ACHIEVED COMPLIANCE
SOLUTIONS

Who Is Responsible for What Under GDPR?

Determining whether your company is primarily a controller or processor under GDPR will significantly impact on the amount of work and resources needed to comply with the law. For example, the requirement to honor individual rights (such as the right to consent, access, correction and erasure) largely falls on the data controller, not on the processor. Similarly, the obligation to perform a privacy impact assessment falls on the controller. Because the burdens can be significantly different, it is imperative for companies to understand what role they play with respect to which data groups.

Many companies will find themselves in the position of being a controller as to some types of data (such as information gathered from employees, vendors, or direct customers) and a processor as to other types of data. Nonetheless, determining the appropriate role can make a drastic difference in the amount of work necessary to comply in those instances when you are primarily a processor.

A controller is a person or entity that determines the purposes and means of processing personal data. For example, a company that collects customer names and email addresses to provide its customers with services is a controller with respect to that information. The company determines how the customer data is used and why it is collected.

A processor is a person or entity that processes personal data on behalf of the controller. If the company from the previous example offers payroll services to its customers, the company is a processor with respect to the payroll information it receives from its customers, because the company processes payroll information only to fulfill the instructions of the customer. A processor may have processors itself; for example, the payroll company may contract with an IT provider to host its files electronically. A person or entity that processes data on behalf of a processor is sometimes referred to as a "subprocessor."

Controller Responsibilities

The controller is responsible for these main obligations:

- ✓ *Demonstrating accountability* to regulators and individuals. (Article 5 (2)).
- ✓ *Determining the lawfulness of the processing* in all instances other than when the individual gives consent. (Article 6).
- ✓ *Performing a data protection impact assessment* when processing is likely to result in a high risk to the rights and freedoms of an individual (Article 35).
- ✓ Assessing whether *further processing is compatible with the original purpose* for which the data was collected by taking into account a number of factors (see, Article 6 (4)).
- ✓ Assessing if *consent is freely given* (Article 7 (4).
- ✓ Keeping *evidence of consent* (Article 7 (1)).
- ✓ Providing *notice of how to withdraw consent* (Article 7 (3).
- ✓ Making reasonable efforts to *verify consent of a parent* when data is collected from individuals under 13 years of age (Article 8).
- ✓ Giving *notice to individuals of their rights* to access, rectify, erase, object to, and transfer their data and *providing mechanisms for the individual to exercise* those rights (Article 12 (1 & 2)).
- ✓ *Responding to individuals* about any action (or non-action) taken on their requests without undue delay and in any even within 1 month of receipt of the request (Article 12 (3 & 4)).
- ✓ *Providing individuals with clear information* about the purposes of the processing of data, where the processing occurs, the legitimate business interests for the same, who the data is shared with, contact information where requests and complaints may be directed, and other required elements of a privacy policy (Article 13 (1)).
- ✓ *Providing further information at the time the data is collected* for fair and transparent processing (Article 13 (2)).
- ✓ When *data is not gathered from the individual*, providing information to the individual about the data collected, the purposes of the collection, the categories of data collected, whether it is transferred to a country outside the EU, how long the data is stored, and other elements (Article 14).
- ✓ *Providing access to records* about whatever individual data that is held by the company and inform individuals of appropriate safeguards for any information transferred to a country that has not been deemed to be adequate (Article 15).
- ✓ *Providing copies of the actual data processed* (Article 15 (3)).
- ✓ *Implementing appropriate technical and organizational measures* to ensure and demonstrate processing is in accord with the law (Article 24).

- ✓ *Designating a representative in the EU if the controller does not have an establishment in the EU* unless their processing is only occasional and is unlikely to result in a risk to the rights and freedoms of natural persons (Article 27).
- ✓ *Utilizing only those processors and subprocessors who can provide sufficient guarantees* of appropriate technical and organizational measures (Article 28).
- ✓ *Putting in place a written contract with processors* that mandates certain aspects of the processing (Article 28 (3)).
- ✓ *Designating a data protection officer* when required (Article 37).
- ✓ Ensuring that any onward transfers of data remain within the EU or if outside the EU that there are *appropriate transfer mechanisms in place* (Article 44).
- ✓ *Notifying the supervisory authority within 72 hours* of any personal data breach (Article 33).
- ✓ *Notifying supervising authorities* of a personal data breach under certain circumstances (Article 34).
- ✓ *Consulting with the supervisory authority prior to any processing likely to result in a high risk*.

Processor Responsibilities

Certain processor duties are required by the regulation itself and others are indirectly required by virtue of the burdens the controller is required to fulfill. For example, controllers may only use processors who can provide sufficient guarantees that the processor itself can implement appropriate technical and organizational measures to meet the requirements of the regulation and protect individual's rights (Article 28 (1)). Because of this requirement on the controller, processors must be prepared to take on duties in support of a controller's obligations.

The regulation *directly* requires processors to:

- ✓ *Process data minimally, lawfully, fairly, and in a transparent manner and not process data in a manner that is incompatible with the original purpose of processing*. While it is up to the controller to demonstrate compliance with this obligation, the obligation itself rests also on the processor (Article 5).
- ✓ *Determine that their processing is lawful (*Article 6).
- ✓ *Implement appropriate technical and organizational measures* to ensure the protection of the data and individual's rights (Article 28).
- ✓ *Designate a representative in the EU if the processor does not have an establishment in the EU* unless their processing is only occasional and is unlikely to result in a risk to the rights and freedoms of natural persons (Article 27).

- ✓ *Obtain consent from the controller before engaging a subprocessor* (Article 28).
- ✓ *Obtain a contract from the controller* with its instructions on how to process data (Article 28 (3)).
- ✓ *Assist the controller in implementing appropriate security* with respect to personal data transferred to the processor.
- ✓ *Notify the controller without undue delay of any personal data breach* (Article 33).
- ✓ *Designate a data protection officer* when core activities require (Article 37).
- ✓ Ensure that any onward transfers of data remain within the EU or if outside the EU that there are *appropriate transfer mechanisms in place* (Article 44).

Joint Responsibilities

Where two or more controllers jointly determine the purposes and means of processing, they are joint controllers. Joint controllers must:

- ✓ Determine their respective responsibilities, in particular, with respect to honoring individual's data rights and their exercise of the same (Article 26).
- ✓ Ensure the individual is informed of who has what responsibilities.
- ✓ Irrespective of their differentiation of duties and responsibilities, each must still respond to any individual's exercise of rights (Article 26 (3)).