulfill other tasks and duties as long as they do not result in a conflict of interest. The DPO shall be bound by secrecy or confidentiality concerning the performance of his/her tasks.

Provisions must be made to enable data subjects to contact the DPO on all issues related to the processing of their personal data and to the exercise of their rights under the GDPR.

The DPO's duties and tasks should be performed with due regard to the risks involved with processing operations. Those duties and tasks are the following:

- Inform and advise on data protection provisions
- Monitor compliance with GDPR and other privacy regulations and with the policies of the controller or processor
- Provide advice where requested about the DPIA, and monitor its performance
- Cooperate with the supervisory authority
- Act as the contact point for the supervisory authority on issues relating to processing

[31] Article 37.

[32] Article 38.

Codes of Conduct[33]

Associations and other bodies representing categories of controllers or processors may create codes of conduct to specify the application of the GDPR. The codes of conduct may contemplate such things as the legitimate interests of controllers, collection and pseudonymization of personal data, information provided to the public and to data subjects, and measures to ensure the security of processing, among others. The codes of conduct should be submitted to the supervisory authority for an opinion about whether they provide sufficient safeguards. Controllers and processors not subject to the GDPR may elect to adhere to these codes of conduct in order to provide the appropriate safeguards for data transfers to third countries, but when they do so, they should make binding and enforceable commitments to apply them. Independent expert bodies may be created to monitor codes of conduct created in this manner.

Certification

The GDPR encourages the creation of mechanisms to certify compliance with its regulations.[34] Such certifications would allow data subjects to quickly assess the level of data protection of relevant products and services provided by controllers or processers. Certification is voluntary. As with the codes of conduct, controllers and processers may obtain certification to demonstrate the existence of appropriate safeguards for data transfers to third countries, but when they do so, they should make binding and enforceable commitments to apply them.

DATA TRANSFERS

The expanded and more finely defined rights and protections pose a challenge for organizations facing the conflict of complying with the GDPR while attempting to use and move data outside the EU. If specific consent to transfer data out of the EU is unattainable, GDPR permits cross-border data transfers if any of the following are present:

- An adequacy decision by the European Commission (Commission) that either the country where data is to be transferred or the international organization (company) has adequate protections for the private information of EU data subjects. At present, the United States has not been deemed an adequate safeguarding territory.[35]
- Appropriate safeguards provided by the controller that proper protections are in place such as legally binding contracts and agreements with local authorities, approved codes of conduct, or other certifications.[36]
- Binding corporate rules outlining legal enforceability of the terms as well as the specified rights of the data subjects, which is approved by the appropriate supervisory authority. This generally covers transfers within an organization and with its agents or third parties.[37]
- International agreement such as the use of The Hague Convention for collection of information pursuant to litigation or an investigation.[38]
- Any of the following derogations as defined in Article 49:
  - Explicit consent where the individual is informed of the possible risks involved in the transfer

[33] Article 40.

[34] Article 42.

[35] Article 45.

[36] Article 46.

[37] Article 47.

[38] Article 48.

- Transfer is necessary for the performance of a contract between the data subject and the data controller
- Transfer is necessary when a contract is in the interest of the data subject
- In the event of an important public interest
- Transfer is necessary for the establishment, exercise, or defense of a legal claim[39]
- Transfer is necessary to protect a vital interest of the data subject where the subject is incapable of giving consent
- Transfer involves the registration of private information intended to provide public information

SUPERVISION AUTHORITY

A primary goal of the GDPR is consistent application and enforcement of privacy rights and regulations across the EU. This goal has dual benefits—strengthening the protection of EU citizens' fundamental right to privacy and lowering the transaction costs of doing business in the EU by having one set of privacy rules with which to comply. The GDPR sets up a regulatory structure for organizations seeking greater certainty on who will investigate certain privacy law issues, and where. Organizations doing business in the EU would be wise to review their data management policies and protocols with an eye toward determining where their privacy enforcement issues might be investigated.

