Intapp Cloud Infrastructure

Addressing privacy concerns in Intapp products

As the number of privacy regulations increases internationally, your firm faces additional compliance requirements. This privacy brief describes how Intapp and Intapp solutions can help your firm comply with privacy obligations while clarifying the role your team will need to take.

This document discusses the general topic of privacy regulations and does not address the specific requirements of specific regulations. However, for consistency, we will in many places use the terms defined in the General Data Protection Regulation (GDPR).

Note that security and privacy are often discussed in the same context. However, they are two separate concepts with different goals:

- **Security aims to ensure** the confidentiality, integrity, and availability (CIA) of any type of data. This is usually done through a combination of internal policies and contractual or technical controls
- **Privacy aims to protect** a data subject's information and rights. While those rights include the security of personal data, they go beyond the security aspect by limiting the purposes for which personal data can be used and addressing the quality and retention of that data

Although security is part of privacy, in some cases, the goals of privacy regulations might be counter to the goals of security controls. Clients will have to weigh their needs and requirements to decide how to implement specific business processes that fulfill those needs and requirements.

This document addresses Intapp's and your firm's responsibilities, as well as general technical capabilities related to privacy regulations. The information in this document applies to all Intapp solutions; product-specific capabilities are described in product-specific documentation.

Shared responsibility model

When using Intapp solutions, your firm is responsible for client data your users upload to those solutions. This includes data entered manually as well as data uploaded through integrations or other automated means. Your firm is, in most cases, the data controller. Intapp acts as a data processor.

Therefore, Intapp and your firm share responsibility for complying with applicable privacy regulations.

Your firm will need to:

- **Ensure that all personal data** is collected, stored, retained, and processed in accordance with relevant privacy regulations. This includes, for example, obtaining consent where needed or establishing a relevant legal basis for processing personal data.
- **Review data subject requests and act on them** according to specific regulatory requirements
- **Establish relevant processes** on how to update, delete, and protect personal data as required by your business and regulatory needs

Intapp will:

- **Provide your firm with the ability** to act on data subject requests
- **Provide your firm with the technical capability** to implement common business processes
- **Support your firm by responding** to reasonable technical questions regarding how to implement relevant processes including performing specific required processes where the solution does not give your firm the ability to perform those actions
- **Provide a secure platform** that protects personal data in a manner which complies with common privacy regulations or inform your firm when specific requirements cannot be fulfilled
- **Execute contractual agreements** that assure your firm that Intapp will protect and process personal data in a responsible manner
- **Forward client-specific data subject requests** to your firm, so that your team can respond as required

Types of personal data processed by Intapp solutions

Although specific solutions process different sets of data, there are some general categories of personal data that most or all of our solutions process.

End-user information

To manage permissions and authentication, Intapp solutions need a minimal set of business contact information, such as name and email address, to provide your users with access to the solution and/or send them reports or notifications.

To provide context for some business logic or to support other users' work, additional information, such as titles, roles, other contact information, or reporting structures, might be stored in Intapp solutions.

To allow your firm to track relevant actions or to implement security checks, actions performed in Intapp solutions might be tracked, and those actions may contain personal data. An example would be a user's login history, which could include the IP address from which the user connected.

Free-text information entered by the user might contain personal data. For example, a note about a client interaction might contain personal data about the end user as well as your client.

Some solutions require or process additional personal data. For example, our experience management components might list educational background, specific achievements, or experience with other clients.

Client information

To characterize and classify information about the services you provide to your clients, it is critical for Intapp solutions to store and process details about your clients. Client information will include:

Client names, which could contain personal information

Client contact information, which contain names and business contact information of persons at client sites

Other information collected about those clients, such as information from news sources or corporate filings

Other personal data

Often, your work for a client will contain information about third parties. Those might be your clients' vendors or suppliers or parties adverse to your clients. In most cases, the information about third parties will be limited to what is needed for the specific engagement.

Several types of personal data are **not** commonly found in Intapp solutions. These are often seen as more sensitive data elements that might require specific treatment or protections. Note that it is possible that a limited set of such information is entered into Intapp solutions. As your firm controls what data is uploaded or entered into Intapp solutions, your team should review the need to process such information, and limit it to cases where such processing is required, ensuring that such personal data is adequately protected. These types of personal data include:

Information about children

Information regarding criminal convictions or offenses

Special categories of personal data, such as genetic, health, or sexual information

Special categories of personal data, such as information about ethnic origin, political orientation, sexual orientation, religious or philosophical beliefs, or trade union membership

Contractual agreements relating to personal data

During the sales process, Intapp and your firm will enter into contractual agreements that provide the legal basis for the engagement of Intapp by your firm.

