Datenethik – ein praktischer Zugang aus Sicht der Compliance

David Rosenthal, Partner VISCHER AG (Zürich)

Immer mehr Unternehmen halten es für angezeigt, sich im Umgang mit Daten auch an ethische Prinzipien zu halten. Das klingt gut und vermarktet sich auch so, doch was Datenethik wirklich bedeutet, bleibt für viele unklar. Eines ist aber gewiss: Um philosophische Fragen geht es meist nicht. Im Vordergrund steht der Wunsch, dass Unternehmen sich im Umgang mit Daten mässigen und nicht alles rechtlich Erlaubte auch tun. Der Ruf ist v.a. dort laut, wo die Öffentlichkeit wenig darüber weiss, was Unternehmen tatsächlich tun wie etwa im Bereich der künstlichen Intelligenz. Doch wie kann ein Unternehmen den ethischen Umgang mit Daten sicherstellen?

Das eine «richtige» Verhalten gibt es nicht

Klären wir zunächst die Begriffe. Wird von «Ethik» gesprochen, ist in der Regel Moral gemeint, nämlich Vorgaben für ein angebrachtes Verhalten. Die Zehn Gebote sind Ausdruck einer bestimmten Moral, nicht Ethik. Letztere meint die Disziplin, mit der unterschiedliche Moralvorstellungen analysiert werden. So gibt es weder die eine Ethik noch die eine Moral. Der kategorische Imperativ von Kant, wonach man nur nach der Maxime handeln solle, von der man zugleich wolle, dass sie ein allgemeines Gesetz sei, kann zwar einem Individuum als moralischer Kompass dienen, für ein Unternehmen passt dieses Prinzip jedoch nicht.

Die «Datenethik» als Begriff ist zwar in jüngster Zeit in Mode, den Umgang mit Daten beeinflusst das ihr unterliegende Prinzip aber schon seit langem: Nicht alles, was das Datenschutzrecht erlaubt, wird von den Beteiligten – Kunden, Mitarbeitern, Medien, Behörden, Politik, Influencern, Aktionären etc. – auch akzeptiert. Umgekehrt kann der Begriff auch dafür sorgen, dass an sich datenschutzwidriges Verhalten als richtig gilt. Es geht um den «gefühlten» im Gegensatz zum rechtlichen Datenschutz. Er bestimmt nicht nur die öffentliche Wahrnehmung. Auch Gerichte und Aufsichtsbehörden lassen sich trotz Gesetzmässigkeitsgebot von ihm leiten.

In einem Aufsatz aus dem Jahre 2012 (https://bit.ly/3kdPnJN) untersuchte ich das damals noch unausgesprochene Phänomen und definierte Regeln für objektivere Wertentscheide. Die Kernaussagen haben sich seither bestätigt. Will ein Unternehmen im Bereich der Datenbearbeitung Schwierigkeiten vermeiden, darf es sich nicht nur an den gesetzlichen Vorgaben ausrichten, sondern muss sich auch fragen, inwieweit die Stakeholder seinen Umgang mit (Personen-)Daten gutheissen (oder was sie als Personendaten erachten).

Auch wenn in Vorträgen, von Beratern oder in der Öffentlichkeit wohlklingend von «verantwortungsvollem», «ethischem» oder «fairem» Umgang mit Daten die Rede ist, geht es in den meisten Unternehmen schlicht darum, den unausgesprochenen Erwartungshaltungen der Stakeholder entgegenzukommen und dazu Regeln zu formulieren, die sich operationalisieren lassen. Dagegen ist auch dann nichts einzuwenden, wenn dies aus rein kommerziellen Überlegungen geschieht.

Der Begriff des «gefühlten» Datenschutzes beschreibt zwar einen zentralen Aspekt des Phänomens, hilft in der praktischen Umsetzung aber oft nicht weiter. Datenethik ist auch nicht Datenschutz, wenn der Begriff als rein rechtliche Vorgabe verstanden wird, wie dies in der Compliance der Fall sein sollte. Dass Unternehmen nicht nur rechtlichen Vorgaben folgen, ist jedoch nicht ungewöhnlich. Nötig ist aber ein passender Compliance-Prozess mit klaren Vorgaben. Fehlt er, bleibt Datenethik ein Lippenbekenntnis, Placebo für ein gutes Gewissen oder ein Experiment mit unberechenbarem Ergebnis.

