Was bedeutet Process Mining für Datenschutz und Mitbestimmung im Unternehmen?

Martin Degeling

Beim Process Mining werden verschiedene Daten, die im Unternehmen entstehen, zusammengeführt und ausgewertet. Das können technische Systemdaten sein, aber auch solche, die direkt oder indirekt einer Person zuordenbar sind. Das wirft Fragen rund um Datenschutz und Verhaltenskontrolle von Beschäftigten auf.

Richtig, aber man muss hier zwischen zwei Rechtsgebieten unterscheiden. Es geht um Datenschutz auf der einen und Mitbestimmung auf der anderen Seite, auch wenn es zwischen beiden eine große Verzahnung und Abhängigkeiten gibt. Beim Datenschutz ist die erste Frage die gestellt werden muss: Hab ich es überhaupt mit personenbezogenen Daten zu tun? Das betrifft direkt personenbezogene Daten, etwa wenn ich feststelle, dass eine Maschine mehrfach am Tag überhitzt, und dann nachschaue, wer damit gearbeitet hat. Es gilt aber auch für die Analyse mit Big-Data-Methoden, bei denen man vorhandenen Daten in ein anderes System überführt und dann dort möglicherweise keine personenbezogenen, sondern rein statistische Auswertungen durchführt – auch dann muss man sich Gedanken machen, welche Datenschutzanforderungen zu beachten sind.

Auf der anderen Seite – und das ist, grundsätzlich ein anderes Rechtsgebiet, das sich vorrangig an den Systemen orientiert und nicht an den Daten – gilt es zu schauen: ist ein System geeignet, das Verhalten von Beschäftigten zu kontrollieren? In dem Fall wird die Mitbestimmung ausgelöst. Das heißt, das System darf nicht eingeführt werden, ohne dass der zuständige Betriebs- oder Personalrat zugestimmt hat. Mitbestimmung und Datenschutz sind die zwei Säulen des Beschäftigtenschutzes.

Wo liegen die Unterschiede?

Natürlich spielt Datenschutz im Rahmen der Mitbestimmung bei der Gestaltung von Systemen eine Rolle. Genauso wie eine Betriebsvereinbarung Vorgaben zur sachgerechten Nutzung und zur Berechtigungsgestaltung enthält, müssen auch Datenschutzanforderungen berücksichtigt werden.

Aber, ganz unabhängig von Mitbestimmung, zum Beispiel auch, wenn es gar keinen Betriebsrat gibt, sind Arbeitgeber verpflichtet, datenschutzkonform zu handeln. Wenn also ein System die Beschäftigten nach Strich und Faden kontrolliert und überwacht, es aber keinen betrieblichen Partner gibt, der das Mitbestimmungsrecht wahrnimmt, müssen die geltenden Datenschutzvorgaben, wie beispielsweise das Verbot mit Erlaubnisvorbehalt eingehalten werden.

Konkret heißt das für das Process Mining: Ich muss mir als Betreiber darüber klar werden, was für mich die Rechtsgrundlage ist. Bei vielen derartigen Systemen dürfte es schwerfallen zu argumentieren, dass sie zur Durchführung des Beschäftigungsverhältnisses notwendig sind. Denn der normale Betrieb, wie Personalbeschäftigung, -bezahlung und -verwaltung sowie die Einsatzplanung konnte auch bisher ohne Process-Mining durchgeführt werden. Außerdem handelt es sich beim Process-Mining ja häufig um eine Systemart, die eher auf

https://doi.org/10.1007/s00287-019-01197-8

Martin Degeling
ist Mitarbeiter am Horst Görtz Institut für IT Sicherheit an der Ruhr-Universität Bochum.
Er forscht zur Anwendungbarkeit von Privacy-by-Design in der Software Entwicklung und Datenschutz im Internet.
E-Mail: martin.degeling@ruhr-uni-bochum.de

der Metaebene liegt: nicht selbst produktiv, sondern andere Systeme analysierend und zur Unterstützung bei der Optimierung betrieblicher Prozesse. Auf der Datenschutzebene und aus Sicht des Unternehmens kann man hier zur Identifizierung einer Rechtsgrundlage eigentlich nur mit eigenen Interessen argumentieren. Denn es liegt im berechtigten Interesse eines Unternehmens, die eigenen Arbeitsweisen kontinuierlich zu optimieren, um wettbewerbsfähig zu bleiben.