Supervisory authorities, established under Articles 51–59 of the GDPR, are independent public bodies responsible for monitoring GDPR application and enforcing application consistency through cooperation with other supervisory authorities and the Commission. Data controllers and processors with operations in the EU will need to identify their lead supervisory authority. The decision a data controller makes about where to set up its "main establishment" (place of central administration) will determine which lead supervisory authority will handle that data controller's cross-border privacy issues. This construction appeals to multijurisdictional organizations because they need only interact with one regulator instead of multiple. As a result, data controllers would expect to face only one fine in an enforcement action, even if the activity being investigated involves multiple EU member states.[40]

The GDPR does not provide much guidance to data controllers and processors with main establishments outside the EU on how to determine their lead supervisory authority. The Article 29 Working Party suggests that there will be "complex situations where it is difficult to identify the main establishment or to determine where decisions about data processing are taken."[41] Data processors and controllers outside the EU should consider the following questions when trying to determine the location of their main establishment under the GDPR:

- Where are decisions about the purposes and means of the data processing given final signoff?
- Where are decisions about business activities that involve data processing made?

---

[39] The Article 29 Working Party recently issued guidance on the interpretation of the derogations (Guidelines on Article 49 of Regulation 2016/679, 6 February 2018). The guidance reminds the reader that the derogations are to be used for specific purposes and should be employed only "occasionally" and not be repetitive in nature. Litigation can be considered a specific act, but should a company seek to preserve or collect EU data indefinitely or in anticipation of general litigation, the derogation may not be in play. Specifically, as it relates to the defense of a legal claim, the guidance states that "data transfers for the purpose of formal pre-trial discovery procedures in civil litigation may fall under this derogation," which clears up some confusion as to whether this derogation would apply in this context.

[40] See https://broadcasting.house/eu-gpdr-lead-supervisory-authorities/ for a list of supervisory authorities current as of August 2017.

[41] "Guidelines for identifying a controller or processor's lead supervisory authority," Article 29 Data Protection Working Party, Revised and Adopted April 5, 2017.

- Where does the power to make decisions effectively lie?
- Where is the director (or directors) with overall management responsibility for the cross-border processing located?
- Where is the controller or processor registered as a company, if in a single territory?

Answering these questions may not necessarily produce a clear answer for data controllers or processors with minimal or no administrative activity in the EU, but they can serve as a helpful starting point.

Disputes between supervisory authorities are to be handled by the European Data Protection Board (EDPB), which is populated by supervisory authorities from across the EU. Article 4(22) of the GDPR introduces the concept of the "Supervisory Authority Concerned." The Supervisory Authority Concerned can be the supervisory authority

- in the member state of the data controller or processor,
- where data subjects affected by processing reside, or
- with which a complaint has been lodged.

Pursuant to Article 56 of the GDPR, concerned supervisory authorities may play a role in privacy investigations, e.g., if the lead supervisory authority declines to handle a case.

Additionally, the member states are advised to create rules regulating their individual supervisory authorities, with the expectation that the authority will operate in secrecy in order to protect the data they come in contact with in the course of their administration.[42] This "obligation of professional secrecy" covers all actions by the supervisory authority while requesting access to personal data from controllers or processors.

COOPERATION AMONG AUTHORITIES

Because the EU regulations will apply to individual EU member states and be enforced through local supervisory authorities, there is also a hierarchy of responsibility and expectation of cooperation outlined in the language of the GDPR. Should one authority need assistance from another member state's authority, it may request such, and the requesting party is expected to provide that assistance freely.[43] The lead authority will work as the coordinating authority should more than one state's authority be involved in an adjudication of violation. Each authority may have a different opinion, and therefore the lead authority will be tasked with harmonizing the opinions,[44] confirming with the EDPB, and notifying the complainant and the controller or processor of the decision. This process is designed to provide a more unified response from the EU cooperative than the previous regime, where different states would apply their own values to similar concepts—often with dissimilar results.

In the event the an allegedly violating controller or processor has operations in more than one member state, or the alleged violation impacts data subjects in various member states, the relevant supervisory authorities will work jointly in the investigation and in devising an opinion. The authorities will share

[42] Article 90.

