HB HOUSEBLEND

Home / Blog

How to Ensure Your NetSuite System Is GDPR-Compliant

November 15, 2024

With GDPR (General Data Protection Regulation) in place, organizations operating within the European Union (EU) or handling data of EU residents must follow strict regulations to protect personal information. If your organization uses NetSuite, understanding how to make the system GDPR-compliant is essential to avoid fines, build trust, and protect your customers' data. This guide walks through the steps necessary to ensure GDPR compliance within NetSuite.

What GDPR Means for Your NetSuite System

GDPR, effective since May 2018, is a comprehensive regulation designed to protect individuals' personal data. It mandates that organizations:

- Obtain clear consent for data collection and usage.
- Ensure data transparency and accountability.
- Provide data subjects with the right to access, correct, and delete their data.
- Report any data breaches within 72 hours.

Failing to comply can result in penalties reaching up to 4% of the company's global annual turnover, so adherence is essential. NetSuite can support GDPR compliance, but it requires careful setup and continuous management to meet the standards.

1. Map Out Data Flow and Storage

Start by understanding how your NetSuite instance collects, stores, and transfers personal data. You'll need a clear map to document all data touchpoints.

- **Identify all sources of personal data** – Include website forms, sales data, customer service interactions, and any third-party integrations.
- **Document how data flows through NetSuite** – Map where personal data is stored within NetSuite, such as customer records, sales data, and customer support logs.
- **Assess third-party connections** – Make sure any third-party system integrated with NetSuite has its own GDPR-compliant practices.

Regularly reviewing data flow ensures you're capturing every data source and managing it according to GDPR requirements.

2. Implement Data Minimization and Access Controls

GDPR mandates data minimization, which means only collecting data necessary for specific, legitimate purposes.

- **Restrict data collection fields** – Avoid capturing data beyond what's necessary. In NetSuite, you can customize fields and restrict the data collected in forms.
- **Limit access to sensitive data** – Set role-based permissions in NetSuite to control which employees can access personal data. Only grant access to those who need it to perform their role.
- **Regularly audit access** – Conduct periodic reviews of access permissions to ensure compliance as roles change or new data is introduced.

Data minimization reduces the risk of misuse and limits potential exposure in case of a breach.

3. Obtain and Document Consent Properly

Consent management is one of the critical components of GDPR. Customers need to provide clear, explicit consent for their data to be collected and processed.

- **Set up consent fields in NetSuite** – Add specific fields within NetSuite records that document consent. This can include checkboxes that record dates and types of consent.
- **Create clear, unambiguous consent forms** – If collecting consent through NetSuite-integrated forms, ensure language is straightforward, explaining why data is collected and how it will be used.
- **Track consent revocation** – GDPR requires that users can withdraw consent at any time. NetSuite can handle this by enabling updates to customer records if a user withdraws their consent.

With proper documentation, you'll have an audit trail showing that you've complied with GDPR's consent requirements.

4. Enable Data Portability and Access Rights

GDPR grants individuals the right to access their data and request that it be transferred to another entity. Implementing data portability and access rights in NetSuite requires the following steps:

- **Create accessible data export tools** – Use NetSuite's export functions to provide data in a commonly used format (e.g., CSV or Excel). This makes data transfer seamless.
- **Allow for on-demand data access** – Configure NetSuite to generate reports that show users the personal data stored on them.
- **Automate responses for data requests** – Set up workflows to streamline processing these requests, ensuring timely responses within GDPR's 30-day requirement.

These actions will allow you to fulfill data portability requests efficiently, helping your customers retain control over their data.

5. Designate a Data Protection Officer (DPO) for Oversight

A Data Protection Officer (DPO) helps ensure that your organization complies with GDPR. While not every company needs a DPO, those processing extensive personal data or operating within the EU should consider this role.

- **Assign a DPO or a privacy officer** – The DPO or a designated privacy officer should oversee compliance efforts, including audits, policy updates, and training.
- **Conduct regular training sessions** – Your DPO or privacy officer can conduct sessions for employees, particularly for those who handle personal data directly.
- **Monitor compliance** – The DPO should regularly assess compliance, stay updated on GDPR amendments, and refine policies as necessary.

Having a dedicated officer helps ensure there's someone focused on maintaining compliance standards and educating the team.

6. Enable "Right to be Forgotten" Procedures

GDPR gives individuals the right to request deletion of their data under certain circumstances, known as the "Right to be Forgotten." NetSuite can facilitate this, but it requires specific configurations.

- **Develop workflows for data deletion** – Use NetSuite workflows to standardize the deletion process, removing personal data from all relevant areas when a request is submitted.
- **Ensure backup deletion** – Confirm that deleted data doesn't remain in backups or archives beyond the necessary retention period.
- **Document data deletion** – Record each deletion to demonstrate GDPR compliance, noting when, why, and how data was erased.

Clear procedures for data deletion ensure that requests are fulfilled accurately, minimizing the risk of retaining unwanted data.

7. Set Up Breach Detection and Reporting

GDPR requires businesses to report any data breach involving personal data within 72 hours of discovery.

- **Implement alerts for unusual activity** – Use NetSuite's customization options to set alerts for unusual data access or changes.
- **Develop a breach notification process** – Outline the steps your team should take if a breach occurs, ensuring timely notification and response.
- **Prepare pre-drafted notifications** – For faster response, have pre-approved notifications ready in case of a breach, detailing the type of data affected and remedial steps.

A well-planned breach response strategy ensures your team can act swiftly if a security incident occurs, minimizing risk and ensuring compliance.

8. Regularly Update and Audit Your Privacy Practices

Compliance isn't a one-time event; it's an ongoing process. GDPR requires you to review and update privacy practices continuously.

- **Schedule periodic audits** – Conduct routine audits of NetSuite configurations, workflows, and permissions to ensure they meet current GDPR standards.
- **Review consent and data retention policies** – Privacy policies should reflect current data practices and be reviewed annually or whenever significant changes occur.
- **Stay informed of GDPR updates** – Keep track of any regulatory changes that could affect how you manage data within NetSuite.

Regular updates to your system ensure that new risks are addressed promptly and that your NetSuite configuration aligns with the latest compliance requirements.

Conclusion

Maintaining GDPR compliance within your NetSuite system requires consistent effort and careful planning. By mapping data flows, managing consent, automating data rights, and developing a solid breach response plan, you can protect your organization against potential fines and build a trustworthy relationship with your customers. Remember that GDPR compliance is not a one-time task but a continuous commitment to data privacy and security.