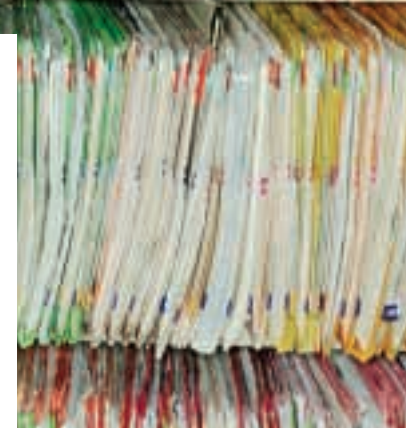




Datenschutzrechtliche Aspekte des Data Mining



Data Mining wird eingesetzt, um aus grossen Datenbeständen neue Zusammenhänge zu erkennen. Haben die benutzten Daten einen erkennbaren Bezug zu bestimmten oder bestimmbar Personen, fällt das Data Mining in den Geltungsbereich des Datenschutzrechts. Die in diesem Zusammenhang wesentlichen Grundsätze des Datenschutzes werden hier erläutert.

Beim Data Mining sollen durch den Einsatz verschiedener Verfahren und Methoden aus grossen Datenbeständen neue Wissenszusammenhänge generiert und bessere Kenntnisse gewonnen werden: über das eigene Unternehmen (Management-Informationssysteme), zur Analyse von Kundenverhalten, zur Erarbeitung spezifisch darauf abgestimmter Angebote oder für Zwecke der wissenschaftlichen Forschung und der Statistik. Mehr dazu im Artikel von Beat Wallimann auf den Seiten 10 bis 12.

Auch im Gesundheitswesen ist ein grosses Interesse am Data Mining erkennbar – sei es im Zusammenhang mit der Diskussion um Kosten und Tarife, dem Qualitätsmanagement oder der medizini-

schen Forschung. Hier zeigt sich das Spannungsverhältnis zum Datenschutz in aller Schärfe. Einerseits gelten Gesundheitsdaten im Datenschutzrecht als besonders schützenswerte Daten und deren Bearbeitung unterliegt erhöhten rechtlichen Anforderungen. Andererseits sind Ärzte und weitere Medizinalpersonen in Bezug auf die ihnen von den PatientInnen anvertrauten Tatsachen der Geheimhaltungspflicht unterstellt. Datenschutz und Arztgeheimnis stehen somit einem uneingeschränkten Data Mining entgegen.

Unproblematische Verwendung anonymer Daten

Datenschutzrechtlich unproblematisch ist Data Mining dann, wenn dabei anonyme Daten genutzt werden. Anonyme bzw. anonymisierte Daten dürfen keine Rückschlüsse auf die betroffenen Personen erlauben und sind somit keine geschützten Personendaten im Sinne des Datenschutzgesetzes. Sie unterliegen auch nicht den Berufsgeheimnissen, wie etwa dem Arztgeheimnis. Data Mining mit solchen Daten ist unbeschränkt zulässig. Es empfiehlt sich daher, immer zu prüfen, ob Personendaten, die für Zwecke des Data Mining Verwendung finden sollen, vorgängig anonymisiert

worden sind – ohne Möglichkeit der Reidentifizierung der betroffenen Personen. In vielen Fällen, beispielsweise in der Forschung oder der Statistik, genügen anonyme Daten zur Datenanalyse im Rahmen des Data Mining. Eine Anonymisierung der Daten ist jedoch nicht immer möglich oder wirtschaftlich sinnvoll.

Vorsicht bei der Verwendung personenbezogener Daten

Wo für das Data Mining personenbezogene Daten verwendet werden – also solche, die sich auf bestimmte (eindeutig identifizierte) oder bestimmbare Personen (unter Verwendung zusätzlicher Informationen ebenfalls eindeutig zuordenbare Daten) beziehen –, ist dies nur unter Beachtung des Datenschutzrechts zulässig. Besondere Regeln gelten zudem für Daten, die durch ein Berufsgeheimnis – wie das Arztgeheimnis – geschützt sind. Lassen sich diese Daten nicht anonymisieren, so ist deren Bearbeitung nur unter zusätzlichen besonderen Ausnahmebestimmungen zulässig, wie sie zum Beispiel für die Verwendung von PatientInnen Daten für die medizinische Forschung gelten.