[43] Article 61 states that the authorities shall work to a common goal, including sharing information, unless the requested authority feels it is not competent in the subject matter or if it believes its assistance in the investigation will somehow violate its local regulations.

[44] Article 60 sets forth specific timelines for completion of the coordination effort among the authorities. Objections from other authorities must be noticed within four weeks, and where the lead authority will follow an objection rather than its original opinion, it must revise the original draft and notify all cooperating authorities within two weeks.

resources where appropriate and act under the supervision of the local authority where they reside.[45] In the interest of consistency, the EDPB also will operate to reconcile the actions of each supervisory authority when issuing opinions.[46] However, to protect the rights of data subjects in an emergency situation, supervisory authorities are given the leeway to act in due haste to swiftly provide appropriate correction.[47]

PENALTIES

EU data subjects are empowered to make their complaints public regarding alleged violations of the GDPR. They have recourse for bringing complaints—including filing a complaint with the supervisory authority of their member state.[48] Pending the finding of the supervisory authority, the data subject may seek a judicial remedy either against the original alleged violator[49] or against the supervisory authority if it does not act within three months of the original complaint. The data subject also may seek judicial remedy if it does not agree with the finding of the supervisory authority, by appealing to the judicial court of the member state of either the controller/processor or the data subject.

Representation of data subjects in filing a complaint and/or exercising the right to judicial adjudication may be performed by nonprofit organizations that act in the public interest. These organizations also may lodge complaints on behalf of data subjects without being requested to do so if the organization believes that there has been an infringement of rights.[50] Individual data subject may be awarded damages by the member state courts in which they seek relief. If the action identifies that multiple controllers and/or processors have violated the GDPR, each may seek contribution from the other once an amount is paid.

Supervisory authorities may impose stricter penalties for noncompliance than have been available in the past. These fines can reach into the millions of euros based on specifically defined damage calculations. For the most serious violations—such as inappropriate transfers and violations of basic principles, including violation of a prior order of the supervisory authority—an organization may be fined up to 4% of its annual global turnover or 20 million euros ($23.8 million), whichever is higher. For lesser infractions such as poor recordkeeping or failure to appropriately notify authorities of data breaches, the fine can be up to 2% of annual global turnover or 10 million euros ($11.9 million), whichever is higher.[51]

The elements used by the supervisory authority to levy said fines include the following:

- Length and significance of the infringement
- Intent or negligence
- Actions taken to mitigate damage
- Whether the infringer has placed sufficient time and energy into creating a secure hosting environment
- Previous infringement

---

[45] Article 62.

[46] Articles 64 and 65 provide mechanism for the EDPB to rule on conflicting supervisory authority opinions and provide resolution within a one-month period.

[47] Article 66.

[48] The appropriate authority in which to bring a complaint can be either their home member state, the member state in which they work, or the member state in which the alleged violation took place. Article 77.

[49] Controller or processor.

[50] Article 81.

[51] Recital 151 indicates that Denmark and Estonia do not permit administrative fines of this type but rather require such fines to be levied as a criminal penalty or misdemeanor.

- Cooperation with the investigation
- Whether the infringement was self-reported by the controller or processor
- Previous action against the infringer and the manner in which the infringer handled the action
- Whether the infringer acted appropriately or had a previous certification in place
- Any other mitigating circumstances[52]

PROCESSING EXCEPTIONS

The GDPR acknowledges that not all instances of processing need to be protected in the manner prescribed above. In fact, there are several enumerated processing examples that are exempt from consent and control by data subjects. For example, should processing data be connected in some way to journalistic freedom or artistic expression, the member states are instructed to exempt that processing from the requirements set forth.[53] Similarly, personal information and the existence of an identification number found in documents held by public authorities will be excluded from protection, provided that access to the data is necessary to protect the public interest.[54]

From an employment perspective, there is a recognition that local state rules may take precedence over those outlined in the GDPR. Member states may create additional legislation regarding recruitment, quality of work, health and safety, and termination that may carry more restrictions than those outlined in the GDPR. Regardless, these individual state rules must provide appropriate safeguards for data subjects' interest in protecting their personal data. Each state is required to inform the Commission of these regulations by the effective date.

