Nyon, 191217

Die 10 wichtigsten Grundsätze für Arbeitnehmerdatenschutz und -sicherheit

Einleitung

Daten, riesige Datamengen und Datensätze haben in Unternehmen zwar zunehmend Einfluss auf das unternehmerische Handeln, doch Arbeitnehmerdatenschutz und Regeln für den Schutz der Privatsphäre existieren praktisch nicht. Dieses Dokument enthält zehn Handlungsgrundsätze für die Auseinandersetzung mit diesem Ungleichgewicht. Da diese Grundsätze konkrete Forderungen im Hinblick auf das Sammeln und Verwenden von Daten durch Unternehmen enthalten, geben sie Arbeitnehmerinnen und Arbeitnehmern die Handhabe dazu, eine ethische und nachhaltige Datennutzung sicherzustellen. Auf jeden Fall besteht unmittelbarer dringender Handlungsbedarf. Wir müssen handeln, um die Interessen der Arbeitnehmer zu wahren und ein ausgewogenes Kräfteverhältnis am Arbeitsplatz aufrechtzuerhalten. Die in diesem Dokument dargelegten zehn Grundsätze wurden von der UNI Global Union zu diesem Zweck entwickelt.

Daten werden als das neue Gold bezeichnet. Sie werden gehandelt, analysiert und zu Marketing- und Werbezwecken und in der Personalverwaltung verwendet. Sie bilden auch die Bausteine für künstliche Intelligenz und Algorithmen. Es wird geschätzt, dass bis 2030 15-20 % des Weltbruttosozialprodukts auf Datenflüssen basieren werden. Gerade auch die Gründung der Vielzahl neuer Unternehmen und Dienstleistungen individualisiert zunehmend viele Aspekte unserer Wirtschaft und Gesellschaft, und dabei sind insbesondere die Plattformen der so genannten Gig Economy zu nennen.

Als Bürgerinnen und Bürger hinterlassen wir täglich Datenspuren, nämlich durch unsere Suchanfragen auf Google, durch die Apps auf unseren Mobiltelefonen, Taxifahrten, Wohnungen, die wir anmieten, Dinge, die wir kaufen, unsere Treuekarten, unsere Gesundheitsdaten und unsere Anrufe bei Kundenkontaktzentren. Ganz zu schweigen von den Orten, die wir besuchen, E-Mails, die wir versenden, unsere Facebookfreunde und Tweets, die wir schreiben. All das liefert Unternehmen Daten – über uns und unser Netzwerk von Freunden. Daten sind schlicht das größte Geschenk, das wir machen, ohne es zu realisieren.

Auch als Arbeitnehmerinnen und Arbeitnehmer liefern wir Daten — unseren Lebenslauf, unsere biometrischen Daten, wie Fingerabdrücke oder Iris-Scans, und die umfangreichen Daten, die im Zuge der Überwachung unserer Arbeitsabläufe durch unsere Arbeitgeber über uns gesammelt werden. Daten oder eher Datensätze von innerhalb und außerhalb des Unternehmens spielen in den Unternehmen auch bei Personalentscheidungen eine Rolle. Wer wird eingestellt? Wer wird befördert? Soll jemand entlassen oder verwarnt werden? Sind die Beschäftigten heute produktiv und falls nicht, warum? Die Anwendung und der Einsatz in Unternehmen warf sogar die Frage auf, ob durch Daten nicht das Humane bei den Humanressourcen verloren geht.

Doch wem gehören denn eigentlich die Daten, die wir liefern? Und welche Daten gibt es ‘da draußen’ über dich und mich? Diese zwei Fragen sind schwer zu beantworten. Der CEO von

LinkedIn sagte, dass die überwiegende Mehrheit der weltweiten Daten letztendlich in den Händen der großen Technologiekonzerne liegt: Google, Facebook, Amazon, Microsoft und Apple. In einem kürzlich verschickten Twitter Feed hieß es, dass man für US-Dollar 1.000 von einem Unternehmen jegliche und alle möglichen Informationen über eine Person bekommen könne. Wir wissen, dass bestimmte Unternehmen Experten darin sind, Daten zu sammeln und sie an andere zu verkaufen, damit diese dann unsere Meinung manipulieren können. Wir wissen jetzt auch, dass sowohl die Ergebnisse der Wahlen in den USA als auch die der Brexit-Abstimmung durch die Nutzung von Daten beeinflusst und manipuliert wurden, indem dafür bezahlt wurde, dass über fingierte Twitter- und Facebook-Accounts bestimmte Versionen und Storys gezielt an uns herangetragen wurden.

