How Non-Disclosure Agreement Risks Factor into EU GDPR Compliance

The European Union's (EU) General Data Protection Regulation (GDPR) enumerated individuals' data privacy and protection rights, established regulations for organizations to comply with, and introduced sweeping operational changes. Any US-based organization that interacts with or processes data belonging to citizens of EU member states must comply with the GDPR.

With that said, does GDPR compliance present organizations (or their employees) with non-disclosure agreement risk, and if so, what are those risks?

Non-Disclosure Agreements (NDA) and the EU's General Data Protection Regulation (GDPR)

Employers commonly use non-disclosure agreements (NDA) to safeguard sensitive information pertaining to organizational activities. To be effective and stand up to legal scrutiny, they must generally cover a specific scope of information and often remain active for a specified duration (e.g., until departure/termination; for a set number of years).

As the GDPR protects personal data confidentiality, many organizations might assume that NDAs are mandatory for compliance. However, NDAs are not explicitly required by the GDPR. Regardless, they do still factor into GDPR compliance in two ways:

- Obligatory data processing agreements (DPA) between data controls and data processors
- Non-obligatory but advised confidentiality and non-disclosure agreements signed by employees of data controllers and processors

Overall, GDPR compliance mandates a substantial amount of agreements and written or electronic consent forms. Given the regulation's wide-ranging applicability, organizations should strongly consider adding NDAs to their other legal documents to best ensure compliance.

EU GDPR—Pragmatic Approaches

The data processing agreements required by the GDPR—Article 28(3)—effectively act as organization-level non-disclosure agreements signed by data processors due to the stipulations expanded upon in points (a) through (h). Understanding how both Article 28(3) and the advised confidentiality and non-disclosure agreements for employees factor into pragmatic GDPR compliance first depends on gaining familiarity with:

- The parties involved with GDPR compliance
- Overall compliance goals and responsibilities

As a compliance and cybersecurity expert, [REDACTED] can help advise your GDPR (and all other sensitive data protection) efforts. GDPR aside, there is a growing legislative trend in the US and elsewhere internationally to establish and enforce similar personal data protections—led domestically by the California Consumer Privacy Act (CCPA) and the Virginia Consumer Data Protection Act (VCDPA).

Whether or not your organization is subject to GDPR compliance, it may soon be required to comply with comparable US state and federal regulations. Therefore, familiarizing yourself with GDPR basics will help your organization prepare for the likely coming changes.

Understanding the GDPR and Its Involved Parties

In 2016, the European Union enacted the General Data Protection Regulation—formally recorded as “Regulation (EU) 2016/679”—as legislative means of protecting member states’ citizens’ personal data. Member states comprise the 27 nations that make up the EU. In addition, the GDPR covers citizens residing in the non-EU countries of Iceland, Lichtenstein, and Norway due to their inclusion within the European Economic Area (EEA).

The GDPR defines covered citizens’ “personal data” in Article 4 as “any information relating to an identified or identifiable natural person.” If your organization implements a GDPR-specific NDA, it should cover the established categories of personal data as the confidential information to be protected, including:

- Name
- Identification numbers
- Residence or physical location data
- Specific identity characteristics:
    - Physical
    - Physiological

    - Genetic
    - Mental
    - Economic
    - Cultural
    - Social

Critically, the GDPR affects all organizations that interact with and process the personal data of these citizens, who are referred to as “data subjects,” for professional or commercial purposes. As a result, compliance is not determined by an organization’s location, industry, or operational activity as it often is with many other regulations.

Parties Involved with GDPR Compliance

The organizations that should be most concerned with GDPR-specific NDAs are those deemed “data controllers” and “data processors.” The GDPR establishes these and other terms for identifying the parties related to compliance:

- **Data subjects** – The individuals whose data is collected and processed (with their informed consent); includes citizens of EU member states, Iceland, Lichtenstein, and Norway.
- **Data controllers** – Any natural or legal person, public authority, agency, or other body that collects data subjects’ personal data and determines the means and purposes of processing.
    - Joint Controllers – Two or more controllers operating together are referred to as “joint controllers.”
- **Data processors** – Any natural or legal person, public authority, agency, or other body that processes personal data at the instruction of a data controller.
    - Sub-processors – If a data processor outsources responsibilities and execution to another processor, the latter entity is referred to as a “sub-processor.”
- **Data protection officers** – An organizational leadership role required by GDPR; oversees an organization’s GDPR adherence.
- **Supervisory authorities** – The independent public authority established by EU members states to oversee GDPR compliance and enforcement.
- **Third parties** – Any natural or legal person, public authority, agency, or other body authorized to process personal data under a controller or processor’s authority; excludes parties identified as data subjects, controllers, and processors in a given relationship.