Regarding the areas of public interest, scientific or historical research, and statistical purposes, Article 89 addresses the balance between this valid public interest and the necessity to protect the personal information of data subjects. Here, the language suggests that these uses may require more flexibility in that they would require longer retention periods for completion of the scientific work. It is suggested that additional safeguards be put in place at the member state level, including the use of pseudonymization and anonymization to protect the identity of the data subject while the data is collected, used, and archived.[55]

REPEAL AND REPORTING

The authors of the GDPR wanted to make it clear that this will be the definitive work of the EU regarding data privacy. As such, it specifically repeals the DPD as soon as the regulation goes into effect. In addition, the Article 29 Working Party, which was tasked with interpreting the DPD, will be carried forward under the new name of the European Data Protection Board.[56] The EDPB will be made up of a chair and a member of each participating supervisory authority from each member state, as well as a member of the Commission. This EDPB is expected to act independently and provide guidance without influence from any other entity.[57]

---

[52] Article 83.

[53] Article 85 does not specify the actions suggested to the member states for exclusion of processing restrictions for journalistic, academic, or artistic expression but does require the states to notify the Commission of the laws enacted to provide such exemptions.

[54] Articles 86 and 87.

[55] Similarly, Article 91 does not infringe on existing data protection rules of churches and religious organizations existing at the time of the regulation, leaving them to their own supervisory authority and not infringed in any way by GDPR requirements.

[56] The EDPB will have the same mandate as the Article 29 Working Party and will inherit the previous opinions of that body.

[57] Articles 68–76 define the makeup of the board and the roles and responsibilities of the board, chair, and secretariat.

The power to enact this regulation is specifically entrusted to the Commission as defined by the European Parliament, which has the authority to object to actions by the Commission and a three-month window to file such an objection. Absent that, the ruling of the Commission is final.[58] Beginning in 2020 and every four years thereafter, the Commission is required to perform an evaluation of the GDPR and report the results to the European Parliament in public. The evaluation will consider transfers of personal data to third countries and any decisions handed down by the Commission and, if appropriate, recommend modifications to the regulation.[59]

International agreements made by member states regarding transfer of personal data to outside countries, prior to the enactment of the regulation, will continue to remain in effect if they comply with the privacy protections identified in the GDPR.

CONCLUSION

The manner in which the GDPR will be interpreted and enforced is still evolving. The language created seems to make clear the rights of EU data subjects, the actions required by data controllers and processors to protect those rights, and the penalties for organizations that do not comply. In a world where electronic data flows freely, almost invisibly, the EU has made a strong statement in clearly enumerating the rights of all EU data subjects and unifying its enforcement of these rights within and beyond its geographic borders.

Contacts

If you have any questions or would like more information on the issues discussed in this White Paper, please contact any of the following Morgan Lewis lawyers:

Philadelphia

Tess Blair	+1.215.963.5161	tess.blair@morganlewis.com
Vincent M. Catanzaro	+1.215.963.4648	vincent.catanzaro@morganlewis.com

About Morgan, Lewis & Bockius LLP

Morgan Lewis offers more than 2,200 lawyers, patent agents, benefits advisers, regulatory scientists, and other specialists in 30 offices* across North America, Asia, Europe, and the Middle East. The firm provides comprehensive litigation, corporate, transactional, regulatory, intellectual property, and labor and employment legal services to clients of all sizes—from globally established industry leaders to just-conceived startups. For more information about Morgan Lewis or its practices, please visit us online at www.morganlewis.com.

*Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan Lewis operates through Morgan, Lewis & Bockius, which is a separate Hong Kong general partnership registered with The Law Society of Hong Kong as a registered foreign law firm operating in Association with Luk & Partners.

[58] Article 92.

[59] Article 97.