



Einsatz von ObservelT nach deutschem Datenschutz

FAQ für den Betriebsrat

Bei der Einführung von ObservelT in Unternehmen muss Bedenken des Betriebsrates oder der Mitarbeiter Rechnung getragen werden. Bei diesen Bedenken stehen Aspekte des Datenschutzes und der Sicherheit im Vordergrund.

Fragen / Einwände

- „Fehler werden immer gemacht, und es ist nicht das Ziel, jeden Fehler eines Benutzers zu erfassen!“
- „Welche Gesetze erlauben die Protokollierung von Anwendern?“
- „Der Überwachte muss wissen, dass er überwacht wird.“
- „Es muss eine klare Trennung zwischen Produktion und Arbeitsplatz bestehen.“

Antworten

- Es werden nur die notwendigen Benutzeraktivitäten protokolliert und entsprechend des Datenschutzgesetzes unter Einbeziehung des Betriebsrates benutzerbezogen ausgewertet.
- Es gibt kein Gesetz, welches die Protokollierung von Anwendern pauschal erlaubt. Um eine Protokollierung von Benutzereingaben zu ermöglichen, muss ein Vertrag mit der Genehmigung, z. B. beim externen Dienstleister, oder eine Betriebsvereinbarung vorhanden sein.
- ObservelT ermöglicht eine breite Palette an Möglichkeiten, um den Anwender darauf hinzuweisen, dass seine Tätigkeiten protokolliert werden.
- Es kann ausgeschlossen werden, dass Screenshots oder Metadateninformation von kritischen Daten, z. B. privaten E-Mails oder privaten Kreditkarteninformationen, gespeichert werden.

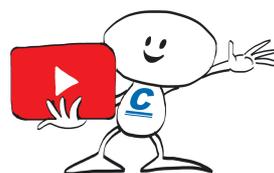
Fragen / Einwände

- „Transparenz ist wichtig.“
- „Keine Protokollierung und Überwachung ist für die Ewigkeit.“
- „Wer überwacht den Überwacher?“
- „Welche Datenschutzgesetze betreffen ObservelT?“
- „Die Hemmschwelle zur Protokollierung von internen Mitarbeitern ist unendlich hoch.“

Antworten

- Es ist für den User jederzeit möglich zu erfahren, was gespeichert wurde (vgl. § 34 BDSG), wer ObservelT konfiguriert oder Zugang zu seinen protokollierten Aktivitäten hat.
- Der Sinn der Protokollierung von Benutzern und Maschinen muss regelmäßig überprüft und mit allen Beteiligten abgestimmt sein. Eine Vorratsdatenspeicherung ist nicht vorgesehen und erlaubt (vgl. §3a BDSG).
- Sämtliche Konfigurationsaktivitäten – auch die der hochprivilegierten Nutzer – werden durch ObservelT protokolliert und stehen anderen SIEM-Tools, wie z. B. Splunk, zur Verfügung. Weiterhin besteht die Möglichkeit, eine E-Mail-Benachrichtigung bei bestimmten Benutzeraktivitäten zu verschicken.
- Es sei auf §1-11 sowie §32-35 des BDSG verwiesen. Im Besonderen seien §4 Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung, §9 Technische und Organisatorische Maßnahmen und §35 Berichtigung, Löschung und Sperrung von Daten erwähnt.
- Durch eine sich verändernde Rechtslage (z. B. IT-Sicherheitsgesetz, BSI, BaFin) und sich verändernde Compliance-Anforderungen (PCI etc.) müssen Unternehmen Wege finden, ihre internen Mitarbeiter für eine Überwachung zu sensibilisieren. Die Überwachung dient dem Schutz des Unternehmens und somit auch dem Schutz des Arbeitsplatzes. ObservelT ist nur die technologische Lösung; die Sensibilisierung erfolgt rein über offene und rechtzeitige Aufklärung der betroffenen Mitarbeiter.

Wünschen Sie weitere Unterstützung rund um das Thema Betriebsrat und Betriebsvereinbarung?



Sprechen Sie uns an:
info@consist.de