Erweiterte Protokollierung für die Arbeitszeiterfassung

Einleitung

Das System der TSI bietet umfangreiche Funktionen, um eine digitale Arbeitszeiterfassung zu realisieren, insbesondere in Anwendungsszenarien mit häufigen Standortwechseln der Mitarbeiter oder Außeneinsätzen, bzw. Mischformen mit festen Mitarbeitern an einem oder mehreren Standorten, sowie standort-wechselnden Mitarbeitern oder Außendienstlern.

Dabei geht das System weit über eine reine Erfassung hinaus und bietet auch zahlreiche Varianten zur Dateneinsicht, zusätzlichen Dateneingaben, Datenkorrekturen sowie zahlreichen Auswertungen und Analysen, die nicht Schwerpunkt dieses Dokuments sind. Da in verschiedenen Fällen personenbezogene Daten erfasst werden, gilt es diese besonders zu schützen, was durch eine vielfältige Ausgestaltung und Einsatzweise des Systems eine Herausforderung sein kann.

TSI Telematic Services GmbH
Rudower Chaussee 29
12489 Berlin

Deutsche Bank
IBAN: DE52 1007 0024 0709 4667 00
BIC: DEUTDEDB

Geschäftsführer: Nico Baumgarten
USt-ID-Nr.: DE 25 11 92 601
HRB: 10 43 46 B Amtsgericht Charlottenburg

T: +49 (30) 6392 6155
F: +49 (30) 2218 5015
E: info@tsi-telematic.com

Datenschutzkonformer Einsatz

Die aktuell in Kraft getretene Datenschutzgrundverordnung (DSGVO), aber auch deren rechtliche Vorgänger, wie das Bundesdatenschutzgesetz, haben schon immer hohe Anforderungen an die Verarbeitung personenbezogener Daten gestellt und wurden in der Konzipierung und Entwicklung der Arbeitszeiterfassungsfunktionen des TSI Systems beachtet, womit ein datenschutzkonformer Einsatz des Systems grundsätzlich gewährleistet ist.

Das System ist über die Zeit gewaltig gewachsen und bietet mittlerweile zahlreiche Komfortfunktionen, aber auch alternative Eingabevarianten, sowie delegierte Zugriffs-, Eingabe- und Änderungsprivilegien, die neue Herausforderungen an den Datenschutz und insbesondere bei den Dokumentationspflichten mit sich bringen.

Die Erweiterte Protokollierung ermöglicht dabei nicht nur die Daten selbst zu erfassen, sondern auch jegliche Eingaben oder Änderungen am System detailliert zu protokollieren und den Ursprung aller Daten nachvollziehbar und beweissicher zu gestalten.

Wann ist eine Erweiterte Protokollierung angeraten?

Die Erweiterte Protokollierung, welche Ursprung und Details zu Eingaben und Änderungen detailliert festhält ist insbesondere dann angeraten, wenn:

- Daten aus nicht manipulationssicheren Quellen stammen,
- Häufiger Bedarf für Datenänderungen besteht bzw. Änderungen ohne geregelten Prozess möglich sind,
- mehrere/viele Nutzer Daten ganz oder teilweise ändern dürfen,
- das System nicht nur für die reine Erfassung/Digitalisierung, sondern bspw. auch (direkt) für die Lohnabrechnung verwendet wird,
- zusätzliche Dokumentationspflichten bestehen.

Manipulationssichere/nicht manipulationssichere Datenquellen

Die Arbeitszeiterfassung beruht in jeder Variante darauf, dass Statuswechsel von Mitarbeitern, also beispielsweise von Arbeitszeit zu Privatzeit, erfasst werden. Dies ist technisch auf verschiedene Weisen möglich.

iButtons, RFID, Mitarbeiterkarten

Zu den manipulationssicheren Varianten dabei zählen Einsatzszenarien, bei denen Mitarbeiter iButtons, RFID-Chips oder Mitarbeiterkarten sowie die dazugehörigen Lesegeräte, welche in der Regel von der TSI geliefert werden, nutzen. Hierbei werden die technischen Geräte zur Erfassung durch das Unternehmen, bzw. durch die TSI kontrolliert, wodurch eine Manipulation bzw. eine unentdeckte Manipulation nicht möglich ist. Diese Systeme haben aber keine oder nur eine sehr eingeschränkte Möglichkeit erfasste Daten zu visualisieren und ermöglichen z.B. keine direkte Einsicht in die erfassten Daten für die Mitarbeiter.

