



Liebe Leserin, lieber Leser

Einen Monat lang beherrscht die zweitwichtigste Nebensache der Welt die Zeitungen. Unser Newsletter macht da keine Ausnahme. In beiden Gerichtsentscheiden geht es um die Entlassung eines Fussballtrainers. Im ersten Fall stellt sich die Frage, ob zur Klärung der Ansprüche ein **Schiedsgericht** genügt oder ob ein ordentliches Gericht anzurufen ist. Der zweite Fall behandelt die **fristlose Entlassung** des Trainers.

Privates Surfen während der Arbeitszeit oder per Geschäftsmail schnell ein paar persönliche Dinge erledigen: Die Nutzung der IT-Infrastruktur sorgt immer wieder für Zündstoff. In unserem ersten Top-Thema sagen wir Ihnen, wie Sie mit einem **IT-Nutzungsreglement** allen Diskussionen einen Riegel schieben. Im zweiten Top-Thema lesen Sie den zweiten Teil unserer Serie über die **juristischen Konsequenzen für den Arbeitgeber im Fall eines Burnouts**.

Herzlichst Ihr

Mathias Liechti, Redaktor

IN DIESER AUSGABE:

- Top-Thema – IT-Nutzungsreglement Seite 1
- Praxisfälle – IT-Nutzungsreglement Seite 4
- Gerichtsentscheid – Schiedsgericht Seite 5
- Top-Thema – Burnout, 2. Teil Seite 8
- Gerichtsentscheid – Fristlose Entlassung Seite 10
- Arbeitshilfe – Fristlose Auflösung des Arbeitsverhältnisses Seite 12

Klare Regeln für einfachere Prozesse

Braucht es ein Reglement für die Nutzung der betrieblichen IT-Infrastruktur und den Umgang mit E-Mail und Internet? Aus vielen Gründen lohnt es sich für Unternehmen, klare Regeln für ihre Mitarbeitenden aufzustellen.

■ Von Elisabeth Glättli

Manch eine Unternehmensleitung mag beim Gedanken an ein neues Reglement zur Nutzung der betrieblichen IT-Infrastruktur und zum Umgang mit E-Mail und Internet wenig bis gar keine Begeisterung verspüren. Neue Regelungen sind unbeliebt, und der Aufwand dafür ist ebenfalls nicht attraktiv. Doch lohnt sich eine Auseinandersetzung mit der Nutzung der eigenen IT-Infrastruktur in verschiedener Hinsicht.

Organisation der eigenen Daten und Datenbearbeitung

Ein Reglement verhilft zu einer geordneten und übersichtlichen Datenbearbeitung. Oft fehlt die Übersicht, wo welche Daten bearbeitet werden. Oft fehlt es an internen Regelungen, wie mit den geschäftlichen Daten und Personendaten umzugehen ist. In einem Reglement kann bestimmt werden, wie und nach welcher Ordnung elektronische Daten

abzulegen, wie geschäftliche E-Mails zu versenden und zu speichern sind und was bei Abwesenheit oder Austritt von Mitarbeitenden zu beachten ist. Zudem können die Verantwortlichkeiten und die Berechtigungen bestimmt werden.

Effiziente Gestaltung der Geschäftsprozesse

Besteht Klarheit, wo welche Daten bearbeitet werden, vereinfacht dies die Geschäftsprozesse. Die erforderlichen Daten sind nachvollziehbar geordnet und auffindbar. Die Zuständigkeiten und der Zugriff auf die Daten sind überschaubar. Regelungen für den Versand und die Speicherung von E-Mails schaffen eine einheitliche und übersichtliche elektronische Korrespondenz, welche auch von anderen Personen oder bei Abwesenheit des



Nicht nur die Technik, auch die Regeln zu deren Nutzung müssen laufend angepasst werden.

gerade bearbeitenden Mitarbeitenden aufgefunden werden kann. Eine solche Gestaltung der Datenbearbeitung steigert die Effizienz und ein zielgerichtetes Vorgehen der Mitarbeitenden ebenso wie einen einheitlichen und klaren Auftritt gegen aussen.

