

Open iT Software and Personal Data Protection

Open iT Group, May, 2026

This paper addresses questions that Open iT customers may have regarding personal data protection generally, and the EU General Data Protection Regulation (GDPR) in particular.

The General Data Protection Regulation (GDPR).

The GDPR applies directly across the EU/EEA, while Member States may adopt national laws that supplement it in specific areas, including employment-related processing. As a result, many organisations use GDPR as a baseline global privacy standard for the handling of personal data.

Is Open iT Software GDPR Compliant?

The short answer is that GDPR compliance depends on the specific processing activities, the purposes for which personal data is processed, and the manner in which the software is configured, deployed, and used. Open iT Software processes data under the customer's instructions and configuration. Depending on the deployment model and services provided, Open iT may act as a processor on behalf of the customer, while the customer typically acts as controller.

Where a company licenses Open iT software for its own environment, that company is generally responsible for determining the purposes and means of processing and for ensuring that an appropriate lawful basis and transparency framework are in place. Open iT is designed to support GDPR-aligned implementation, including data minimization, access controls, and security oriented configuration options.

In practice, Open iT is typically one component of a broader privacy and compliance framework that customers already maintain for their IT environment and workforce data processing activities.

As with most enterprise systems, software and infrastructure environments generate technical records such as system logs, authentication events, and usage-related telemetry. Such information is commonly used to operate, secure, troubleshoot, and administer IT environments.

Open iT differs in that it collects, processes, aggregates, and reports on usage-related data in order to help customers understand software utilisation, support license optimisation, and improve IT asset management.

“So Is Your Software GDPR-Compliant?”

- There just is no such thing as GDPR compliant software. Open iT – like any application, network or operating system - collects data of how individual users interact with IT systems. It is you – as a Data Controller – that needs to be GDPR compliant.
- In the default installation of Open iT a person with login access to the Open iT portal will see actual user names in generated reports. There is no breach of GDPR compliance if the company has a legitimate business interest in doing so.
- If you are of the opinion that access is not in line with company privacy policy, you have three easy options to mask user names;
 - **data anonymization**
 - at the collection level (irreversible)
 - at the processing level (partly reversible, but where reprocessing is needed)
 - or at the reporting interface level (reversible),
 - in addition to **role configuration** (different login users can only see a subset of usage data).

© 2026 Open iT, Inc. All rights reserved. Company Confidential.



FIGURE 1: Is Open iT software GDPR compliant?

When is processing of personal data of employees allowed?

To use Open iT Software in a GDPR-compliant manner, the customer should ensure that an appropriate governance framework is in place, including a lawful basis for processing, employee facing privacy information where required, access controls, retention rules, and internal use limitations.

GDPR Art. 6: Lawfulness of processing (of personal data)

Processing shall be lawful only if and to the extent that **at least one** of the following applies:

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

© 2026 Open iT, Inc. All rights reserved. Company Confidential.



FIGURE 2: GDPR Art. 6 When is it lawful to process personal data

Article 6 GDPR sets out the legal bases on which processing of personal data may be lawful. In employment-related contexts, particular attention is commonly given to legal obligation and legitimate interests. Consent should be relied on with caution because, in many employer employee relationships, it may not be considered freely given. Only one valid legal basis is required for a specific processing purpose, but that basis must be assessed and documented in light of the actual use case.

6 a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes. Consent may be relied upon only in limited circumstances. In an employment context, consent is generally not considered freely given, and other legal bases such as legitimate interest or legal obligation are typically more appropriate.

6(c) Processing is necessary for compliance with a legal obligation to which the controller is subject. This legal basis may apply where the customer must process certain user-related information in order to comply with binding legal or regulatory requirements. It would not ordinarily apply merely because a contract with a software vendor refers to named users or usage based pricing.

In many Open iT use cases, the more relevant legal basis is likely to be legitimate interests, subject to a documented assessment of necessity, proportionality, and the impact on the rights and freedoms of the affected individuals.

6(f) Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

Legitimate interests is not a blanket basis for employee monitoring. It should be used only where the purpose is lawful, clearly identified, and real; the processing is necessary for that purpose; and a balancing test shows that the organisation's interests are not overridden by the rights and freedoms of the data subjects. In employment settings, that assessment should be undertaken with particular care.

Depending on the customer's environment and documented assessment, examples of potentially legitimate purposes may include software asset management, license optimisation, internal cost allocation, capacity planning, security administration, and related operational analytics.

The proportionality analysis will depend on the categories of data collected, the level of identifiability, the scope of access, the transparency provided to employees, and the safeguards implemented to reduce privacy risks.