Das heißt, dass man nicht versucht, mit der Durchführung des Beschäftigungsverhältnisses zu argumentieren, oder gar Einwilligungen einzuholen. Beides verspricht datenschutzrechtlich keinen Erfolg. Das Eigeninteresse muss dann allerdings gut begründet werden: ich muss nachvollziehbar darlegen, dass ich genauso vorgehen muss, wie ich es vorhabe. Die entscheidende Frage ist dann, ob es gelingen kann, die Verarbeitung, im Sinne der betroffenen Beschäftigten so datenschutzfreundlich zu gestalten, dass eine datenschutzrechtlich saubere Abwägung zwischen deren Rechten und meinen eigenen Interessen zu meinen Gunsten ausgeht.

In einer solchen Abwägung muss abzulesen sein, welche Einschränkungen der Persönlichkeitsrechte der Beschäftigten zu erwarten sind, um welche es sich handelt, und wie schwerwiegend diese jeweils sind. Und auf der anderen Seite muss dargelegt werden, wie groß mein Interesse an der Durchführung der Verarbeitung ist und worauf es sich stützt.

Warum ist die Einwilligung keine sinnvolle Rechtsgrundlage?

Generell ist die Einwilligung eine potenzielle Rechtsgrundlage für Verarbeitung personenbezogener Daten, aber sie ist an bestimmte Voraussetzungen geknüpft. Eine wesentliche ist: Sie muss freiwillig sein. Die zweite: sie muss jederzeit zurücknehmbar sein und es dürfen keine negativen Konsequenzen für den Betroffenen daraus erwachsen. Das ist im Arbeitsverhältnis in den seltensten Fällen möglich. Vor allem, weil es kein Kräftegleichgewicht zwischen Arbeitgeber und Beschäftigten gibt. Wenn ich als Arbeitnehmer von meinem Chef gefragt werde: „Du bist doch bestimmt einverstanden, dass ich das und das mit deinen Daten mache!“ habe ich schnell das Gefühl: Wenn ich jetzt „Nein“ sage, dann werde ich Nachteile haben. Da kann von einer freiwilligen Einwilligung keine Rede sein.

Es gibt nur sehr wenige Situationen im Arbeitsleben, in denen wirksam eine Einwilligung von Beschäftigten durch den Arbeitgeber eingeholt werden kann. Und mein weiterer Zweifel beruht auf Praktikabilität: ich muss – egal, ob im Beschäftigungsverhältnis oder sonst wo – bei Einwilligung immer dafür sorgen, dass ich in der Lage bin, einen Widerspruch angemessen zu behandeln. Das heißt, wenn jemand mir heute eine Einwilligung gibt, seine Daten dann verarbeitet werden, und die Person morgen kommt und die Einwilligung zurückzieht, dann muss ich bzw. mein System in der Lage sein, dessen Daten herauszusuchen und die Verarbeitung einzustellen. Und wenn das eine größere Menge von Personen macht, dann müssen meine Verarbeitungen trotzdem noch sinnvoll möglich sein. Wenn etwa plötzlich 50 % meiner Beschäftigten der Verarbeitung widersprechen, dann werden Ergebnisse meiner Berechnungen vermutlich nicht mehr repräsentativ sein. Deswegen glaube ich nicht, dass in einem solchen Zusammenhang eine Einwilligung wirklich eine sinnvolle Rechtsgrundlage ist.

