LOGPOINT

GDPR and the protection of SAP data

www.logpoint.com

EXECUTIVE SUMMARY

The implementation of the General Data Protection Regulation (GDPR) in May 2018 revolutionized how businesses, both inside and outside the European Union (EU), trade, protect, and handle sensitive data. GDPR compliance is not optional, and companies that do not handle personal data correctly may face severe punishment such as fines and risk the reputation of their business and the loyalty of their customers.

The almost constant increase in cybercrime is making the task of achieving GDPR compliance even more difficult with 90% of cyberattacks being financially motivated. Therefore, preventing unauthorized access to data such as personal information or corporate intellectual property is of paramount importance, not only from the outside but also from the inside of businesses. To effectively protect this data, organizations need to understand where it resides, who has access to it, and how to monitor what is happening to it.

As a huge amount of the world's corporate data sits within an SAP® system, that is a great first place to start when looking at the protection of that data. So how can SAP systems be exploited, how can this be monitored, and what does it mean for organizational compliance and GDPR strategy?

SAP contains vast amounts of GDPR-relevant data that requires protection to meet compliance

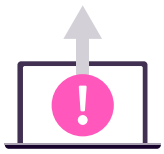
The protection of corporate intellectual property is becoming more and more important in times of cybercrime. **Intellectual property (IP) is stored in the IT systems of companies.** Networks and IT systems today need comprehensive protection, this remains an eternal race against ever-new vectors of attack. In addition to the intellectual property of companies, personal data is another important area of sensitive data. These must not only be protected against unauthorized access from the outside but also from within the company. **The Verizon DBIR report 2021 estimates that 85% of breaches involve a human element and 61% of breaches involve valid credentials.**

When looking at the use of SAP systems, different industries and countries store data in a multitude of different ways, so it is useful to understand the types of data that can reside in SAP and examples of how they can be misused.

Areas like hospitals need to protect access to patient data, financial institutes, and insurance companies, as well as – critical infrastructure organizations need to protect sensitive data from unauthorized access. Below are some examples and scenarios.

Government: Social Security/National Insurance Number

Government agencies often store social security numbers in an SAP system. These systems are therefore often targeted for misuse, with unauthorized access to one system potentially leading to a mass breach of highly valuable social security numbers. The consequences of this can be catastrophic and potentially life-changing for victims if this information is extracted from an SAP system.



Government: Tax evaders

Tax authorities carry information about tax evaders in SAP systems and employees of the tax authorities specialists are instructed to work with the SAP data in a confidential and restrictive way. Nevertheless, SAP allows to use data search and provides input help for search fields with wildcard symbols, which can return result lists without restrictions on data access. For example, loading the entire list of tax evaders available in the system. Exporting this list is a simple process. The delivery of a similar list to the press with information about high-status tax evaders is a conceivable, already reported incident.

Finance: Salaries and pensions

Information regarding salary or pension payments are very familiar pieces of data to have in an SAP system. An example could be this. Information regarding salary or pension payments to ex-employees has been printed and either left at those machines or left in kitchens on purpose.

Of course, sensitive data requires confidentiality. A print-out itself is already a violation, and the disclosure of such data is certainly abuse and often is motivated by a corporate policy background. The questions that need to be asked are:

- Who had access to this information?
- Which accounts have been accessed in the last few days?
- And. Who printed the data – and why?

HR/Operations: Job changes

Job rotation is a welcome and standard part of most thriving companies, but rotation can lead to inefficiencies. Over time, employees may hold different positions in multiple business units or departments. It is questionable whether the SAP accounts and authorizations of these employees are always adjusted accordingly, or whether the new roles are simply added, and the old ones never removed. It could be that changing an employee from HR to the Legal Department yields interesting combinations of entitlements, and that old SAP roles are still being used to access sensitive data by persons who should no longer have that access.

The challenges in the logging infrastructure of SAP and the risk of a GDPR compliance failure

The above-mentioned cases and scenarios are examples of potential or actual real cases for **GDPR compliance failure**. The Data Protection Act of the EU underpins the importance of protecting personal sensitive data and foresees penalties for non-compliance or failure to enforce protective measures in the handling of personal data.