In Japan bereitet die Regierung den Ausbau so genannter Datenbanken vor. Dabei geht es um öffentliche Ämter, die Bürgern bei der Entscheidung dabei, welche Daten sie verfügbar machen möchten, helfen werden. In Estland, einem Land mit einem der umfassendsten elektronischen Regierungssysteme und einer der umfangreichsten Datennutzung der Welt, unterliegen die Daten von Bürgern strengen rechtlichen Grundsätzen, die den Einzelnen dazu ermächtigen, darüber zu entscheiden, welche Daten er verfügbar machen möchte und wie diese genutzt werden können. Noch hinken viele Länder hinterher, wenn es darum geht, Bürgern einen klaren und transparenten Weg dazu aufzuzeigen, wie sie herausfinden können, welche Informationen existieren und nicht zuletzt auch Möglichkeit zur Kontrolle der Informationen zu haben.

Datenschutz und Gesetze über den Schutz der Privatsphäre gibt es in vielen Ländern zwar in verschiedenen Formen, aber die Daten, die im Zuge der Überwachung von Beschäftigten gesammelt werden, fallen nicht unbedingt unter diese Gesetze. UNI Global Union arbeitet mit der globalen Organisation IEEE zusammen, um einen internationalen Standard für eine transparente Verwaltung von Arbeitnehmerdaten durch Arbeitgeber zu schaffen. Die Gewerkschaften müssen unbedingt auch weiterhin versuchen, über betriebliche und/oder sektorale Tarifverträge die Rechte der Arbeitnehmer an ihren Daten sowie Schutzbestimmungen durchzusetzen. Ohne die genannten Bestimmungen werden die Machtverhältnisse in Unternehmen für immer und ewig zugunsten der mit Daten gefütterten einseitigen Managemententscheidungen ausfallen. Angesichts der relativ einfachen Kombinierbarkeit von Daten aus vielen verschiedenen Quellen, ohne Mitspracherecht und Einfluss darauf, welche Daten verwendet werden und wie, werden Arbeitnehmer extrem im Nachteil sein. In der Tat kann man getrost sagen, dass Arbeitnehmerdatenrechte und deren Schutz im Zuge der Herausbildung der digitalen Wirtschaft die nächste große Herausforderung für Gewerkschaften darstellt.

In Anbetracht der Bedeutung von am Arbeitsplatz gesammelten Daten fordert die UNI Global Union, dass **Arbeitnehmer und ihre Gewerkschaftsvertreter das Recht auf Zugang, Einfluss, Bearbeitung und Löschung von Daten, die im Zuge ihrer Arbeitsprozesse über sie gesammelt werden, haben müssen.**

In diesem Dokument wird diese zentrale Forderung operationalisiert und in zehn spezifische Aktionspunkte unterteilt.

Inhalt

1 Arbeitnehmer müssen Zugang zu und Einfluss auf die über sie gesammelten Daten haben

Arbeitnehmer müssen das Recht auf Zugang zu Daten, die über sie gesammelt werden, einschließlich des Rechts auf eine Berichtigung, Blockierung oder Löschung von Daten, haben.

Dies umfasst:

a) dass eine Zustimmung nicht die Rechtsgrundlage der Datenverarbeitung bei der Arbeit sein kann und sollte.
b) Beschäftigte sollten in der Lage sein, auf Anfrage in angemessenen Abständen und ohne übermäßig lange Wartezeit eine Bestätigung der Verarbeitung personenbezogener Daten im Zusammenhang mit ihm oder ihr zu erhalten. Die Kommunikation sollte in verständlicher Form stattfinden und alle Informationen über die Herkunft der Daten sowie auch alle anderen Angaben, um deren Vorlage der Datenerfasser gebeten wird, enthalten, um die Transparenz der Verarbeitung zu gewährleisten.
c) Ein Arbeitnehmer muss das Recht auf Portabilität der Daten haben, das heißt, das Recht, z. B. Rating- und Rankingsysteme von einer Plattform zu einer anderen zu verschieben.
d) Im Einklang mit den nationalen Rechtsvorschriften und Praktiken oder den Bedingungen von Tarifverträgen, können die personenbezogenen Daten den Arbeitnehmervertretern mitgeteilt werden, jedoch nur in dem Umfang, in dem diese Daten notwendig sind, damit sie die Interessen der Arbeitnehmer entsprechend vertreten können oder wenn solche Daten für die Einhaltung und Überwachung der in den Tarifverträgen festgehaltenen Verpflichtungen erforderlich sind.