Wenn der gangbare Weg ist, über das berechtigte Interesse zu argumentieren: Wie muss dann eine Abwägung aussehen?

Das Ziel aus Sicht derer, die personenbezogene Daten verarbeiten wollen, ist es, die eigenen Interessen nicht künstlich, aber berechtigt und gut nachvollziehbar, hoch einzuschätzen und auf der anderen Seite ist genauso nachvollziehbar darzulegen, dass die Interessen der Betroffenen nicht überwiegen. Dazu müssen ausreichende Schutzmaßnahmen ergriffen werden, damit die Einschränkungen der Persönlichkeitsrechte der Betroffenen möglichst gering bleiben.

Darunter fallen die üblichen Maßnahmen, wie beispielsweise die frühzeitige Anonymisierung oder zumindest Pseudonymisierung. Und echte Anonymisierung bedeutet wohlgemerkt die Entfernung eines Personenbezugs, nicht nur das einfache Löschen von direkt identifizierenden Merkmalen, wie z. B. des Namens.

Zu den Schutzmaßnahmen gehört aber auch die ordentliche Strukturierung und Konzeptionierung der Sicherheit des Gesamtsystems. Die einfache Zusicherung, man wolle die Zweckbindung einhalten, ist nicht ausreichend. Sondern auch durch technisch sichere Gestaltung des Systems muss dafür gesorgt werden, dass diese auch eingehalten werden kann.

Etwa durch ein sachgerechtes Berechtigungssystem. Es ist aber auch zu beachten, wo die Daten verarbeitet werden. Passiert das vor Ort oder werden sie in einen Cloud-Dienst überführt, dessen Server im nicht-europäischen Ausland stehen? Dies würde zu einer schwierigeren Abwägung der eigenen Interessen mit denen der Beschäftigten führen, weil Beschäftigte ein sehr hohes Interesse daran haben, dass ihre Daten den Geltungsbereich der Datenschutzgrundverordnung nicht verlassen.

Wichtig, und auch „gern" vergessen, wird ein ordentliches Löschkonzept. Das heißt, es muss klar sein, wann welche Daten nicht mehr erforderlich sind und wann sie gelöscht werden. Das betrifft nicht nur den Datenpool, in dem Daten aus verschiedenen Systemen für das Process Mining zusammengeführt werden, sondern auch die Quelldatenbanken selbst. Es ist also festzulegen, wann welche Daten nicht mehr erforderlich sind und wann sie gelöscht werden. Gelöscht werden müssen außerdem die Ergebnisse von Analysen, wenn diese personenbezogene Daten enthalten. Und auch für Ergebnisse und Auswertungen, die papierhaft weiterverarbeitet werden (z. B. in Infos an das Management) sind Vernichtungsregeln festzulegen, wenn sie personenbezogene Daten enthalten.

Dazu müssen auch organisatorische Prozesse betrachtet werden. Alle Löschfristen und deren Begründung müssen sachgerecht dokumentiert werden.

Am Ende sollten durch die ergriffenen Sicherheits- und technisch-organisatorischen Schutzmaßnahmen die Risiken für die Beschäftigten so überschaubar und gering sein, dass man im Rahmen der Abwägung berechtigterweise von einem überwiegenden Eigeninteresse ausgehen kann.

Das ist aber nur die eine Seite.

Genau, da kommen wir zurück auf die andere Säule. Auch wenn eine Lösung datenschutzkonform ist, müssen trotzdem noch Mitbestimmungsrechte eingehalten werden, wenn das System zur Verhaltenskontrolle geeignet ist. Natürlich können all die erwähnten Schutzmaßnahmen auch Inhalt der Betriebsvereinbarung sein. Im Einzelfall kann eine solche Betriebsvereinbarung dann sogar selbst die Rechtsgrundlage sein. Dann gehen Datenschutz und Mitbestimmungsrechte Hand in Hand.