With the introduction of the General Data Protection Regulation (GDPR), data privacy and protection become a vital topic for SAP systems. This covers the need to ensure compliance by managing access, consent management, data and information life cycle management and the protection of sensitive data.

Data Privacy & Protection of sensitive data has two aspects. First, it is about preventing access by establishing role-based access control (RBAC) and **segregation of duties (SoD)**, making sure that only authorized accounts can access the relevant data. Second, it is about establishing automated and continuous monitoring of access to data to identify unauthorized access, and potential data breaches as well as to react to breaches as soon as possible utilizing Security Orchestration, Automation, and Response (SOAR).

The monitoring of access to personal data is key to fulfilling requirements in GDPR and reducing the number of incidents such as the ones listed above, but what is the best way of **monitoring access** in an SAP system?

A vital component under GDPR is the logging of read access to sensitive data. Deciding the best way to implement this can provide an SAP security challenge while raising several questions such as:

- Where is personal data stored in an SAP system?
- By what means is access to personal data possible?
- Which SAP logs are monitoring access to personal identifiable information?
- How to configure SAP for such monitoring?

The challenge - classic SAP logs do not provide the necessary evidence in the event of suspicion

Classic logging in SAP is lacking the details required to monitor precisely and efficiently and, at the same time, provide the necessary evidence in the event of suspicion. While SAP has a logging infrastructure, the following log types do not suffice to fit the criteria for GDPR compliance:

SAP Security Audit Log

The SAP security audit log is not explicit and precise enough to trace the access to personal identifiable information. It is not logging at the required field level (e.g. access to salary information, address data, social insurance number). Furthermore, the security audit log may not be activated entirely for all audit classes or all possible activities for all users in the landscape.

SAP „STAD" data

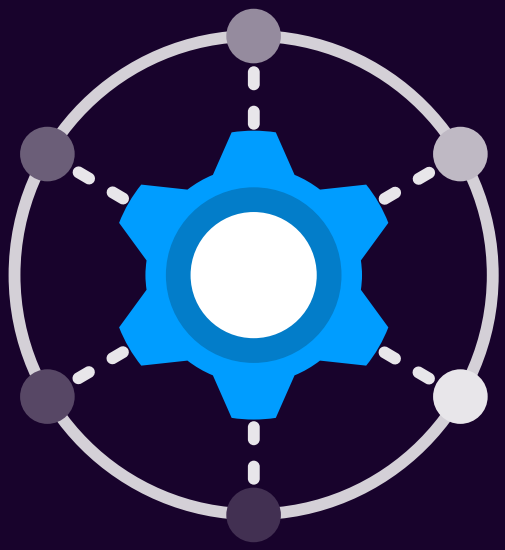
SAP STAD logs which transactions users have accessed, but unfortunately SAP transaction usage does not provide evidence of what fields have been accessed. Therefore, it is also too high-level for detecting the relevant pieces of activities and leaves critical areas uncovered.

Database audit trail

The database audit trail logs database layer access via database administrator tools, **such as the SAP HANA cockpit**. Usually, only database administrators have direct access. Therefore, logging is recommended. The logging of SAP technical application access via the sidadm account, is not efficient in terms of data volume and performance. An audit trail can log SQL queries, but monitoring is inefficient and imprecise.

The way out - advanced access monitoring in SAP that can give evidence

Separate from the logging methods, SAP provides a powerful log source called SAP Read Access Log for precise and efficient monitoring of access to sensitive data. This is the only log source in SAP that protocols on the application layer on a field level, who has accessed what field respectively or a piece of information in SAP, in read or write access mode.



SAP Read Access Log – pros and cons of the SAP standard

SAP Read Access Logging shows how to get a grip on logging access to personal data. The read access log has essential advantages over the classic security logs from SAP. However, the RAL requires manual configuration efforts and gives organizations the following challenges: Extensive configuration and missing centralized log management and monitoring capabilities.

Extensive configuration as a pre-requisite

The configuration of SAP Read Access Log is very time-consuming and not at all trivial. Upfront it requires knowledge regarding:

- Where is the relevant and personal data stored in SAP?
- What is GDPR relevant?
- How do SAP teams configure the RAL?
- Which transactions, input, and output fields on SAP screens are important for logging?