Smartphones

Die Erfassung der oben genannten Statuswechsel durch ein Smartphone ist ebenfalls möglich und liegt im Trend, insbesondere, weil es hier leicht ist zusätzliche Komfortfunktionen zu ermöglichen, wie zum Beispiel eine direkte Dateneinsicht für die Nutzer oder Mitarbeiter.

Das Problem bei Smartphones ist, dass diese heutzutage nicht, nur eingeschränkt oder nur mit hohem Aufwand durch das Unternehmen zu kontrollieren sind und somit grundsätzlich nicht als vertrauenswürdige Datenquelle dienen. Besonders das sehr offene Mobilsystem Android (und dessen Ableger) sind sehr leicht und kaum überprüfbar zu manipulieren. Als Beispiel, sei hier die

Standorterfassung genannt, die durch den Nutzer selbst nicht nur leicht abgeschaltet, sondern auch mittels zahlreicher Apps und Optionen beliebig überschrieben werden kann – Nutzer können so leicht vorgeben an einem anderen Ort zu sein.

Verschärft wird das Problem bei der Nutzung von privaten Endgeräten (BYOD-Konzepte), die zwar insbesondere für das Unternehmen kostengünstig sind, aber schwierige Herausforderungen mit sich bringen – nicht nur durch die Vielzahl der Hardwarevarianten und deren sehr unterschiedlich unterstützten Funktionen, sondern auch bei der Provisionierung der nötigen Applikationen und der Absicherung des Gerätes gegen unbefugte Zugriffe oder bösartige Software (Viren, Trojaner, etc).

Demgegenüber stehen zusätzliche Optionen nicht nur im Komfortbereich, sondern auch Möglichkeiten für erweiterte Funktionen, wie zusätzliche Daten oder Zusatzinformationen zu erfassen, Korrekturen oder Ergänzungen an Daten vorzunehmen und primäre Eingabeprüfungen an (z.B. Teamleiter) zu delegieren – und dass auch ohne einen traditionellen Computer-Arbeitsplatz.

Dadurch kann ein Einsatz grundsätzlich „nicht manipulationssicherer“ Smartphones für die Arbeitszeiterfassung durchaus gerechtfertigt sein, auch wenn dies ein Maß an Vertrauen gegenüber den Mitarbeitern voraussetzt.

> *Grundsätzlich möchten wir noch darauf hinweisen, dass ausnahmslos jedes System manipuliert werden kann. Es gibt aber qualitative und praktische Unterschiede, insbesondere dabei, wieviel Aufwand betrieben werden muss, damit eine Manipulation möglich wird und diese auch nicht im System automatisch oder durch andere Nutzer entdeckt wird. In diesem Fall zählen wir zu den manipulationssicheren Systemen jene, wo der nötige Aufwand für eine Manipulation sehr hoch ist und im Regelfall nicht zu erwarten ist, dass ein Mitarbeiter die nötigen Mittel dafür aufbringen kann und/oder technische Kompetenz aufweist.*

Datenänderungen

Werden personenbezogene Daten verarbeitet, wie dies bei einer Arbeitszeiterfassung zwangsläufig der Fall ist, stehen den betroffenen Personen verschiedene Rechte zu, angefangen von Auskunftsrechten, aber auch Rechte auf Berichtigung (falscher) Daten, und ggf. auch deren Löschung.