Though not defined within Article 4, data controllers and processors' employees are effectively regarded as their respective organizations' agents concerning GDPR compliance. As a result, regulatory adherence responsibilities ultimately fall upon organizations regardless of employees' activities, which is why non-disclosure agreements concerning processed personal data are strongly advised.

Article 6—Established Criteria for Lawful Personal Data Processing

Per GDPR Article 6, the overarching restriction on any organizations' lawful ability to process data subjects' personal data requires at least one of six criteria to be met. These criteria make up the permitted instances where personnel interact with any NDA-covered information.

The six criteria are:

- **6(a)** – The data subject has provided informed consent
- **6(b)** – Due to obligations specified in a contract with a given data subject or during the preliminary stages of formalizing a contract and at the data subject's request
- **6(c)** – The organization must process a given subject's personal data as part of legally obligated compliance efforts
- **6(d)** – Either a given data subject's or another natural person's vital interests necessitate processing
- **6(e)** – Tasks executed in the interest of the public or via official public authority necessitate processing
- **6(f)** – An organization's legitimate interests that are not overridden by data subjects' interests or personal data rights
    - Especially pertains to circumstances where the given data subject is a child
    - Public authorities are exempt from point (f)

The GDPR's Enumerated Rights for Data Subjects

Coinciding with six criteria that determine lawful personal data processing, the GDPR primarily recognizes four rights belonging to data subjects. Disclosure to a data subject of their own personal data would not constitute an NDA violation. GDPR-specific NDAs must be constructed with these four rights kept in mind:

- **Transparency and modalities** – Enumerated in Article 12. Prior to any instance of data collection or processing, organizations must provide data subjects with notice and gain their written or electronic consent. All notices and consent gathering must be written in a

"concise, transparent, intelligible, and easily accessible form, using clear and plain language, in particular for any information addressed specifically for a child."

- **Information and access** – Predominately enumerated in Article 15. Data subjects may request confirmation of and information pertaining to any of their processed personal data, including:
    - Processing purposes
    - The disclosed personal data's categories
    - The recipients or categories of recipients of their personal data, especially if the recipients are located in another country
    - The estimated period for which their personal data will be stored
    - The existence of the right to request rectification, erasure, or processing restrictions pertaining to their personal data
    - The right to lodge complaints with a country's supervisory authority
    - Any available information pertaining to the source of personal data if a controller did not directly collect it
    - Whether any automated decision-making (e.g., profiling) is utilized, along with information pertaining to the determining logic, significance, and expected consequences
- **Rectification and erasure** – Predominately enumerated in Article 17. Data subjects hold the right to obtain rectification of inaccurate or incomplete personal data without delay, per Article 16. Sometimes referred to as the "right to be forgotten," data subjects also hold the right to obtain the erasure of their personal data without delay so long as one of the following criteria is met:
    - The data is no longer needed for its initial collection or processing purposes
    - The data subject revokes their consent (and there is no other legal basis for the processing)
    - The data subject objects to processing due to personal circumstances and on the basis of Article 6(e) or (f) (see above) or if their personal data is used for direct marketing purposes
    - The data subject's personal data was processed without any legal grounds for doing so
    - The personal data must be erased due to an organization's compliance requirements related to either party's national laws

    - The personal data was collected as part of the offering of information society services, which are defined in Directive (EU) 2015/1535 as “any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.”

- **Right to object and automated individual decision-making** – Predominately enumerated in Article 21. Data subjects hold the right to object to decisions regarding their personal data that are solely carried out via automated processing (Article 22). Data subjects may otherwise object to processing according to the following criteria:
    - Personal circumstances and on the basis of Article 6(e) or (f) (see above), unless the data controller can provide a compelling and legitimate legal basis
    - If their personal data is used for direct marketing purposes
    - If their personal data is processed for scientific, historical, or statistical purposes unless it is determined as necessary to execute a task based on public interest

While the data subjects’ enumerated rights are generally ironclad, there do exist exceptions based on the grounds of legal and compliance obligations, public interest, and “compelling reasons” that are not listed here for brevity. Therefore, please consult the GDPR’s full text or a GDPR compliance advisor before making any organizational policy and process decisions.