Ok, kommen wir nochmal zurück zur Frage der Clouddienste. Häufig sind diese ja auch attraktiv, weil man diese auch für einen ersten Test nutzen kann, um kurzfristig die Auswertung der Daten zu starten, ohne eigene Infrastruktur aufzubauen. Wie ist das mit dem Datenschutz vereinbar?

Sowohl für Mitbestimmung als auch für den Datenschutz, gibt es keinen Testbetrieb, der in irgendeiner Weise schwächere Anforderungen hätte als ein Regelbetrieb. Und daher muss ich auch für einen Testbetrieb sowohl datenschutzrechtliche als auch mitbestimmungsbezogene Überlegungen anstellen. Denn in dem Moment, in dem ich das erste personenbezogene Datum in die Cloud übertrage, habe ich eine datenschutzrelevante und mitbestimmungsrelevante Verarbeitung vorgenommen.

Im Bereich der Mitbestimmung kommt es häufig vor, dass man sich auf Pilotvereinbarungen einigt, in denen festgelegt wird, was das Ziel des Tests ist und die Begrenzungen in Bezug auf Laufzeit, Umfang der Verarbeitung, Zugriffsrechte und Zwecke enthalten.

Wenn sich anschließend abzeichnet, dass ein System dauerhaft genutzt werden soll, kann man dazu die endgültige Betriebsvereinbarung erarbeiten. Auf der Datenschutzebene ist dieses stufenweise Vorgehen aber nicht möglich. Wenn Clouddienste genutzt werden, muss immer ein Auftragsverarbeitungsvertrag abgeschlossen werden, der den Anforderungen der Grundverordnung entspricht, unabhängig davon, ob die Nutzung testweise oder dauerhaft erfolgt.

Beim Process Mining werden Daten ja häufig für einen anderen Zweck genutzt als ursprünglich vorgesehen. Was gibt es da zu beachten?

Die Zweckänderung von Daten erfordert letztlich immer, dass man nochmal von vorne mit der Prüfung der Rechtsgrundlage anfängt. Man hat Daten für einen bestimmten Zweck rechtmäßig erhoben und muss, wenn man Sie für einen anderen Zweck nutzen will, auch hier wieder Erforderlichkeit, Rechtmäßigkeit und so weiter nachweisen. Wenn man dann zum Schluss kommt, dass man sie auch für den neuen Zweck erheben dürfte und es gibt noch keine Betriebsvereinbarung die genau diesen neuen Zweck anschließt, muss man diesen mindestens in der alten ergänzen.

Sie haben bereits kurz die Problematik von Pseudonymisierung und Anonymisierung angesprochen. Können Sie hier noch etwas in die Tiefe gehen?

Wir können heute mit Sicherheit sagen, dass z. B. das einfache Löschen einer Namensspalte aus einer Tabelle in großen Datenbeständen keine Anonymität herstellt. Es gibt einfach zu viele Möglichkeiten, auch über Querverbindungen und Zusatzwissen noch Aussagen darüber treffen zu können, um wen es sich da wohl handelt. Anonymität herzustellen stellt in der Informatik eine anspruchsvolle Aufgabe dar. Aber das bedeutet nicht, dass es unmöglich ist. Bei vielen existierenden Systemen ist mein Eindruck eher, dass die Umsetzung von Anonymität versäumt wurde, weil es methodisch und inhaltlich nicht trivial und damit eben auch teuer für die Hersteller ist.

Im wissenschaftlichen Bereich ist die Diskussion relativ weit gediehen, aber ich bin mir nicht sicher wie weit das in Systemen umgesetzt ist. Ähnliche Probleme gab es viele Jahre im Bereich der Löschkonzepte. Auch vor 10 Jahren war schon bekannt, dass Unternehmenssoftware Löschkonzepte vorsehen muss, aber damals hat sich ein sehr bekannter, deutscher Hersteller einer verbreiteten Unternehmenssoftware noch auf einer Konferenz so geäußert: „Wenn ein Kunde kommt, der uns eine Million in die Hand drückt, weil ihm das wichtig ist, dann kümmern wir uns ums Löschen. Solange machen wir das nicht." Hier hat die Diskussion um die Datenschutzgrundverordnung gezeigt, dass, wenn es Kunden an den Geldbeutel zu gehen droht, bestimmte Funktionalität stärker nachgefragt und dann auch umgesetzt wird.