Wahrnehmung der internen und externen datenschutzrechtlichen Verantwortlichkeit

Über die datenschutzrechtlichen Dos und Don'ts bestehen oft Unsicherheiten und wenig Bewusstsein. Folge eines unsachgemässen Umgangs mit Personendaten können Datenschutzverstösse sein. Ohne arbeitgeberseitige Weisungen besteht die Gefahr, dass Mitarbeitende oder der Arbeitgeber selbst Personendaten rechtswidrig bearbeiten, indem etwa Personendaten unbefugterweise bekannt gegeben werden oder der Arbeitgeber unzulässigerweise Einsicht in private Daten der Mitarbeitenden nimmt. Zudem können durch einen gesetzeswidrigen Umgang mit Daten der Schutz von Unternehmensgeheimnissen und Geheimhaltungspflichten gegenüber Kunden und anderen Personen verletzt und der Ruf des Unternehmens aufs Spiel gesetzt werden.

Produktiver Mitarbeitendeneinsatz

Übermässiges Mailen und Surfen der Mitarbeitenden für private Zwecke führt zu Beeinträchtigungen der Arbeitszeit und zu einer unsorgfältigen Arbeitsausführung. Mit klaren Richtlinien für die Nutzung des Internets und des Mailens zu privaten Zwecken kann solchem quantitativem Missbrauch des Internets und des E-Mail entgegengewirkt werden. Der Arbeitgeber kann überdies Nutzungsvorschriften inhaltlicher Art erlassen und definieren, welche Nutzungen im Betrieb verboten sind (z.B. Aufrufen von Internetseiten oder Versand von E-Mails mit illegalen Inhalten oder mit vom Arbeitgeber als unerlaubt definierten Inhalten, Mobbing, anonyme oder Massenmails). Zur Durchsetzung der Weisungen können Kontrollmöglichkeiten vorgesehen und Sanktionen festgelegt werden.

Prävention von IT-Pannen

Übermässiges Surfen, E-Mails oder das Herunterladen von Seiten von grossem Umfang können zu einer Gefährdung der Datensicherheit und der gesamten Nutzung der IT-Infrastruktur führen. So kann eine nicht sachgerechte Nutzung von Internet und E-Mail oder eine unregelmässige Anwendung von Peri-

pheriegeräten Überlastungen des Netzwerkes und der Speicherkapazität sowie Beeinträchtigungen des Systems durch eingeschleuste Viren, Würmer und Trojaner zur Folge haben. Mit Regelungen, welche gefährliches Tun einschränken oder untersagen, durch verbessertes Bewusstsein und allfällige Meldepflichten der Arbeitnehmenden kann derartigen Gefährdungen entgegengewirkt werden.

Compliance: Einhaltung des Datenschutzgesetzes (DSG)

Ein Reglement und die Auseinandersetzung mit der Datenbearbeitung im Unternehmen fördern das datenschutzrechtliche Know-how und die Compliance hinsichtlich der datenschutzrechtlichen Vorschriften, wie sie insbesondere im Bundesgesetz über den Datenschutz (DSG) vom 19. Juni 1992, in Kraft seit 1. Juli 1993, geregelt sind (vgl. auch Art. 328b OR). Das DSG enthält die grundsätzlichen Vorschriften für die Bearbeitung von Personendaten. Zentral ist, dass bei der Bearbeitung solcher Daten die Grundsätze der Verhältnismässigkeit, der Zweckbindung, der Richtigkeit und der Sicherheit der Datenbearbeitung eingehalten werden. Datenbekanntgaben setzen grundsätzlich die Einwilligung der betroffenen Person, ein überwiegendes Interesse des Bearbeiters oder eine gesetzliche Bestimmung voraus. Die betroffene Person hat gegenüber dem Inhaber einer Datensammlung ein Auskunftsrecht darüber, ob und welche Daten über sie bearbeitet werden (Art. 8 DSG).