Data Processing Agreements—Effectively Organization-Level NDAs

With a general understanding of the GDPR’s enumerated rights for data subjects and compliance obligations for controllers and processors, the nuanced relevance of non-disclosure agreements becomes clearer.

In terms of obligatory documents and per Article 28(3), data controllers and processors are required to formalize a contract stipulating “the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the data controller.” This contract is referred to as a “data processing agreement” (DPA).

Given the GDPR’s compliance restrictions, DPAs effectively operate as organizational-level NDAs that forbid personal data disclosures or processing outside of the specifically established purposes. The non-disclosure agreement risk of not establishing a DPA is noncompliance and any resulting penalties. DPAs must contain, at a minimum, eight stipulations pertaining to these restrictions:

- Personal data may only be processed following documented instructions provided by the controller and, if legal or compliance obligations dictate otherwise, processors must notify controllers of any non-instructed activity.
- The individuals processing personal data are either:

    - Sworn to confidentiality
    - Bound by appropriate statutory obligations of confidentiality
- Activities related to personal data must adhere to the “Security of processing” requirements established in Article 32.
- Any relationship entered into between processors and sub-processors requires the controller’s authorization—directly or with the processor providing notice in the case of general authorizations—and remains subject to the original DPA.
- Processors must assist with controllers’ obligations to data subjects’ execution of their rights.
- Processors must assist with controllers’ “security of processing” (Article 32) and “prior consultation” (Article 36) obligations. Article 36 requires data controllers to consult with the applicable supervisory authority if processing would constitute a “high risk” in the absence of mitigation measures.
- Processors must delete or return all disclosed personal data to the controller upon the conclusion of processing services unless continued storage is a legal or compliance requirement (and for the specified storage duration).
- Processors must make all compliance-related information pertaining to Article 28 available to data controllers and assist authorized auditors.

GDPR Article 28(3)—Concerning Employee-Level NDAs

While the GDPR obligates an effective NDA at the organizational level per Article 28(3)(a), it does not specify any requirement for a signed contract with employees operating as their respective employers’ agents. However, the employee confidentiality referred to in Article 28(3)(b) does mean that NDA contracts are strongly encouraged to help ensure compliance.

As a result, any employee-level non-disclosure agreement risk more accurately pertains to the threats of compliance enforcement should no contract exist. Thus, a GDPR-specific NDA should cover employees’ confidentiality obligations regarding data subjects’ personal data insofar as they will not disclose the information to any party or for any purpose outside the scope of the data controller’s explicit instructions.

However, crafting enforceable NDAs is often a complicated process.

What Should a GDPR Non-Disclosure Agreement Include?

Non-disclosure agreements are generally complex legal documents due to their broad legislative inclusion and somewhat subjective enforceability. A search of The Office of the Law Revision Counsel database that compiles the permanent US Code of Law retrieves over 600 results across “non-disclosure,” “nondisclosure,” and “non disclosure.” NDA disputes may fall into various jurisdictions depending on applicable legislation and the involved parties’ locations.

Your organization’s GDPR-specific NDA may require:

- Certain language
- Established timeframes of applicability
- The precisely specified scope of the confidential information covered
- Not placing undue burdens on the signatories

For example, the Whistleblower Protection Enhancement Act of 2012 requires specific language to be included in any NDA provided to federal employees as conditional for enforcement.

To ensure that your organization’s GDPR-specific NDA is enforceable, consult appropriate legal advice.

How To Sign a Non-Disclosure Agreement

Guidance on how to sign a non-disclosure agreement is significantly more straightforward than crafting the document itself. Non-disclosure agreements may be signed as a physical copy (i.e., with a pen) or electronically. Electronic signatures completed by US citizens must use one of three NIST-approved digital signature algorithms:

- DSA
- RSA
- ECDSA

GDPR NDAs Made Simple

Establishing GDPR-specific NDAs is both effectively mandatory (i.e., in the case of DPAs) and not (i.e., for employees). However, the extent of personal data protections and the organizations that must comply with the GDPR make NDAs a wise inclusion within your organization’s legal documents.

Any non-disclosure agreement risk related to GDPR compliance pertains to not having a signed document on record.

As a compliance and cybersecurity expert, [REDACTED] will help advise your organization's personal data protections to help ensure adherence with GDPR and other regulations, such as the CCPA. Contact [REDACTED] today to begin rethinking your GDPR compliance.