By contrast, uses that are intrusive, excessive, or unrelated to a clearly defined business purpose may not be justified. For that reason, customers should define clear internal rules regarding permitted use, access rights, and escalation procedures before using identifiable employee data in reports or analyses.

What data does the Open iT Software monitor and how is it done?

Open iT would like to clarify the categories of information that may be collected by its solutions in light of applicable data protection requirements. The description below refers specifically to LicenseAnalyzer Levels 1, 2, and 3.

Open iT uses a five-layer client-server architecture designed to support security, performance, and scalable reporting. Data may be collected from sources such as software license managers, operating system components, network services, application-level signals, and other configured system metrics. At defined intervals, relevant data is transferred to an Open iT data store for reporting and analysis at the configured level of granularity.

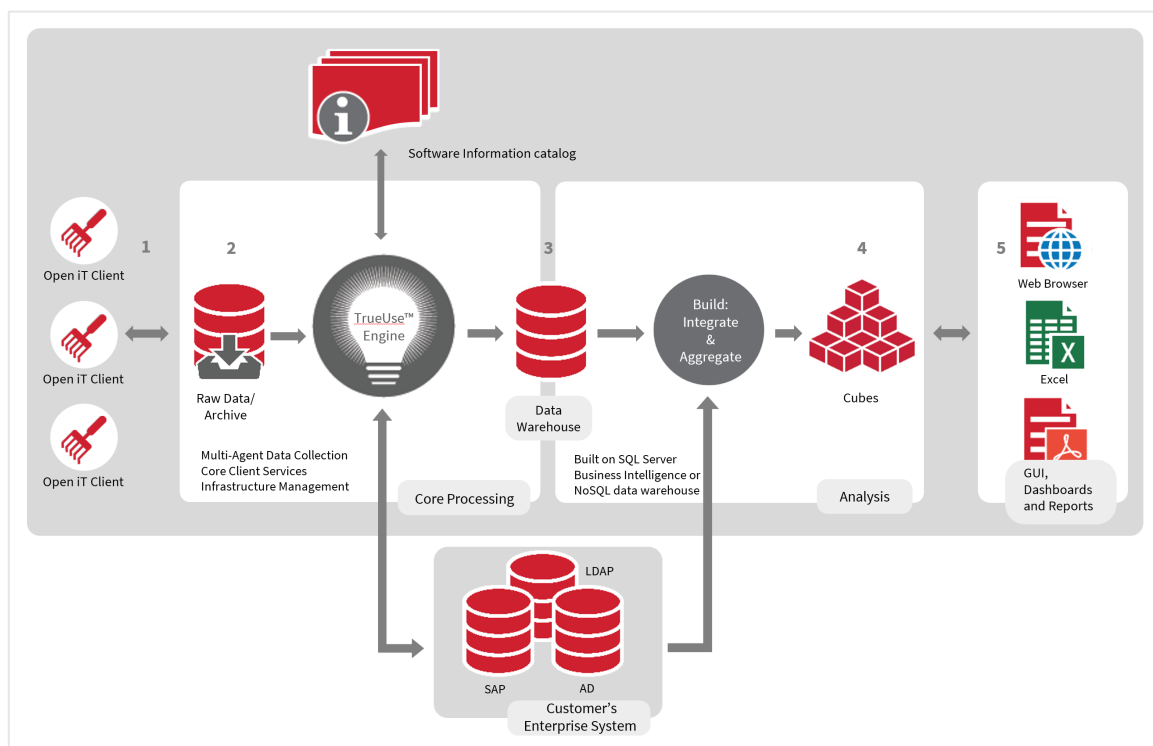


FIGURE 3: Open iT Software Five-Layer Architecture

LicenseAnalyzer Level 1 data is derived from feature usage information collected from the license manager, such as licence check-out and check-in timing, log files, licence files, and *lmstat* output.

LicenseAnalyzer Level 2 and 3 uses keyboard and mouse activity solely to detect application usage for licence optimisation purposes and only for explicitly configured applications. It records event counts, such as the number of keypresses or mouse clicks, but does not record the actual content of keystrokes. This event data is used to distinguish active from inactive usage for threshold tuning and reporting.

In addition, this activity data is processed in memory on the user workstation, and only aggregated event counts are transmitted to the Open iT Core Server. As a result, the database does not store raw keystrokes or raw mouse-click content.

How Open iT addresses customers concerns about Personal Data

We recognize that customers may have questions about the interpretation of lawful bases under the GDPR, including legitimate interests, as well as about employee privacy rights and appropriate safeguards.