Missing monitoring capabilities

Once SAP RAL logs are in the system, the next challenges will occur

- How can SAP teams extract, manage and retain the logs? From all relevant systems in the landscape? (Log retention)
- What is the best way to evaluate the log? (analysis)
- How can automated monitoring be achieved, and an alarm be generated?

Those last points present organizations with unsolvable tasks in the SAP standard.

Logpoint BCS for SAP – unlocking the full potential of SAP Read Access Log

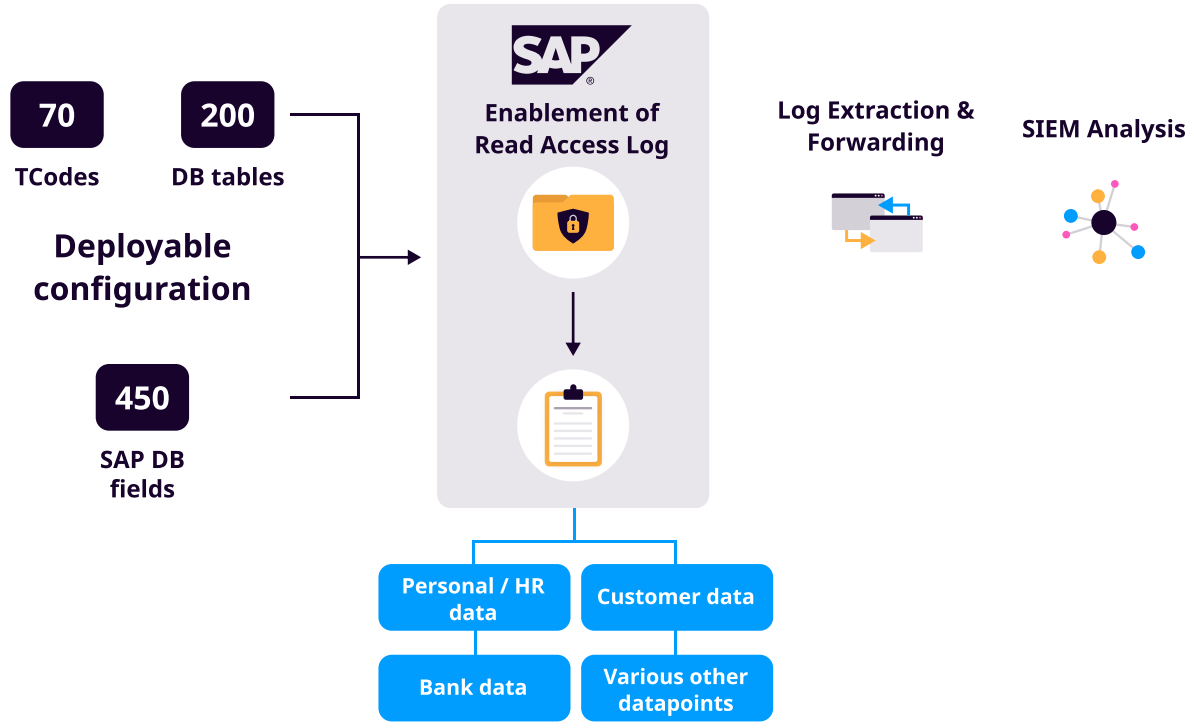
Logpoint took on the challenges in the area of SAP Read Access Logs and worked on a comprehensive value proposition. How to configure Read Access Log for customer systems by providing an SAP transport to activate the Read Access Log with a special focus or filter: Logging access to personal data.

Logpoint also provides solutions to continuously extract the read access log and forward the logs to the SIEM - for central monitoring of all RAL logs of the entire SAP system landscape, for storage and retention (log management), as well as for continuous, automated monitoring. In the Logpoint search templates, there are filtering options on RAL logs that are not available in SAP (RAL monitor) today.

Deployable configuration of SAP RAL – activate logging on a mouse-click

Logpoint BCS for SAP offers crucial value by activating the Read Access Logs via Logpoint customizing, enabling SAP systems to log access to personally sensitive information.