Zweckbestimmungsgebot

Von besonderer Bedeutung im Zusammenhang mit dem Data Mining ist der allgemeine datenschutzrechtliche Grundsatz, wonach Personendaten nur für diejenigen Zwecke verwendet werden dürfen, die bei der Beschaffung der Daten gegenüber den betroffenen Personen angegeben wurden, für diese aus den Umständen ersichtlich waren oder gesetzlich vorgesehen sind. Die Daten von KundInnen bzw. PatientInnen dürfen nach diesem Grundsatz ohne weiteres zur Abwicklung der entsprechenden KundInnen- bzw. PatientInnenverträge, etwa für die Rechnungsstellung, verwendet werden. Eine Verwendung der Daten zum Beispiel für das Direktmarketing ist hingegen nicht vorbehaltlos zulässig, weil diese Art der Verwendung ihrer Daten zum Zeitpunkt der Datenbekanntgabe für die KundInnen bzw. PatientInnen nicht erkennbar war.

Erforderliche Einwilligung der Betroffenen

Datenbearbeitung zu Zwecken, die bei der Erhebung der Daten für die Betroffenen nicht ersichtlich sind, bedürfen der ausdrücklichen oder stillschweigenden Einwilligung der Betroffenen. Eine rechtsgültige Einwilligung setzt voraus, dass sie der Einwilligende in Kenntnis ihrer Tragweite erteilt hat. Eine abstrakt formulierte Einwilligung, wonach zum Beispiel zu sämtlichen künftig möglichen Datenbearbeitungen generell eingewilligt wird, ist rechtlich nicht genügend.

Wenn Daten für das Data Mining genutzt werden sollen, ist es daher erforderlich, die Betroffenen bei der Erhebung der Daten darüber zu informieren, dass diese für bestimmte Zwecke verwendet werden sollen. Dies stellt an die Information und die Formulierung des Einwilligungstextes erhöhte Anforderungen, da mit dem Data Mining typischerweise neue, möglicherweise überraschende Er-

kenntnisse gewonnen werden können. Zu welchen Zwecken dieses Wissen verwendet wird, ist im Voraus nicht immer absehbar, sondern ergibt sich oft erst aus den Erkenntnissen selbst.

Hinreichend präzise Formulierung der Nutzungszwecke

Information und Einwilligung der Betroffenen könnten beispielsweise dahin gehend formuliert werden, dass die Daten mittels Data Mining dazu genutzt werden sollen, um auf die Betroffenen zugeschnittene Angebote zu erstellen oder um für bestimmte Zwecke Forschung zu betreiben. Data Mining für Zwecke, die ausserhalb dessen liegen, womit die Betroffenen bei der Datenerhebung rechnen mussten, sind nach der geltenden Rechtslage unzulässig. Eine Ausnahme gilt lediglich dort, wo für eine Datenbearbeitung ein gesetzlicher Rechtfertigungsgrund besteht. Für private Unternehmen ist dies nur ausnahmsweise und unter besonderen Voraussetzungen denkbar. Für die Datenbearbeitung durch Behörden und öffentliche Institutionen verhält es sich demgegenüber anders.

Fortsetzung auf Seite 19

LES ASPECTS DE LA PROTECTION DES DONNÉES DANS LE DATA MINING

Du point de vue de la protection des données, seul un «data mining» basé sur une anonymisation des informations étudiées est légal et ne comporte aucun risque de dérapage.

Si on travaille avec des données sensibles qui touchent à la personnalité, les personnes concernées doivent donner leur consentement. Ceci présuppose bien entendu que ces dernières soient avisées et disposent des informations appropriées.

Les administrations et les institutions publiques qui exploitent ce type d'informations sont soumises aux réglementations en vigueur et ne sont autorisées à effectuer du «data mining» qu'en respectant ces prescriptions. Les données qui ne sont plus utilisées pour leurs objectifs initiaux doivent être supprimées sans retard. Tous ces aspects sont à considérer dès la phase de planification d'un projet et doivent être appliqués de manière professionnelle tout au long de sa réalisation. Car seule une exploitation de données en accord avec la législation favorisera l'acceptation du «data mining» par les personnes concernées.

DR. URSULA WIDMER

Die Autorin ist Rechtsanwältin in Bern und Lehrbeauftragte für Informatikrecht an der Universität Bern. Ihre Anwaltskanzlei, Dr. Widmer & Partner, ist spezialisiert auf Fragen des Informatik-, Internet- und E-Businessrechts – insbesondere auch im Medizinalbereich – sowie des Telekommunikationsrechts.

Kontakt:
ursula.widmer@widmerpartners-lawyers.ch



Fortsetzung von Seite 17

Wahrung gesetzlicher Aufgaben durch die öffentliche Hand

Datenbearbeitung durch Behörden und öffentliche Institutionen – etwa öffentliche Spitäler – ist nur insoweit zulässig, als sie im Rahmen der gesetzlichen Aufgaben der betreffenden Behörde bzw. Institution erfolgt. Data Mining ist daher nur insoweit zulässig, als die damit verfolgte Erkenntnis neuer Wissenszusammenhänge zwischen Daten der Erfüllung der gesetzlichen Aufgaben dient. Und auch bei Vorliegen der Einwilligung der Betroffenen ist für Behörden und öffentliche Institutionen eine Datenbearbeitung ohne die erwähnte gesetzliche Grundlage nicht zulässig.