Die Berichtigung falscher Daten ist natürlich auch im Interesse des Unternehmens. Je nach Einsatzvariante ist der Bedarf zu Datenänderungen aber sehr unterschiedlich. Werden z.B. die oben als manipulationssicher eingestuften Technologien primär verwendet, sind Berichtigungen der Daten nur selten notwendig, da die Erfassungssysteme den Mitarbeiter ja nachweislich an dem Erfassungsgerät eindeutig erfassen und die Daten somit im Regelfall quasi zwangsläufig korrekt sind. Berichtigungen in diesem Fall sind dann üblicherweise lediglich die Ergänzung fehlender Meldungen, z.B. wenn Mitarbeiter eine Registrierung vergessen haben. Dies kann in Unternehmen leicht zentralisiert durchgeführt werden und würde sich auch selbst dokumentieren/protokollieren, wenn betroffene Mitarbeiter für vergessene Meldungen z.B. ein Formular ausfüllen müssen. In diesem Fall wären die technischen Optionen des TSI Systems zur Erweiterten Protokollierung überflüssig.

Werden nicht vertrauenswürdige Systeme eingesetzt, oder Systeme, bei denen Nutzer potentiell Eingabefehler machen können, ist der Bedarf für Datenänderungen ungleich größer, nicht nur zur Einhaltung der Rechte zu Berichtigung der betroffenen Person, sondern auch im Interesse des Unternehmens, welches die erfassten Daten z.B. für eine Abrechnung nutzen möchte.

Hier kann es dann leicht sein, dass die Zentralisierung von Datenkorrekturen einen deutlichen Mehraufwand darstellt, wohingegen eine Delegation der Korrekturaufgaben z.B. an Team-Leiter oder gar den betroffenen Mitarbeiter selbst sinnvoll ist. Insbesondere in letzterem Fall mit weitreichenden Privilegien für die Mitarbeiter kann dies Probleme bedeuten, z.B. wenn das Unternehmen die Arbeitszeiterfassung nicht nur als reine Datenerfassung, sondern auch für die direkte Lohnabrechnung verwendet und damit bestimmte Nachweispflichten erfüllen muss. Änderungen, insbesondere nachträgliche oder gar mutwillig falsche, können dann problematisch für das Unternehmen werden und gar rechtliche Konsequenzen nach sich ziehen. In diesem Fall ist die Erweiterte Protokollierung sehr angeraten, so dass das Unternehmen jederzeit nachweisen kann, wann welche Daten erfasst und ggf. zu welchem Zeitpunkt durch wen geändert wurden.

Mehrere/Viele Nutzer mit Änderungsprivilegien

Es ist möglich und in vielen Anwendung-Szenarien sinnvoll, an mehrere oder auch an zahlreiche Nutzer Änderungsprivilegien zu delegieren, insbesondere, bei größeren Anwendungen mit sehr vielen Mitarbeitern oder wenn häufiger Änderungsbedarf besteht (siehe oben).

In diesen Fällen ist die Option Erweiterte Protokollierung aus mehreren Gründen anzuraten. Zum ersten ermöglicht es Nutzern zuvor gemachte Änderungen nachzuvollziehen, so dass die Absicht oder der Zweck einzelner Korrekturen klar wird. Dies erleichtert die Zusammenarbeit und vermeidet zusätzliche Fehler durch Nutzer welche gleichzeitig am gleichen Datenbestand arbeiten.

Weiterhin kann das Unternehmen auf diese Weise leicht Dokumentations- und Nachweispflichten nachkommen und gegenüber betroffenen Personen leicht aufzeigen, wie durch wen und wann Daten erfasst wurden, insbesondere, wenn Ungereimtheiten auftreten oder Personen Auskunftsrechte wahrnehmen möchten.

Letztlich, wenn viele Nutzer in der Lage sind Änderungen vorzunehmen, senkt dies auch die Hürden für Manipulationen ganz gleich ob fahrlässig oder gar mutwillig. Durch die Protokollierung einzelner Änderungen und der durchführenden Nutzer werden auch Verantwortungen dokumentiert und können im Einzelfall als Nachweis dienen.