Welche Möglichkeiten für datenschutzfreundliches Process Mining gibt es noch?

Eine zentrale Frage ist ja: Brauche ich eine Zuweisung zu irgendeiner eindeutigen personenbezogenen Kennung, damit ich überhaupt eine allgemeine Entwicklung im Unternehmen wahrnehmen kann? Muss ich unbedingt wissen, dass: ein bestimmter Datensatz in Zusammenhang mit Person X entstanden ist und darüber hinaus personenbezogen alle Datensätze in Zusammenhang mit Person X in Beziehung setzen können? Oder bliebe die Erkenntnis die gleiche, auch wenn ich die Datensätze ohne Personenbezug beliebig durcheinander würfeln würde? Eine weitere Frage: welche Angabe stellt an diesem jeweiligen Datensatz der Personenbezug her? Recht häufig kann man den durchaus vermeiden, ohne den Erkenntnisgewinn zu schmälern. Nehmen wir das Beispiel Versandhandel. Eine Mitarbeiterin geht mit einem Handscanner durch das Lager und hat vom System eine Liste mit Waren bekommen, die sie zusammenstellt. Sie scannt jeden Artikel und das datenschutzrechtliche Problem entsteht erst in dem Moment, in dem die Zuordnung von Handscanner zur Person möglich wird. Das Unternehmen interessiert sich nun vielleicht dafür, wie die Prozesse funktionieren und sucht Optimierungspotenziale. Dafür muss es aber eigentlich nicht wissen, wer den Handscanner benutzt hat. Statt die Daten technisch vor der Auswertung zu anonymisieren, könnte man auch Prozesse geschickt gestalten. So zum Beispiel, indem man im beschriebenen Fall einfach ein rollierendes System einsetzt, bei dem der Handscanner jeden Tag von jemand anderem benutzt wird. So lassen sich die Prozesse über die Handscanner-Nummer beobachten, ohne zu wissen, welcher konkrete Beschäftigte da jeweils diesen Handscanner in der Hand gehabt hat.

Natürlich ist das eine sehr spezifische Lösung, aber häufig lassen sich auch organisatorische Lösungen finden, die technisch weniger aufwändig sind.

Abschließend die Frage nach der Umsetzung. Welche Rollen können Datenschutzbeauftragte spielen?

Datenschutzbeauftragten haben den Datenschutz für die Beschäftigten genauso zu beachten und zu fordern wie für die Kundendaten oder für Partnerdaten. Das gilt ganz unabhängig von Mitbestimmungsrechten. Die Rolle der Datenschutzbeauftragten unterscheidet sich auch nicht, wenn es keinen Betriebsrat gibt. Gibt es jedoch einen Betriebsrat und sind Betriebsvereinbarungen in Kraft, die auch datenschutzrelevante Regelungen enthalten, dann muss der Datenschutzbeauftragte auf deren Einhaltung hinwirken – genauso wie auf die Einhaltung aller anderen Datenschutzvorschriften.

Vielen Dank für das Gespräch.

Karin Schuler
freiberufliche Beraterin für Datenschutz, IT-Sicherheit und Mitbestimmung (www.schuler-ds.de)
Gründungsmitglied des Netzwerks Datenschutzexpertise (www.netzwerk-datenschutzexpertise.de)
Mitglied der Fachgruppe PET der Gesellschaft für Informatik e. V.
E-Mail: buero@schuler-ds.de

Das Interview wurde am 12. April 2019 von Martin Degeling geführt.