DEFINITION

Moral und Ethik sind keine Synonyme. Unter dem Begriff der Moral sind Vorgaben für ein angebrachtes Verhalten zu verstehen. Ethik hingegen bezeichnet die philosophische Disziplin, mit der unterschiedliche Moralvorstellungen analysiert werden.

Verhaltenskodizes oft nur Marketing?

Manche Ansätze hierzu haben sich als nicht sehr erfolgreich erwiesen. Ethik-Richtlinien klingen gut, fallen jedoch meist so generisch aus, dass sie für eine Operationalisierung unbrauchbar sind. «Don't be evil» verlangt Googles Ethik-Code seit 20 Jahren, und doch gehen die Meinungen, was darunter zu verstehen ist, weit auseinander. Auch Ethik-

Beauftragte erweisen sich leider häufig als Alibi- und Marketingübung: Sie haben in der Second Line richtigerweise keine Entscheidbefugnisse, werden in ihren Ansichten vom Business aber oft nicht akzeptiert, weil als subjektiv wahrgenommen und da Moral kein der fachlichen Expertise zugängliches Thema ist. Ein Experte kann einem Unternehmen höchstens Erfahrung im Umgang mit bestimmten Themen durch andere Unternehmen bieten.

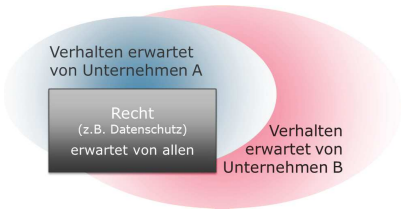
Auch Verhaltenskodizes von Verbänden sind oft keine Lösung, da sie zwar zeigen mögen, welche Themen unter den Nägeln brennen, sie sich aber gerne auf Allgemeinplätze und generische Appelle beschränken, nur den kleinsten gemeinsamen Nenner wiedergeben oder schlicht schöner oder detaillierter ausformulieren, was ohnehin von Gesetzes wegen gelten würde. Die Bekenntnisse in der jüngst veröffentlichten «Swico Charta für den ethischen Umgang mit Daten» gehen zum Beispiel in diese Richtung.

Realität ist hingegen, dass Datenethik in der Datenschutzberatung bereits stattfindet, indem Datenschutzstellen in den Betrieben die ihnen vorgelegten Vorhaben bewusst und noch öfters unbewusst nicht nach dem beurteilen, was der Gesetzgeber wirklich verlangt, sondern was sich nach ihrer Wahrnehmung gehört; ein Grund ist, dass die Grenzen zwischen beidem, selbst behördenseitig, längst verwaschen sind. Dies ist doppelt unbefriedigend: Erstens sind solche Einschätzungen vom Zufall geprägt und zweitens führen sie schleichend zur Verschärfung der Rechtslage. Richtig wäre, zwischen gesetzlichem und übergesetzlichem Verhalten klar zu trennen und sich bei Bedarf bewusst für Letzteres zu entscheiden.

Warum Unternehmen Datenethik betreiben

Um die Sache systematischer anzugehen, sollte sich ein Unternehmen zuerst im Klaren darüber werden, was es sich von Datenethik ehrlicherweise verspricht. Das bessere externe oder auch interne Image ist nur ein Grund. Die Vermeidung rechtlicher, regulatorischer oder gesetzgeberischer Interventionen ist ein weiterer (die DSGVO verdanken wir dem als unpassend empfundenen Verhalten der Internet-Konzerne). Datenethik kann auch der Förderung einer bestimmten Kultur, Einstellung oder Denkweise im Betrieb dienen.