2 Umsetzung nachhaltiger Sicherungsmaßnahmen für die Datenverarbeitung

Für alle Formen der Datenverarbeitung sollten die Arbeitgeber die Wahrung folgender Sicherheitsvorkehrungen gewährleisten. Insbesondere:

a) Die Beschäftigten sollten vor der Einführung von Informationssystemen und -technologien, die die Überwachung ihrer Tätigkeiten ermöglichen, klar und umfassend informiert werden. Die Informationen sollten auf dem neuesten Stand gehalten werden und untenstehenden Grundsatz 3 berücksichtigen. Die Informationen sollten auch den Zweck der Maßnahme, den Speicherungs- oder Back-up-Zeitraum sowie die Existenz der Arbeitnehmerrechte auf Zugriff und Berichtigung und wie diese Rechte ausgeübt werden könnten, umfassen. Zu dieser Sicherungsmaßnahme gehört auch, mitzuteilen, wenn sich Überwachungszweck und Systeme ändern;
b) Es sollten geeignete interne Maßnahmen im Zusammenhang mit der Verarbeitung dieser Daten ergriffen und die Beschäftigten im Vorfeld benachrichtigt werden. Dazu gehört die Durchführung einer Bewertung der Auswirkungen auf die Privatsphäre, wenn Technologien zu einem hohen Risiko für den Einzelnen führen können, wie etwa im Fall einer potenziellen Profilerstellung oder wenn Entscheidungen anhand von automatisierten Systemen gefällt werden (siehe Grundsatz 5 unten).
c) In Situationen, in denen vermutet wird, dass die Arbeitnehmerrechte auf Wahrung der Privatsphäre und der menschlichen Würde möglicherweise verletzt wurden, sollte Rücksprache mit den Mitarbeitern gehalten werden. In den genannten Fällen sollte das Recht eines jeden Arbeitnehmers auf Einspruch im Hinblick auf die genannte Datenüberwachung gewahrt werden, bis der Arbeitnehmer schriftlich beweisen kann, dass die Arbeitnehmerrechte auf Achtung der Privatsphäre und der menschlichen Würde

vollkommen gewahrt werden und er anschließend die Zustimmung des Arbeitnehmers erhält (siehe Grundsatz 5);

d) Gemäß innerstaatlichem Recht sollte die nationale Aufsichtsbehörde für die Verarbeitung personenbezogener Daten konsultiert werden.

3 Der Grundsatz der Datenminimierung muss angewendet werden

Nach diesem Grundsatz dürfen die Arbeitgeber nur:

> „Daten sammeln und nur die richtigen Daten für die richtigen Zwecke und nur für die richtigen Zwecke, die von den richtigen Menschen und nur von den richtigen Menschen über den entsprechenden Zeitraum und nur über den entsprechenden Zeitraum genutzt werden."

Die Arbeitgeber sollten geeignete Maßnahmen entwickeln, um sicherzustellen, dass Sie die Grundsätze und Verpflichtungen in Bezug auf die Verarbeitung von Daten für Beschäftigungszwecke in der Praxis wahren. Dies umfasst die Grundsätze der Verhältnismäßigkeit und der Subsidiarität: Die Datenerhebung muss auf das Notwendige begrenzt sein, um die Ziele der jeweiligen Datensammlung zu erreichen, d. h., dass Inhalt und Form der Maßnahme im Einklang mit dem angestrebten Ziel stehen müssen.

