

FAQ - Addition of New Subprocessor(s) Under the Acumatica DPA

A. General Notice and Business Purpose

1. Why have we received this notification?

Acumatica uses third-party service providers to assist in delivering, supporting, and improving its services. In some cases, these third party service providers may process customer personal data on Acumatica's behalf as part of the services they provide. These third party service providers are considered subprocessors, under applicable data protection laws and Acumatica's Data Processing Addendum (DPA). Before engaging a new third-party in processing customer personal data on Acumatica's behalf, Acumatica provides notice to customers in accordance with its DPA and applicable privacy obligations. This notification is intended to keep customers informed about changes to Acumatica's subprocessor list.

2. Why is Acumatica adding Intercom Inc, (doing business as Fin) ("Intercom") as a subprocessor under the DPA?

To improve your support experience, Acumatica is introducing **Acumatica Messages**, an in-product support experience. Intercom helps Acumatica in delivering Acumatica Messages and is added as a subprocessor because it is required to process personal data in this capacity.

3. What service, feature, or business function will Intercom support? What is the purpose of the processing performed by Intercom?

Intercom will support Acumatica Messages, Acumatica's newly introduced in-product support experience. Intercom is a leader in conversational customer engagement and support experience. To provide you with the best experience, rather than building from scratch, Acumatica utilizes Intercom for Acumatica Messages. The purpose of the processing performed by Intercom is to provide you with optimal in-product support experience.

4. Does the addition of Intercom require me to sign a new agreement or updated DPA?

No, you are not required to sign a new agreement with Acumatica. The updated subprocessor information is incorporated into Acumatica's DPA, which is, in turn, incorporated into your main agreement with Acumatica.

5. Where can I review Acumatica's current subprocessor list and the updated DPA?

The current list of subprocessors is included in the Acumatica DPA and can be accessed under "Acumatica Data Processing Addendum" at <https://www.acumatica.com/agreements/>.

B. Scope and Applicability



1. Does this subprocessor apply to all customers, or only to those using specific products, features, deployment models, or services? Does this apply to SaaS customers? Does this apply to PCS and PCP (self-hosted) customers?
Intercom applies to and processes the personal data of all Acumatica customers. This includes SaaS, PCS, and PCP.
2. How does Intercom relate to my data, systems, and environment?
Acumatica uses Intercom to provide customer support services. Intercom will be integrated with Acumatica's support ecosystem. Depending on how you interact with Acumatica support, Intercom may process information related to your support requests and related account details. Intercom will only receive information required to provide customer support services.
3. Is this subprocessor used only if a customer uses a particular feature or functionality?
Intercom will process your data only when you interact with Acumatica support through the in-product support experience, Acumatica Messages.
4. Am I required to take any action as a result of this change?
No action is required from you as a result of this change.
5. Can I disable, opt out of, or avoid use of this subprocessor, and if so, what functionality may be affected?
Yes. You can disable Acumatica Messages from the appropriate settings page on the Acumatica platform. If you choose to disable Acumatica Messages, Intercom will not process your information. More information is available [here](#).

C. Data Categories and Processing Purposes

1. What data is Acumatica collecting, transmitting, storing, or otherwise making available to Intercom? What specific access will Intercom have to my data?
Intercom will receive account information, contact information, and support communications associated with your use of Acumatica.
2. What categories of personal data are processed by Intercom?
The personal data Intercom may process in connection with its service include: name (first and last), title, position and employer; contact information (company, email, phone, business address); ID data (username, user ID, visitor and account IDs); connection data, localization data (e.g., IP address); website and platform usage information; system usage data (including behavioral usage telemetry); application integration data, metadata (product edition, deployment type, user role); and communications data (e.g., provided through the in-product support experience, Acumatica Messages).

3. Will Intercom have access to financial, transactional, ERP, general ledger, or historical business data?

Intercom is not provided access to your ERP, general ledger, or transactional data as part of its function. However, since Acumatica Messages, the in-product support experience, processes whatever you submit to it, Intercom will process such information if you choose to include it in your interaction with Acumatica Messages.

4. Will Intercom process customer content, support cases, chat messages, attachments, or communications submitted by users?

Yes, Intercom will be integrated with Acumatica's support ecosystem, and accordingly it will process information you may provide when interacting with our support system.

5. Will personal data, pseudonymized data, deidentified data, or a combination of these be processed by Intercom?

Yes, Intercom will process personal data of the categories of personal data described above.

6. Will any Protected Health Information (PHI) be processed by Intercom?

No, the new subprocessor will not be processing PHI on behalf of Acumatica.