Lohnabrechnung oder weitere Dokumentationspflichten

Wird das Arbeitszeiterfassungssystem der TSI direkt oder als primäre Quelle (und ohne weitere Zwischenprüfung) für die Lohnabrechnung verwendet, kann das Unternehmen zusätzlichen Dokumentationspflichten unterliegen, die auch einen Nachweis über den Ursprung der erfassten Daten bzw. deren Änderungen beinhalten. In diesem Fall ist die Aktivierung der Erweiterten Protokollierung ebenfalls anzuraten.

Wird das System vorrangig zur Abrechnung von erbrachten Leistungen gegenüber den Kunden des Unternehmens verwendet, obliegt es im Regelfall dem Ermessen des Unternehmens, inwieweit eine Datenprotokollierung erwünscht ist.

Je nach Anwendungsfall und Tätigkeitsprofil des Unternehmens können weitere Dokumentationspflichten bestehen, für die eine Erweiterte Protokollierung vorteilhaft ist.

Ist ein Datenschutzkonformer Einsatz auch ohne Erweiterte Protokollierung möglich?

Wir beurteilen dies mit einem ganz klarem Ja. Es hängt dabei aber vieles auch von der Ausgestaltung Ihrer Prozesse ab. In vielen Einsatzfällen, gerade bei klassischen Konstellationen ohne Einbindung von Smartphones, ist eine Erweiterte Protokollierung für den Datenschutz nicht erforderlich.

Nach unserer Einschätzung ist die Erweiterte Protokollierung immer dann sinnvoll, wenn eine oder mehrere der oben erörterten Situationen auf Ihr Unternehmen zutreffen, aber auch das kann von einem Ermessen und von einer Auslegung der Rechtslage abhängig und deutlich differenzierter sein. Eine einschlägige Rechtsprechung insbesondere in Bezug auf die DSGVO steht derzeit noch aus.

Wir weisen aber darauf hin, dass wir an dieser Stelle keine qualifizierte, rechtsverbindliche Beratung ersetzen können. Details sollten Sie in jedem Fall gemeinsam mit Ihrem Datenschutzbeauftragten und Ihrer Rechtsabteilung oder Rechtsvertretung erörtern.

Da Sie aber, wovon wir ausgehen, die Vorgaben des Datenschutzes in Ihrem Unternehmen bereits umgesetzt haben, können Sie die Vorteile und Notwendigkeit einer Erweiterten Protokollierung für Ihren Einzelfall viel besser beurteilen.

Optionen für die Erweiterte Protokollierung

Die Erweiterte Protokollierung für die Arbeitszeiterfassung im System der TSI ermöglicht verschiedene Detailstufen der Protokollierung, sowie verschiedene Optionen in der Realisierung, die insbesondere die Datenspeicherung betreffen und in Bezug auf den Datenschutz relevant sein können.

Detailstufen der Erweiterten Protokollierung

Aktivierung

Mit der Aktivierung der Erweiterten Protokollierung wird automatisch jede Datenänderung erfasst und hierbei werden folgende Details festgehalten:

- Änderungszeitpunkt
- Autorität des Ändernden und dabei:
  a) Login Informationen zum Änderungszeitpunkt
  b) Zugewiesenes Team-Mitglied/Manager (sofern zutreffend)
  c) Autoritätsstatus (Supervisor/Administrativer Nutzer; sofern zutreffend)

Diese Informationen werden auch für die Erstellung von Datensätzen protokolliert, sofern die verwendete Datenquelle eine eindeutige Zuordnung dieser Art erlaubt. Dies ist der Fall bei der Verwendung von Smartphones oder einem Webzugang. Nicht der Fall ist dies bei der Erstellung eines Datensatzes mittels iButton, RFID, oder Mitarbeiterkarte.

Sofern die Erweiterte Protokollierung für das Unternehmen aktiviert ist, ist diese Erfassung und Aufzeichnung von erstellenden und ändernden Personen nicht abschaltbar.