SAP systems do not have such a customizing of RAL out-of-the-box. The solution provides a deployable configuration for our SAP customers that enables the RAL to log application access to more than 450 fields that are stored in more than 200 database tables which are accessible via more than 70 transaction codes – giving access to personal data. Not only dialog access via SAPGUI is logged, but also the technical accounts' access (e.g. RFC, OData, Web UI) For example, accessing employee data in SAP ERP HR from SAP SaaS solution Success factors.



In SAP, centralized log management and monitoring are not possible. Monitoring the RAL through a comprehensive logging solution like a **security information and event management (SIEM)** system is the answer.

Merging SIEM and SAP for thorough SAP monitoring

By introducing a SIEM solution to SAP, the SIEM at first takes care about the topics continuous log extraction from SAP, storage and retention (log management). Second, the SIEM centralizes the monitoring of SAP logs taken from the entire SAP landscape. And the data can be analyzed in a continuous, automated, holistic way. And third, an automated alerting can be used to immediately inform and respond to security issues.

The Read Access Log information can not only be monitored on its own, but also in cross-correlation with other log sources that are available in the SIEM, taken from all kinds of security or network devices such as firewalls, VPN, email gateways, to name only a few. Access and download of sensitive information can then be tracked, when this information is leaving the organization via an email gateway, sent to a private email account or being put on a USB stick.

This cross-correlation of several security and network devices and SAP is a major benefit in the monitoring of SAP, providing SAP monitoring a far greater context than a classic, SAP-centric monitoring solution could achieve.

This is only possible in a SIEM, where you have the holistic view of SAP and an organization's entire security operation.

End-to-end value proposition – helping to meet GDPR compliance

The configuration of Read Access Log in SAP with the aspect access to personal information, the continuous extraction of logs and the automated evaluation of the Read Access Log provide an essential, end-to-end monitoring solution for SAP Read Access Logs and represents an essential element of SAP security monitoring, particularly for GDPR compliance – from the creation of logs in SAP, data extraction, collection and monitoring with appropriate rules in SIEM.

Introducing Security for Business-Critical Security - Complexity in security

Business-critical systems are the heartbeat of an entity. They house all the data that is vital to ensure that a company or organization runs as smoothly and efficiently as possible, and so that data and those systems need protecting. Some systems are easier to defend than others, take an SAP system for example. It houses a wealth of data, but is not friendly towards integrating with security solutions, for that it needs something extra.

SAP is not designed to send security-relevant information to a SIEM system. To address this crucial issue, we conducted an in-depth technical breakdown of SAP and created a bridging technology that integrates SAP into a SIEM system, called BCS for SAP.

The solution extracts a broad set of security, audit, and compliance-related information from SAP system and sends the data to the SIEM. In addition, the system provides additional SAP security intelligence with a set of rules that listens to the incoming SAP information and analyzes the data.

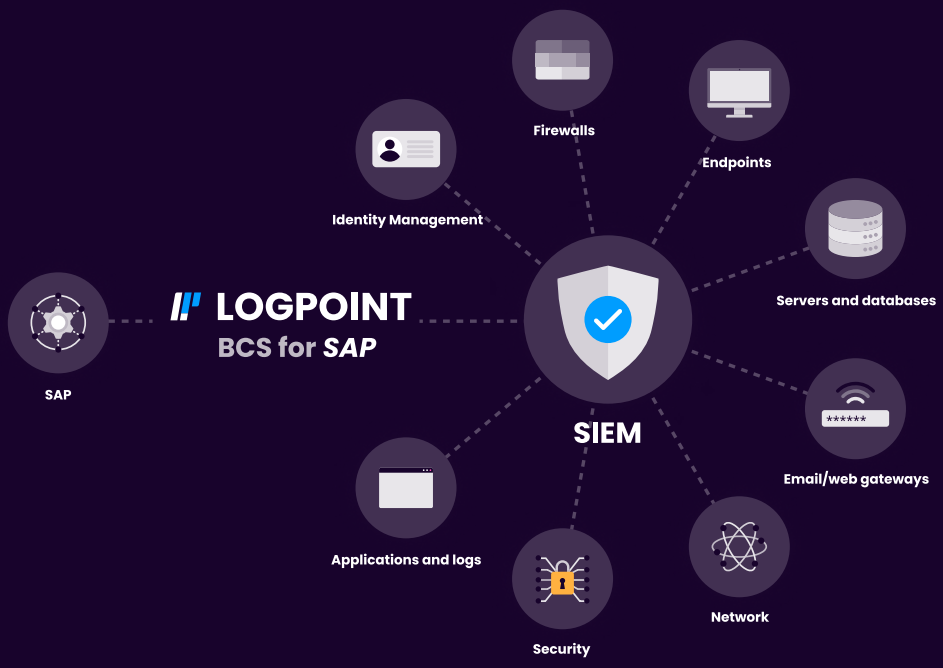
BCS for SAP continuously extracts and transfers the SAP RAL information into the SIEM providing automated analysis and log management of the SAP data. These benefits include:

- Continuous extraction and transfer of SAP RAL information into SIEM
- Automated analysis of SAP RAL information in near real-time
- Log Management of SAP RAL Information
- Additional capabilities for after-the-fact log analysis and forensic analysis
- Cross-correlation of SAP data with IT Security data and events

The Solution

SAP SIEM / log management integration

- Continuous extraction and transfer of SAP RAL information into SIEM
- Automated analysis of SAP RAL information
- Log management of SAP RAL information (storage for months and years)
- After-the-fact log analysis and forensic analysis
- Cross-correlation of SAP data with IT security data and events



BCS FOR SAP IN ACTION

The following visualizes the result of Read Access Log monitoring in SIEM.

Use case example - detection of access to salary information by unauthorized user group outside HR

Let's assume, a high-privileged account (firefighter, maintenance user) misuses the given authorizations to access transaction PA20 for the access to personal sensitive information like salary information.

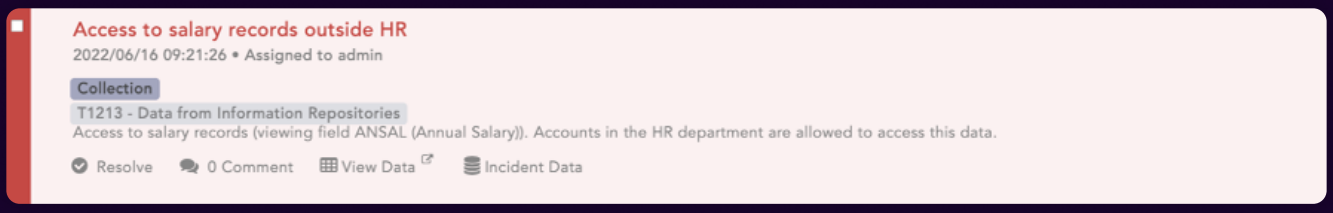
Classic monitoring via SAP security audit logs might only give evidence that the firefighter account was accessing PA20. The necessary evidence of accessing the technical filed "ANSAL" (Annual Salary) is not logged. Therefore, no clear proof of access will be possible.

The Logpoint customizing of SAP Read Access Log enables a log being created that proofs the access to this field. Giving also the context of what employee number record has been accessed, by what terminal (workstation), when exactly on which SAP system and SAP Client, and more.

Automated alerting – immediately inform and trigger response action

In SIEM, the relevant alert rule is implemented and will trigger immediately, when the log is received by the SIEM system.

The alert rule triggering, a Logpoint Incident can then forward the Incident data via email, can create a ticket in a ticketing system, or trigger automated security response playbooks in our Logpoint SOAR.