Sind die Erwartungen geklärt, muss das Unternehmen seine eigene Datenethik (besser: Datenmoral) definieren. Auch wenn die Mantren gewisser Ethiker das Gegenteil suggerieren, gibt es keine universell gültige Regelung für den richtigen Umgang mit Daten in Unternehmen. Denn Recht und Ethik sind unterschiedliche Regelwerke:



Eine bestimmte Datenanalyse mag für eine Grossbank ein No-Go sein, während sie bei einer jungen Internet-Bank zum guten Stil gehören kann. An diesem Punkt sind Unternehmen versucht, einen Satz an Regeln festzulegen, an welchem sie ihre künftigen Datenbearbeitungen ausrichten, wie z.B. dass eine Versicherung ihre Kundendaten nie für versicherungsfremde Zwecke nutzt. Das funktioniert meist nicht wirklich, da dazu alle künftig denkbaren Formen der Datennutzung in all ihren Facetten schon bekannt sein müssten. Sind sie aber nicht. Es entstehen Regeln der Vergangenheit.

Bewährt hat es sich, den Prozess umzudrehen: Die Regeln werden nicht vorab definiert, sondern es wird eine Ethik-Praxis anhand konkreter Projekte entwickelt. Und es wird mit Werten gearbeitet, die zeitloser sind. Das hat den Vorteil, dass einzelfallgerecht entschieden werden kann, ohne dass starre Regeln geschaffen werden, die Innovation verhindern. Der Nachteil ist die fehlende Vorhersehbarkeit: Soll die First Line über den gesetzlichen Datenschutz hinausgehende Restriktionen einhalten, muss sie die Spielregeln kennen, damit sie diese bei der Ausgestaltung ihrer Projekte einplanen kann. Messgrössen wie «soziale Akzeptanz» sind jedoch keine Spielregeln und daher untauglich.

ACHTUNG

Haben Unternehmen definiert, was aus ihrer Sicht Datenethik bzw. Datenmoral ist, werden danach typischerweise konkrete Regelsätze ausgearbeitet, an denen sie sich bei der Datenbearbeitung orientieren können. Dieses Vorgehen ist allerdings nicht optimal, da starr formulierte, oft fallbezogene Regeln nicht zielführend sind, um zukünftige Entwicklungen abzudecken.

Jedem Unternehmen seine eigene Datenmoral

Vorangehend genanntes Manko wird in der Praxis so gelöst, dass Unternehmen einerseits einen Datenethik-Beurteilungsprozess für Projekte und andererseits Vorgaben zur Beurteilung festlegen. Bewährt hat sich, dass ein Unternehmen fünf bis sieben Kriterien definiert, anhand derer es Datenbearbeitungen in ethischer Hinsicht beurteilen will. Das sind keine Regeln, sondern auf Wertvorstellungen basierende Ziele, wie z.B. «Keine Diskriminierung», «Nutzen für Kunden», «Entscheidfreiheit wahren» oder «Transparenz». Auch die zitierte Swico Charta nennt solche, wie etwa «Schadenvermeidung». Es geht nicht um Vollständigkeit, sondern um eine zum Unternehmen passende Auswahl, entsprechend den Werten, die das Unternehmen den anvisierten Stakeholdern vermitteln will. Sie bildet die Basis seiner Datenmoral.

Der Beurteilungsprozess wiederum sollte wie ein klassischer Compliance-Prozess organisiert sein. Jede geplante Datenbearbeitung wird ihm unterzogen, beispielsweise nach erfolgter Datenschutzprüfung. In einer Vorprüfung durch die Compliance-Stelle wird geklärt, ob die Datenbearbeitung ethische Fragen aufwirft oder andere Aufgreifkriterien gegeben sind, die eine eingehende Prüfung erfordern. Sie ist also nur nötig, wenn etwaige ethische Vorbehalte bestehen, die mit ihr ausgeräumt werden oder eben nicht. Diese Prüfung wird inhaltlich nicht von der Compliance-Stelle vorgenommen, sie begleitet die Prüfung aber und stellt sicher, dass diese in strukturierter Weise erfolgt. Dies ist für die Entscheidqualität und damit die Vorhersehbarkeit wichtig.