Werte-Historie

Über die Aktivierung der Protokollierung hinaus lässt sich eine Werte-Historie aktivieren. Mit dieser werden nicht nur Änderungszeitpunkte und ändernde Personen erfasst, sondern es wird auch festgehalten, welche konkreten Änderungen durchgeführt und welche Werte ggf. geändert werden. Das heißt es werden auch die Werte vor und nach einer Änderung protokolliert, so dass auch nachvollziehbar ist, welche Eigenschaften und Daten ein Datensatz zu jedem Zeitpunkt besaß[1].

[1] Für die vollständige Rekonstruierbarkeit eines Datensatzes muss die Werte-Historie für alle Änderungen aktiviert gewesen sein. Wird eine Änderung zu einem Zeitpunkt durchgeführt, an dem die Werte-Historie Option nicht für das Unternehmen aktiviert ist, bricht dies das Änderungsprotokoll und eine vollständige Rekonstruktion des Datensatzes ist ggf. nicht mehr möglich, bzw. kann ggf. nur teilweise und durch manuelle technische Eingriffe der TSI getätigt werden.

Realisierungsoptionen

Sofern Datensätze lediglich erzeugt und geändert werden, ist die Protokollierung technisch vergleichsweise einfach, verglichen damit, wenn Datensätze aus welchen Gründen auch immer gelöscht werden sollen.

Denn eine Löschung schließt zwangsläufig auch eine Löschung aus der Dokumentation, Protokollierung und Werte-Historie mit ein. Ansonsten handelt es sich nicht wirklich um eine Löschung, insbesondere wenn eine Löschung aus einem Recht darauf durch eine betroffene Person im Sinne der Datenschutzgrundverordnung geschehen soll.

Dies wird auch nicht dadurch einfacher, dass sich hier rechtlich mehrere widersprüchliche Ziele und Vorgaben gegenüberstehen können. Zum einen gibt es Dokumentations- und Berichtigungspflichten für Unternehmen bzw. Rechte für betroffene Personen, zum anderen gibt es das besagte Recht auf Löschung insbesondere für falsche Informationen. Eine Dokumentation und eine vollständige Löschung können aber natürlich nicht gleichzeitig realisiert werden. Auch ein Für und Wider der einen Option über der anderen, kann sich von Einsatzfall zu Einsatzfall stark unterscheiden.

Daher ist das System der TSI flexibel ausgelegt und unterstützt mehrere Optionen:

Löschungen grundsätzlich erlaubt

Löschungen sind grundsätzlich erlaubt und können durch jeden beliebigen Nutzer, der für eine Datenänderung/Löschung berechtigt ist, durchgeführt werden[2]. Bei der Löschung wird der Datensatz vollständig entfernt, was die Protokollierung für diesen Datensatz und ggf. die Änderungs- und Werte-Historie dieses Datensatzes mit einschließt. Auch eine Wiederherstellung des gelöschten Datensatzes ist nicht (im System) möglich[3].

Löschung generell nicht erlaubt

Löschungen sind generell nicht erlaubt und Datensätze bleiben permanent im System, inklusive deren Protokoll und ggf. Werte-Historie. Falsche oder nicht benötigte Datensätze können im System als solche markiert („ignoriert“) werden, und fließen nicht in weitere Auswertungen, Analysen oder Datenexporte mit ein. Für normale Nutzer und Anwendungsfälle ist es als ob der ignorierte Datensatz nicht existiere. Der ignorierte Datensatz selbst kann aber jederzeit im Management-Bereich als solcher eingesehen werden inklusive dessen Protokoll und Änderungshistorie. Ignorierte Datensätze können auch jederzeit reaktiviert werden und fließen dann wieder normal in weitere Auswertungen mit ein.

Löschung nur durch spezielle Supervisor-Nutzer erlaubt

Löschungen sind für normale Nutzer nicht erlaubt und können lediglich, wie oben beschrieben, ignoriert werden. Davon ausgenommen sind spezielle Supervisor-Nutzer, die neben der Option einen Datensatz zu ignorieren, auch die Möglichkeit besitzen Datensätze vollständig und nicht wiederherstellbar zu löschen, was, wie oben beschrieben, auch das Protokoll und ggf. die Werte-Historie des Datensatzes einschließt.