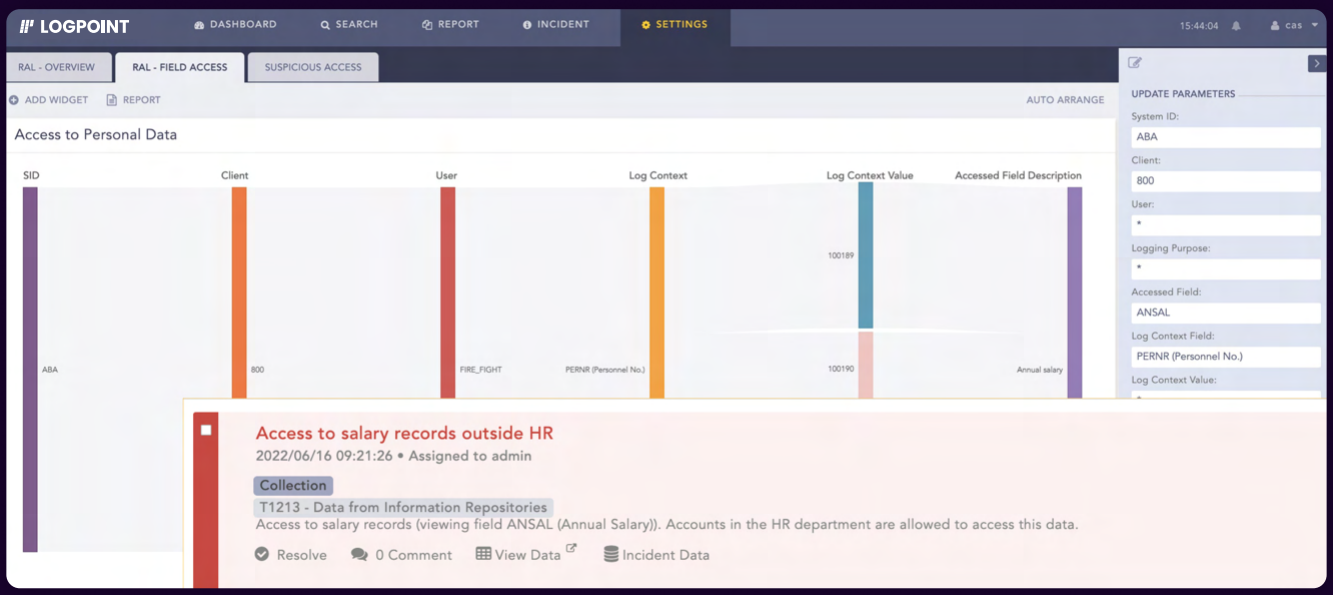


Log analysis in Logpoint Search Template for RAL – the next-gen RAL monitor

In BCS for SAP, log analysis looks completely different than in the “SAP RAL manager”. The log analysis in Logpoint is both user-friendly and high performing.

The diagram below shows a Logpoint Search Template for Read Access Logs. On the right side one can see input fields (filter parameters) that can be used to search for certain logs and data:

- SAP System Id
- SAP Client
- SAP User account
- RAL Logging Purpose
- Accessed field (technical field name: e.g. ANSAL)
- Log Context Field (RAL Log Context, e.g.: PERNR – Personnel No.)
- Log Context Value (e.g. a specific employee number)
- ... others possible



CONCLUSION

The monitoring of access to personal data in an SAP system is key to fulfilling requirements in GDPR, however, it remains a security challenge in many organizations. The SAP Read Access Log provides a means for SAP users to log access to sensitive data, however, when monitoring the RAL through a SIEM solution, you can get a holistic view of SAP and the organization's entire infrastructure. As SAP is not designed to send relevant information to a SIEM solution, BCS for SAP provides a bridging technology that integrates SAP into the SIEM solution, helping to fulfill the regulatory compliance requirements of GDPR or supplementing an organization’s GDPR strategy.

ABOUT LOGPOINT

Logpoint is the creator of a reliable, innovative cybersecurity operations platform — empowering organizations worldwide to thrive in a world of evolving threats.

By combining sophisticated technology and a profound understanding of customer challenges, Logpoint bolsters security teams' capabilities while helping them combat current and future threats.

Logpoint offers SIEM, UEBA, and SOAR technologies in a complete platform that efficiently detects threats, minimizes false positives, autonomously prioritizes risks, responds to incidents, and much more.

Headquartered in Copenhagen, Denmark, with offices around the world, Logpoint is a multinational, multicultural, and inclusive company.

For more information visit **www.logpoint.com**