Grundsatz der Verhältnismässigkeit

Sowohl von Behörden und öffentlichen Institutionen als auch von Privaten ist ein weiterer allgemeiner datenschutzrechtlicher Grundsatz, das Verhältnismässigkeitsprinzip, zu beachten. Personendaten dürfen nur so weit bearbeitet werden, als dies für die Bearbeitung nötig und zur Zweckerreichung geeignet ist. Im Zusammenhang mit dem Data Mining ist dabei problematisch, dass die Daten oft über lange Zeit in einem Data Warehouse gespeichert werden. Für Personendaten ist dies nur dann zulässig, wenn es zur Erfüllung des Datenverarbeitungszweckes nötig ist. Die Speicherung von Daten auf Vorrat für noch nicht bestimmte Zwecke ist unzulässig.

Management Summary

Aus datenschutzrechtlicher Sicht unbedenklich und ohne Einschränkung zulässig ist das Data Mining mit anonymisierten Daten. Falls personenbezogene Daten verwendet werden, verlangt der Grundsatz der Zweckbindung, dass die Einwilligung der Betroffenen vorliegt. Dies setzt bei der Erhebung der Daten die entsprechende Information der Betroffenen voraus. Nicht zulässig ist hingegen die Verwendung von Daten zu beliebigen Zwecken, mit denen die Betroffenen anlässlich der Erhebung nicht zu rechnen brauchten. Behörden und öffentliche Institutionen sind bei der Datenbearbeitung generell an ihre gesetzlichen Aufgaben gebunden. Ein Data Mining ist für sie nur in diesem Rahmen zulässig. Bei der Aufbewahrung von Daten verlangt der Grundsatz der Verhältnismässigkeit, dass Daten, die für die ursprünglich erhobenen Zwecke nicht mehr benötigt werden, zu löschen sind. Es ist daher nicht zulässig, Daten in Data Warehouses auf unbestimmte Zeit zu speichern, um diese gegebenenfalls für beliebige, im Voraus nicht bestimmte Zwecke durch Data Mining zu nutzen.

Es ist wichtig, dass die erwähnten Aspekte des Datenschutzrechts bereits in der Planungsphase eines Data-Mining-Projektes erkannt und im Rahmen der Implementierung rechtzeitig und professionell umgesetzt werden. Denn gesetzeskonforme Datenverarbeitung ist Basis für eine breite Akzeptanz von Data Mining durch die Betroffenen.

Umsetzung der Informationssicherheitspolitik. Der SAS ist als Stabsstelle direkt der Geschäftsleitung unterstellt.

Vertraulichkeit, Verfügbarkeit, Verbindlichkeit

Das primäre Ziel der Medgate-Informationssicherheit ist die Einhaltung der rechtlichen Rahmenbedingungen, die vor allem die Vertraulichkeit der Daten im Auge haben. Darüber hinaus gibt der Einsatz komplexer IT-Systeme drei weitere Ziele vor: hohe Verfügbarkeit der Informationen, Garantie der Integrität oder Richtigkeit sowie Verbindlichkeit (Nachvollziehbarkeit) der Informationen.

Als Grundlage der Sicherheitskonzepte dienen dem Medgate-Sicherheitsausschuss neben den gesetzlichen Grundlagen der ISO-Standard 17799 und für die Massnahmenplanung das Grundschutzhandbuch des Deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI). Im Rahmen des Krisenmanagements wurden ein Notfallkonzept und ein Disaster-Recovery-Konzept entwickelt, um die mit den KundInnen vereinbarte Verfügbarkeit der Dienstleistungen garantieren zu können. Massnahmen, die

den sicheren Umgang mit PatientInneninformationen betreffen, werden vor allem bei der Konzeption und Anwendung der Informations- und Kommunikationstechnologie (IKT) umgesetzt. Ein ebenso wichtiger Bestandteil der Informationssicherheit ist die regelmässige Information und Schulung der Mitarbeitenden im Umgang mit vertraulichen und sensiblen Daten sowie im Verhalten in Krisensituationen.

DR. MED. DANIEL MÜLLER

Der Autor arbeitet beim medizinischen Beratungszentrum Medgate als Abteilungsleiter Medizinische Netzwerke und leitet den internen Sicherheitsausschuss. Er ist FH-NDK-zertifiziert in Datenschutz- und Informationssicherheit an der Hochschule für Wirtschaft in Luzern und bildet sich zurzeit an der Universität St. Gallen zum MBA aus.

Kontakt: daniel.mueller@medgate.ch