Auf Antrag der Aufsichtsbehörde sollten Arbeitgeber in der Lage sein, ihre Einhaltung solcher Grundsätze und Verpflichtungen nachzuweisen. Diese Maßnahmen sollten an den Umfang und das Wesen der verarbeiteten Daten und die Art von durchgeführten Aktivitäten angepasst werden und es sollten etwaige Auswirkungen auf Grundrechte und -freiheiten der Arbeitnehmer berücksichtigt werden.

4 Datenverarbeitung muss transparent sein

a) Informationen über personenbezogene Daten, die sich im Besitz von Arbeitgebern befinden, sollten dem oder der unmittelbar betroffenen Arbeitnehmer/in entweder direkt oder über ihre oder seine Vertreter zur Verfügung gestellt werden oder ihm oder ihr über andere geeignete Mittel zur Kenntnis gebracht werden.

b) Die Arbeitgeber sollten Mitarbeitern folgende Informationen bereitstellen:
   i. die Kategorien von zu verarbeitenden personenbezogenen Daten und eine Beschreibung der Zwecke dieser Verarbeitung;
   ii. die Empfänger oder Empfängerkategorien der personenbezogenen Daten;
   iii. die Möglichkeiten, die Arbeitgeber zur Ausübung ihrer in Grundsatz 1 dargelegten Rechte haben, unbeschadet günstigerer Möglichkeiten, die vom innerstaatlichen Recht oder in ihrer Rechtsordnung vorgesehen sind;
   iv. und alle sonstigen Informationen, die notwendig sind, um eine gerechte und rechtmäßige Datenverarbeitung zu gewährleisten.

c) Von den Kategorien personenbezogener Daten, die von IKT-Systemen gesammelt werden können, einschließlich einer Videoüberwachung und deren möglicher Verwendung, muss eine klare und vollständige Beschreibung vorgelegt werden.

d) Die Angaben sollen in einem zugänglichen Format vorgelegt und auf dem neuesten Stand gehalten werden. Auf jeden Fall sollten solche Informationen zur Verfügung gestellt

werden, bevor ein Mitarbeiter die jeweilige Tätigkeit oder Maßnahme durchführt und über die Informationssysteme, die normalerweise von dem Mitarbeiter benutzt werden, ohne Weiteres verfügbar gemacht werden.

5 Gesetze zum Schutz der Privatsphäre und Grundrechte müssen im gesamten Unternehmen geachtet werden

Dies schließt die Wahrung aller globalen und regionalen Übereinkommen über Menschenrechte ein[1], darunter auch:

- die Allgemeine Erklärung der Menschenrechte der Vereinten Nationen
- der Verhaltenskodex des Internationalen Arbeitsamtes von 1997 zum Schutz der personenbezogenen Daten von Arbeitnehmern.

Der Arbeitgeber muss auch:

a) Respekt vor der Menschenwürde zeigen. Privatsphäre und der Schutz personenbezogener Daten sollten bei der Verarbeitung von personenbezogenen Daten zu Beschäftigungszwecken sichergestellt sein, insbesondere um die freie Entfaltung der Persönlichkeit des Beschäftigten und den Aufbau individueller und sozialer Beziehungen am Arbeitsplatz zu ermöglichen.
b) Die Kommunikation muss rechtmäßig sein und darf keine beleidigenden oder verleumderischen Äußerungen enthalten.
c) Firmeneigene Kommunikationseinrichtungen dürfen nicht als Mittel der sexuellen Belästigung oder zur Verbreitung anstößiger Kommentare mit der Absicht der Diskriminierung benutzt werden.

Der Arbeitgeber kann für die interne und externe Kommunikation von Beschäftigten einen Haftungsausschluss verlangen, um festzuhalten, dass die zum Ausdruck gebrachten Ansichten ausschließlich jene des Autors und nicht des Unternehmens sind.

6 Arbeitnehmer müssen volles Recht auf Erklärung haben, wenn Daten verwendet werden

Dieser Grundsatz bezieht sich auf Entscheidungen, die von der Geschäftsleitung getroffen werden. Dies beinhaltet die Erfassung von Daten sowohl innerhalb als auch außerhalb des Unternehmens. Bei internen und externen Einstellungsverfahren müssen die Arbeitnehmer das Recht darauf haben, zu wissen, auf welcher Grundlage eine Entscheidung getroffen wurde. Das soll die Arbeitnehmer vor diskriminierenden Entscheidungen auf der Grundlage von datenbasierten Vorhersagen nicht zuletzt im Hinblick auf ihre Gesundheit schützen.