Open iT implements appropriate technical and organizational measures in accordance with Article 32 GDPR, including:

- role-based access control and authentication mechanisms
- encryption in transit and, where appropriate, at rest
- system logging and monitoring
- incident detection and response procedures
- data minimization and access restriction controls
- regular security reviews and updates”

Open iT provides both anonymization and pseudonymization capabilities. Where data can be re identified, it is considered pseudonymized personal data and remains subject to GDPR. Only irreversible anonymization removes data from the scope of GDPR.

Open iT includes functionality that can reduce identifiability of user data at different stages of collection, processing, and reporting. Depending on configuration, these measures may constitute anonymization or pseudonymization. Where re-identification remains possible, the data remains personal data and continues to be subject to GDPR requirements.

Open iT provides three main configuration approaches that can enhance privacy protection:

At the data collection level: If configured accordingly, personal data can be transformed at the point of collection. Where that transformation is irreversible and individuals are no longer identifiable, the resulting data may be considered anonymized. For example, reports may display generic labels such as user1 or user2, or other non-identifying values.

At the data processing level: Personal data can also be transformed after collection but before aggregation and reporting. Where re-identification remains possible through additional information or reprocessing, this would generally be regarded as pseudonymization rather than anonymization.

At the data reporting level: Personal data can also be masked at the reporting layer. Because this approach is typically reversible, it should generally be treated as a form of pseudonymization or access restriction rather than irreversible anonymization.

Restrict access to reports with end user data

Users who generate reports in Open iT must authenticate with their assigned credentials. Access to personal data can therefore be limited to individuals whom the customer has expressly authorized to generate or review reports in the Open iT application.

It is also possible to apply more granular restrictions to the generation and viewing of reports, including access controls for particular datasets, report folders, or specific reporting outputs.

These controls can be configured so that an authorized user can access only the data relevant to a defined business unit, application set, geography, or other approved scope. This supports purpose limitation and need-to-know access principles.

This functionality is supported within Open iT Software and can be enabled as part of the customer's implementation. Likewise, scheduled reports may be distributed to defined recipients under customer-controlled permissions and security settings.

Open iT also supports techniques that enable customers to apply protected transformations to usernames so that only persons with access to the relevant key or mapping information can re-identify the underlying user. In most cases, this should be treated as pseudonymization rather than anonymization.

Aggregate or pseudonymize end-user data in group reporting

Another approach is to report data in aggregated form across groups of individuals. Aggregation can reduce privacy risk, but GDPR may still apply where individuals remain directly or indirectly identifiable. The legal assessment should therefore focus on the practical risk of re-identification in the relevant context.

For example, reporting can be structured around groups such as department, location, or profession, with additional measures to reduce identifiability within the group. Customers should determine appropriate minimum group sizes and other safeguards based on their own risk assessment, legal requirements, and internal policies.

Open iT as Software as a Service (SaaS) in a cloud environment

Where Open iT Software is deployed as SaaS in a cloud environment, the parties should ensure that appropriate data processing terms are in place and, where personal data is transferred outside the EU/EEA, that a valid transfer mechanism is used. Depending on the circumstances, this may include an adequacy decision, the European Commission's Standard Contractual Clauses, and any supplementary measures required by law.

If Open iT provides the software SaaS, the relevant cloud provider's technical and organizational controls will also form part of the overall compliance picture. Customers should assess hosting locations, remote access arrangements, subcontracting, and the provider's published privacy and security documentation as part of their transfer and vendor-risk review.

For convenience, links to AWS and Microsoft Azure privacy resources are included below.

<https://aws.amazon.com/compliance/data-privacy-faq/>

<https://azure.microsoft.com/en-us/overview/trusted-cloud/privacy/>

Conclusion

All software applications leave information about users such as when they log in, when they log out, and if a checked out application is in active use or not.

Article 6 GDPR sets out an exhaustive list of lawful bases for processing personal data. In the context described in this paper, the most relevant legal bases will often be legitimate interests and, in some cases, legal obligation or contractual necessity, depending on the specific processing purpose and the customer's role and obligations.

Access to the Open iT portal and to reports containing user-related data can be restricted through authentication, role-based permissions, and scoped reporting rights. This enables customers to limit visibility to authorized personnel and approved use cases.

Open iT maintains data processing agreements with its customers and intra-group entities where required. These agreements define the roles and responsibilities of each party and incorporate appropriate safeguards, including where applicable the European Commission's Standard Contractual Clauses.

If further privacy protection is required, Open iT supports measures such as anonymization (where irreversible), pseudonymization, aggregation, and role-based access restrictions. These measures may be applied at the collection, processing, or reporting stage, depending on the customer's implementation choices and compliance requirements.