7. Will any payment card data, bank account data, or other PCI-DSS-regulated data be processed by Intercom?

No, the service provided by Intercom is not intended to process payment card data, bank data, or other PCI-DSS regulated data. You are responsible for not including such data when interacting with Acumatica Messages, the in-product support experience.

8. Does Intercom process data on Acumatica's behalf only, or may it use the data for its own purposes?

Per the agreement between Intercom and Acumatica, Intercom processes your data only on behalf of Acumatica and solely for the purpose for which Acumatica shared your data with Intercom. Intercom is not authorized to use your data for its own purposes.

D. Hosting, Data Residency, and International Transfers

1. Where will customer data processed by Intercom be hosted, stored, or processed?

Intercom hosts data in Amazon Web Services (AWS) facilities. Depending on the regional configuration (US, EU, or Australia), data is processed in the US (us-east-1, Northern Virginia), EU (eu-west-1, Dublin, Ireland), or Australia. Acumatica's integration will leverage appropriate regional hosting where available.

2. Will customer data be transferred outside the customer's jurisdiction?

Transfers may occur depending on the customer's location and Intercom's regional hosting configuration. Standard transfer mechanisms (e.g., SCCs, UK Addendum, Data Privacy Framework) continue to apply per Acumatica's DPA. Customers requiring certain data residency or seeking to minimize international transfers should contact Acumatica to discuss available Regional Data Hosting options.

3. Does Intercom support data residency or geographic processing restrictions?

Yes. Intercom offers Regional Data Hosting in the US, EU, and Australia, allowing data to be processed and stored within the chosen region (with limited exceptions).

4. What transfer mechanisms are used for international personal data transfers, such as SCCs, UK Addendum, Data Privacy Framework, or other approved mechanisms?

The addition of Intercom as a new subprocessor has not changed Acumatica's transfer mechanisms. Please refer to the "Data Transfers" section under the DPA for more information.

E. Security Measures and Access Controls

1. What encryption standards are applied to data handled by Intercom?

Intercom applies industry-standard encryption: TLS 1.2+ (with strong cipher suites and Perfect Forward Secrecy) for data in transit, and AES-256 for data at rest.

2. Is data encrypted in transit?

Yes. All data sent to or from Intercom is encrypted in transit using TLS 1.2+

3. Is data encrypted at rest?

Yes. Customer data is encrypted at rest using AES-256.

4. How is access to customer data controlled, restricted, logged, and monitored?

Access is controlled via role-based access controls (RBAC), least privilege principles, multi-factor authentication, and strict need-to-know policies. All access is logged and monitored as part of Intercom's security program.

5. What security controls are in place to prevent unauthorized access to customer data?



Controls include encryption (in transit and at rest), network segmentation, intrusion detection and prevention, regular vulnerability scanning, access logging/monitoring, and contractual restrictions on sub-processors.

6. How does Acumatica review and monitor Intercom's ongoing security and privacy posture?
Acumatica conducts due diligence, reviews Intercom's compliance attestations (SOC 2 Type II), and maintains ongoing contractual oversight over Intercom's security and privacy obligations.
7. Does Intercom perform regular penetration testing, vulnerability assessments, or independent security reviews?
Yes. Intercom conducts regular vulnerability assessments, penetration testing, and independent security audits as part of its SOC 2 Type II and ISO 27001 compliance programs.
8. What incident response procedures apply if Intercom experiences a security incident affecting customer data?
Intercom maintains a formal incident response process. Security incidents are investigated promptly, and Acumatica is notified without undue delay in accordance with the DPA between Acumatica and Intercom and applicable privacy laws. Intercom cooperates fully with investigations and remediation.

F. Compliance, Audit, and Assurance

1. Will Intercom be covered by Acumatica's SOC reports?
Intercom maintains its own SOC 2 Type II report, which Acumatica reviews as part of subprocessor due diligence. It is not directly covered under Acumatica's SOC reports.
2. Will there be any additional complementary user entity controls (CUECs) that customers should consider?
You are not required to implement any CUECs specifically related to Intercom's function as an Acumatica subprocessor. Acumatica recommends that you refresh your personnel's knowledge about what information they should and should not share when interacting with Acumatica Support. Specifically, they should not provide Acumatica Support (through Acumatica Messages, or otherwise) with any Sensitive Information, such as protected health information subject to the Health Insurance Portability and Accountability Act (HIPAA), payment card or cardholder data subject to Payment Card Industry Data Security Standard (PCI-DSS), or any other information subject to heightened legal or regulatory protection.
You should review Acumatica's SOC reports to learn more about the general CUECs suggested by Acumatica.