Die Beschäftigten müssen informiert werden, wenn wichtige Entscheidungen basierend sowohl auf internen als auch auf externen Daten getroffen werden.

[1] http://www.ohchr.org/Documents/Publications/CoreTreatiesen.pdf

7 Biometrische Daten und persönlich identifizierende Informationen (PII) müssen ausgenommen werden

Das Sammeln und Weiterverarbeiten von biometrischen Daten sollte nur durchgeführt werden, wenn keine anderen, weniger einschneidenden Mittel zur Verfügung stehen und nur, wenn sie von geeigneten Vorkehrungen, einschließlich der zusätzlichen Garantien gemäß Grundsatz 2 begleitet werden.

Die Verarbeitung biometrischer Daten und anderer PII sollte auf wissenschaftlich anerkannten Methoden basieren und sollte den Anforderungen strikter Sicherheit und Verhältnismäßigkeit entsprechen.

8 Systeme zur Ortung von Mitarbeitern

Systeme zur Ortung des Aufenthaltsorts der Mitarbeiter sollten nur eingeführt werden, wenn es sich als für die Erfüllung der rechtmäßigen Zwecke des Arbeitgebers erforderlich erweist und ihre Verwendung sollte nicht zur kontinuierlichen Überwachung von Beschäftigten führen. Insbesondere sollte Überwachung nicht der Zweck, sondern lediglich eine indirekte Konsequenz einer Maßnahme zum Schutz der Produktion, Gesundheit und Sicherheit oder zur Sicherung des effizienten Ablaufs eines Unternehmens oder einer Organisation sein. Angesichts des Potenzials zur Verletzung der Rechte und Freiheiten betroffener Personen durch die Verwendung dieser Systeme, sollten die Arbeitgeber sicherstellen, dass alle erforderlichen Sicherungsmaßnahmen für das Arbeitnehmerrecht auf Privatsphäre und Schutz personenbezogener Daten, einschließlich der in Grundsatz 2 vorgesehenen Sicherungsmaßnahmen gegeben sind.

In Übereinstimmung mit Grundsatz 3 über Datenminimalisierung sollten Arbeitgeber besonderes Augenmerk auf die Zwecke, für die solche Systeme verwendet werden, richten. Die Arbeitgeber sollten geeignete interne Verfahren im Zusammenhang mit der Verarbeitung dieser Daten anwenden und sollten die betroffenen Personen im Voraus darüber informieren.

9 Ein multidisziplinäres unternehmensübergreifendes Datenkontrollorgan sollte eingesetzt werden

Es sollte ein multidisziplinäres unternehmensübergreifendes Datenkontrollorgan eingesetzt werden. Dazu gehören Bestimmungen, dass alle in diesem Gremium sitzenden Vertreter, einschließlich Vertrauensleute, eine entsprechende datenbezogene Schulung erhalten, um für die Arbeit mit Unternehmen im Hinblick auf die Aufrechterhaltung und Wahrung einer nachhaltigen Datenschutzpolitik vorbereitet zu sein.

10 Alle oben genannten Punkte sollten in ein kollektives Abkommen implementiert werden

Die vorstehenden Grundsätze sollten über Tarifverhandlungen auf Unternehmens- oder Sektorebene implementiert und durchgesetzt werden. Gibt es keine solchen Tarifverhandlungen, sollte der Arbeitgeber ein Kontrollorgan gemäß Grundsatz 9 einsetzen.

Quellen:

In dieses Dokument sind Anregungen und Einsichten aus folgenden einschlägigen Dokumenten eingeflossen:

1) General Data Protection Regulation (Allgemeine Datenschutzbestimmung) (http://ec.europa.eu/justice/dataprotection/document/review2012/com_2012_11_en.pdf)

2) Europarat (2015) Empfehlung CM/Rec(2015) des Ministerkomitees an die Mitgliedstaaten über die Verarbeitung personenbezogener Daten im Rahmen des Arbeitsverhältnisses: https://www.apda.ad/system/files/cm-rec-2015-5-en.pdf

3) 2017): ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 2/2017 on data processing at work http://ec.europa.eu/newsroom/document.cfm?doc_id=45631