Verwaltung durch Supervisor-Nutzer

Wird die Erweiterte Protokollierung für ein Unternehmen lizensiert, kann der Supervisor-Nutzer dieses Unternehmens die einzelnen, lizensierten Optionen der Erweiterten Protokollierung verwalten, d.h. diese nach den Unternehmensvorgaben einrichten bzw. aktivieren. Im Regelfall ist

[2] Hiervon ausgenommen sind maschinell (z.B. durch iButton oder RFID) erfasste Datensätze. Diese sind nicht löschbar.

[3] Eine manuelle Wiederherstellung durch Neu-Anlegen eines gleichen Datensatzes ist jederzeit durch einen berechtigten Nutzer möglich.

dies für das Unternehmen vorteilhaft, da hier der Supervisor des Unternehmens leicht selbst alle Einstellungen vornehmen kann und nicht auf Unterstützung durch die TSI angewiesen ist, welche zwar im Regelfall schnellstmöglich zur Verfügung steht aber meist doch zeitlich zumindest kleine Verzögerungen bedeutet.

Es ist aber auch möglich, die Verwaltung der Optionen der Erweiterten Protokollierung durch das Unternehmen selbst gänzlich einzuschränken. Dies kann dann sinnvoll sein, wenn eine generelle Löschung von Datensätzen in keinem Fall erlaubt werden soll. Das Unternehmen kann damit gänzlich ausschließen, dass irgendjemand Löschungen vornehmen kann und somit Kunden oder Mitarbeitern vollständige Dokumentation und Nachweissicherung garantieren.

Diese Option sichert auch gegen ein, wenn auch unwahrscheinliches Szenario ab, in welchem ein (böswilliger) Supervisor seine Rechte missbraucht und ungenehmigt Löschungen vornimmt, da dem Supervisor normalerweise auch die Konfiguration der Löschung unterliegt.

Löschung durch die TSI

Die TSI löscht Datensätze grundsätzlich nicht und hält alle Datensätze für den vereinbarten Speicherungszeitraum vor. Wenn die TSI eine Löschung durchführen soll, ist in jedem Fall dafür ein schriftlicher Auftrag notwendig, in dem Fall, dass die Erweiterte Protokollierung[4] für ein Unternehmen aktiviert ist, bestehen wir auch auf eine rechtlich verbindliche Beauftragung (Fax, Einschreiben), die wir selbstverständlich auch vollständig dokumentieren.

Rechtliche Hinweise

Die technischen Beschreibungen und Erläuterungen in diesem Dokument wurden nach bestem Wissen und Gewissen sorgfältig zusammengestellt und sind zum Veröffentlichungszeitpunkt zutreffend. Eine Gewähr oder jegliche Haftung insbesondere für die Richtigkeit und Vollständigkeit kann nicht übernommen werden. Es wird besonders darauf hingewiesen, dass das System der TSI stetig weiterentwickelt wird und regelmäßig technische und funktionale Erweiterungen integriert werden, so dass nicht auszuschließen ist, dass Beschreibungen und Erläuterungen oder Teilaspekte dieser zu einem späteren Zeitpunkt nicht länger oder nur eingeschränkt zutreffend sind. Die TSI steht für die Investitionssicherheit ihrer Produkte und – sofern möglich – legen wir bei Neuerungen größtes Augenmerk auf den Erhalt von Funktionen oder liefern Alternativen, welche Funktionen gleichwertig oder wirksamer ersetzen.

Dieses Dokument ist nicht rechtsverbindlich und ersetzt nicht eine qualifizierte rechtliche Beratung. Für eine abschließende rechtliche Einschätzung Ihres konkreten Anwendungsfalls fragen Sie bitte Ihre Rechtsabteilung oder Rechtsvertretung.

Fehler und Auslassungen vorbehalten.

Letzte Änderung: 10. Januar 2019

[4] Hierbei ist die Erweiterte Protokollierung ohne Löschmöglichkeit und ohne Verwaltung durch den Supervisor-Nutzer gemeint.