3. Does Intercom maintain a SOC 1 report?
No. This is not applicable to Intercom's services.
4. Does Intercom maintain a SOC 2 report?
Yes, Intercom maintains a SOC 2 Type II report covering security, availability, and confidentiality.
5. Is Intercom certified under ISO 27001 or any other recognized security standard?
Yes, Intercom is ISO 27001:2022 certified (and holds related certifications).
6. Does Intercom comply with PCI-DSS or other financial data security standards, and is PCI-DSS applicable to the data processed?
No. Providing PCI-DSS controlled information (such as credit card or bank account information) to Acumatica support, including through Acumatica Messages, the in-product support experience, is prohibited.
7. Is HIPAA applicable to Intercom's services?
HIPAA is not applicable to the nature of the services provided by Intercom. Providing PHI to Acumatica support, including through Acumatica Messages, the in-product support experience, is prohibited.

G. AI and Automated Technologies

1. Does Intercom use artificial intelligence, machine learning, or automated technologies to provide the service?
Yes, the service includes a support services AI agent.
2. If AI or machine learning is used, are customer data, support queries, telemetry, or interactions used to train the Intercom's models?
Customer data and interactions will not be used to train Intercom's AI or LLM models. Intercom may use aggregated, pseudonymized or deidentified data for service improvement purposes.
3. What safeguards are in place to prevent customer data from being exposed to other customers through AI-generated responses or model outputs?
Safeguards include isolation of customer data, retrieval-augmented generation (RAG) limited to authorized knowledge bases, temporary processing only, contractual prohibitions on third-party LLM training, and output filtering/monitoring.

H. Retention, Deletion, and Return of Data

1. For how long will data be retained by Intercom?

Intercom retains your data for as long as needed to provide the services and to fulfill applicable legal obligations.

2. What happens to customer data when it is no longer needed for the processing purpose?

Customer data is securely deleted or deidentified once it is no longer required for delivering the services or meeting legal obligations. Intercom uses secure deletion methods to ensure data cannot be recovered.

3. How is customer data deleted or returned following termination of the applicable services or expiration of retention periods?

Upon termination or expiry of services (or at customer request), Intercom will, following Acumatica's request, return or delete all customer personal data. Deletion occurs as soon as reasonably practicable following Intercom receiving a request (within a maximum of 30 days).

4. Are backup copies retained, and if so, for how long?

Backup copies will be retained for 14 days before they are deleted, unless further retention is required by law.

5. Can I request deletion of data held by Intercom, and if yes, how?

Yes. Data subjects (i.e., natural person end users) may submit requests regarding the deletion of personal data through Acumatica. Additional information may be requested to verify your identity or locate the relevant records.

I. Customer Rights, Objections, and Contractual Protections

1. What happens if I do not agree to the use of Intercom?

You have the right to raise your concern and/or object to a newly appointed subprocessor within thirty (30) days of receiving this notice in accordance with the "[Sub-processors](#)" section of the DPA.

2. What rights do I have if I object to the appointment of a new subprocessor under the DPA?

In accordance with the DPA, if an objection cannot be addressed through good faith discussions, you will be entitled to terminate your engagement with Acumatica, at your discretion.

3. What is Acumatica's process for reviewing and responding to customer objections to newly appointed subprocessors?

When Acumatica receives a customer objection regarding a new subprocessor, Acumatica reviews the concern with its privacy, legal, security, and business teams to assess the underlying issue and determine whether reasonable alternative measures are available.

4. Does Acumatica remain responsible for the acts and omissions of its subprocessors as required under the DPA?

Acumatica enters into contractual agreements with its subprocessors containing data protection obligations which are no less protective of personal data as in Acumatica's DPA. Consistent with applicable data protection laws and the DPA, Acumatica remains responsible for its subprocessors' processing of your personal data to the extent set forth in the DPA and for ensuring that they process your personal data in accordance with Acumatica's instructions and contractual commitments.

J. Impact on Services, Fees, and Customer Experience

1. Will this change affect system functionality, performance, support, integrations, customizations, or existing workflows?

The introduction of Intercom is intended to improve your support experience. Otherwise, it will not affect system functionality, performance, integrations, customizations, or existing workflows.

2. Will this change result in any service interruption or downtime?

No service interruption or downtime is expected as a result of the addition of the new subprocessor.

3. Will the use of Intercom increase my subscription fees or other costs?

No, your fees remain governed by your existing agreement, order form, and any other applicable documentation and will not change as a result of the addition of the new subprocessor.

4. Who should I contact if I have additional questions?

Your questions and concerns can be directed to legal@acumatica.com.