Bezüglich der Prüfung der heiklen Datenbearbeitungen hat sich die Beurteilung durch eine Gruppe statt einzelner Personen bewährt, also eine Ethik-Kommission oder ein Datenethik-Board. Sie sollte divers zusammengesetzt sein. Juristen oder Datenschützer sind nicht nötig, da es nicht um rechtliche Fragen geht. In der Gruppe sollte nicht nur die First Line vertreten sein und nicht nur oberes Kader. Das Gremium sollte geheim beraten, nur in Vollbesetzung entscheiden, es sollte Stimmzwang herrschen und Entscheide sollten mit qualifiziertem Mehr erfolgen. Ist der Entscheid getroffen, sollte er vom gesamten Gremium vertreten werden (Kollegialitätsprinzip). Dies alles dient letztlich der Entscheidhygiene und der Akzeptanz der Entscheide.

Beides setzt voraus, dass die Entscheide in der Gruppe strukturiert getroffen werden und nicht einfach nach «wilder» Beratung. Wird ein Projekt dem Gremium vorgelegt, erhalten die Vertreter des Projekts die Gelegenheit, es vorzustellen und darzulegen, inwiefern es jedem der definierten Kriterien gerecht wird. In der Beratung wird das Projekt bezüglich jedem dieser Kriterien von den Mitgliedern des Gremiums bewertet, diskutiert und erneut bewertet. Sind alle Aspekte bewertet worden, wird darüber entschieden, ob die Umsetzung des Projekts uneingeschränkt oder nur mit Auflagen oder Vorbehalten empfohlen oder nicht empfohlen wird. Die Punktzahl ist nicht bindend, sondern hilft einzig, qualitativ bessere Entscheide zu treffen. Diese müssen zudem begründet werden.

Der Endentscheid zur Umsetzung liegt wiederum nicht bei diesem Gremium, sondern bei der Unternehmensleitung als Organ der First Line. Abweichen wird sie in der Praxis allerdings nur selten.

Konstanz und Akzeptanz durch dokumentierte Fallpraxis

Auf die erläuterte Weise kann ein Unternehmen seine eigene Datenethik anhand konkreter Projekte entwickeln und ohne feste Regeln fortschreiben, den Projektverantwortlichen über die fünf bis sieben Kriterien und den strukturierten Prozess aber trotzdem eine gewisse Vorhersehbarkeit bieten. Ihre Vorhaben werden nicht einfach nach Bauchgefühl, sondern nach objektivierten Massstäben beurteilt, an denen sie sich ausrichten können – in der Gestaltung ihrer Projekte und in deren Präsentation vor dem Gremium. Auch dies ist für die Akzeptanz wichtig. Zugleich besteht damit ein geordneter Compliance-Prozess, der von der Second Line begleitet werden kann.

Dem Sammeln und internen Publizieren der Empfehlungen kommt dabei eine wichtige Rolle zu: Es entsteht so eine Fallpraxis, welche allen Beteiligten die Beurteilung neuer Projekte erleichtert und für zusätzliche Verlässlichkeit sorgt. Die Compliance-Stelle wiederum erhält damit die nötigen Quellen, um die First Line in der Ausgestaltung ihrer Vorhaben zu beraten und zu unterstützen.

Der Prozess, der sich im Bereich der Datenethik bereits bewährt hat, lässt sich in ähnlicher Form auch in anderen Fragen als nur für solche zum ethischen Umgang mit Daten einsetzen. Während für die externe Kommunikation die vom Unternehmen definierten Werte wichtig sein werden, ist für den internen Erfolg die Operationalisierung und Berechenbarkeit des Vorgangs meist wichtiger. Unternehmen kämpfen in der Regel mit Letzterem, nicht Ersterem.

ÜBER DEN AUTOR

David Rosenthal ist Partner bei der Wirtschaftskanzlei VISCHER AG in Zürich. Zudem ist er als Lehrbeauftragter an der ETH Zürich sowie an der Universität Basel tätig und Autor zahlreicher Publikationen unter anderem zum Datenrecht.