Master Subscription and Services Agreement (MSSA, intapp.com/intapptermsandconditions)

The MSSA contains commitments pertaining to the engagements and the responsibilities of each party. Specifically, it describes the commitment regarding the protection of confidential data, including client data.

Data Processing Addendum (DPA, intapp.com/dpa)

The DPA specifically addresses the requirements around processing personal data, including:

- **Limiting processing** by Intapp to that required to provide your firm with the subscribed service
- **Securing personal data** to an adequate level compliant with relevant regulations
- **Describing how Intapp will respond** to data subject requests
- **Regulating** cross-border transfers and sub-processing

Standard Contractual Clauses (SCC, intapp.com/dpa)

The SCCs provide assurances around protecting personal data when transferred to a different country. The SCCs also contain a detailed listing of the security controls in place for Intapp solutions.

Location of data processing

We host Intapp Cloud Infrastructure in multiple global locations; your firm can select your service delivery region of preference. This flexibility lets you locate your applications within the region that matches your business requirements. For instance, European firms can choose to leverage clusters in the European Union to avoid regulatory uncertainty.

By default, client instances are deployed in the region where their primary address is located, as described in the MSSA. Global firms are encouraged to determine whether a different geographic region might be better suited based on their regulatory and compliance needs.

Intapp solutions are generally accessible from any location, even outside the geographic region in which they are deployed. Intapp relies upon the SCCs to provide a contractual commitment regarding the protection of personal data when transferred to a country outside the relevant geographic region.

Security of processing

Intapp has a mature security program designed to address the need for confidentiality, integrity, and availability of all client data, including any personal data included therein.

Specifically relevant to privacy, Intapp solutions are certified to be compliant with the controls in ISO 27018 and ISO 27701, which address the security of personally identifiable information in public clouds.

Support for data subject requests

Various privacy regulations have different requirements and/or allow data subjects to request certain restrictions or information.

Keeping personal data updated

Yoru firm has control over all client data and will be responsible for keeping personal data updated. To support your firm, we provide APIs which allow integrating data flows to and from other client systems.

Restricting the processing of personal data

While clients need to make their own assessment, in many cases processing personal data in our solutions is required for business processes or regulatory needs, so the need for restricting of processing capabilities is very limited.

In Dispatch for Intapp DealCloud, your users can mark contacts as “opted out” of marketing communication which simplifies compliance with local opt-out or opt-in requirements.

Deleting and retaining personal data

While clients need to make their own assessment, in many cases, processing is required for legal and business purposes. This means data needs to be retained for an extended period and the need for deleting information during the business relationship is often limited. For example:

- During an intake process, an AML or KYC check is legally required, and evidence of that check must be retained to demonstrate such compliance
- Compliance with SEC rules or security forensics requires clients to retain certain logs or audit information

Privacy requirements that favor minimizing the amount of data retained and processed can, as such, run counter to some aforementioned obligations. Clients will have to determine their needs and policies.

In some instances, business requirements to retain data are less stringent than previously mentioned requirements (e.g., SEC compliance). In these instances, Intapp's automated data retention rules are in place to remove information when applicable.

	Data set	Retention period
Intapp Cloud Infrastructure identity management	Log data	1 year
Intapp Documents and Intapp Workspaces	Log data Client data	1 year Only stored during processing
Intapp Time	Captured activities Time entries	45 days 3 years
Intapp Billstream	Client data	Only stored during processing

Please note that client data removed at the end of the retention period might be available in data backups for a limited time after it has been removed from the live instance. To support a "right to be forgotten" request, Intapp DealCloud lets your users delete contact records and mark a record in such a way that the record cannot be added again.

Data access and minimization capabilities

Intapp solutions provide an extensive role-based permission model which allows clients to limit end-user access to only the data required to perform that user's role. In addition, the solutions support implementing ethical wall restrictions to limit access to information on specific clients or engagements.

For questions or concerns regarding the contents of this document, please contact your Intapp representative

© 2024 Intapp. All rights reserved. Intapp is a registered trademark of Intapp or its affiliates. Other trademarks held by their respective owners.