Für das Unternehmen bedeutet dies etwa, dass einem Mitarbeitenden Einsicht in das gesamte Personaldossier gewährt werden muss (mittels Kopien), dass es für gewisse Datenerhebungen das Einverständnis des Mitarbeitenden braucht (z.B. Durchführung von Eignungstest, Schriftgutachten, Persönlichkeitsbeurteilungen, Bekanntgabe von Daten), dass der Arbeitgeber Daten nur beschränkt erheben und nur zweckgebunden verwenden darf, dass die Daten richtig sein und nach einer gewissen Zeit gelöscht werden müssen. Die Einsicht in private E-Mails ist grundsätzlich nicht zulässig, ebenso wie das Aufzeichnen aller Aktivitäten. Auswertungen von Logfiles (Protokollierungen der Internet- und E-Mail-Aktivitäten) zwecks Überwachung von E-Mail und Internet sind nur zulässig,



wenn sie vorher für den Mitarbeitenden erkennbar waren, das heisst, umschrieben und angekündigt wurden. Will ein Unternehmen die Datenbearbeitung in ein anderes Land auslagern, muss garantiert sein, dass ein dem DSG vergleichbarer, angemessener Datenschutz gewährleistet ist.

Werden die Auskunftspflicht oder andere bestimmte Informationspflichten vorsätzlich verletzt, ist dies strafbar. Ebenso kann auf Antrag bestraft werden, wer vorsätzlich geheime, besonders schützenswerte Personendaten oder Persönlichkeitsprofile unbefugt bekannt gibt, von denen er bei der Ausübung seines Berufes, der die Kenntnis solcher Daten erfordert, erfahren hat.

Anpassung an aktuelle Rechtsentwicklungen (EU-DSGVO, revidiertes DSG)

Die aktuellen Entwicklungen in der datenschutzrechtlichen Gesetzgebung, namentlich das Inkrafttreten der EU-Datenschutzgrundverordnung (DSGVO oder GDPR) für die Schweiz am 25. Mai 2018 und gelegentlich die Totalrevision des schweizerischen

Datenschutzgesetzes (DSG), machen eine Auseinandersetzung mit dem Datenschutz unerlässlich. Eine bereits vorhandene Inventarisierung und Ordnung der Datenbearbeitung ist dabei eine grosse Hilfe für die Beurteilung, ob bei den anstehenden Gesetzesänderungen Massnahmen im Unternehmen ergriffen werden müssen.

Die DSGVO sieht unter anderem erweiterte Informationspflichten mit einem Ausbau der Rechte der Betroffenen, Dokumentations- und Meldepflichten sowie Datensicherheitsmassnahmen vor. Anwendbar ist die DSGVO, wenn Daten im Zusammenhang mit einer Niederlassung oder einem Auftragsverarbeiter in der EU bearbeitet werden, aber auch, wenn – ohne Niederlassung in der EU – EU-Bürgern Waren oder Dienstleistungen angeboten werden oder das Verhalten von Personen in der EU, namentlich bei der Nutzung des Internets, beobachtet wird.

Die DSGVO sieht bei Widerhandlungen erhebliche Sanktionen vor, so etwa Bussen bis EUR 20 Mio. oder 4 Prozent des weltweiten

Jahresumsatzes. Der Entwurf zur Totalrevision des DSG wurde der DSGVO angenähert, damit die Schweiz weiterhin als Drittstaat mit einem angemessenen Datenschutzniveau anerkannt ist und die grenzüberschreitende Datenübermittlung möglich bleibt. Der Entwurf zum totalrevidierten DSG sieht nun Bussen bis CHF 250 000.– vor.

Eine Überprüfung, ob und inwiefern die eigene Geschäftstätigkeit an die Bestimmungen der EU-DSGVO oder an die kommende Totalrevision des DSG angepasst werden muss, setzt die Inventarisierung der Datenbearbeitung im Unternehmen voraus. Eine Bestandesaufnahme und Regelungen des Datenschutzes im eigenen Unternehmen sind eine gute Grundlage dafür und erfolgen daher am besten so umgehend wie möglich.



AUTORIN

RA Dr. Elisabeth Glättli ist Fachanwältin SAV Arbeitsrecht und Inhaberin und Geschäftsführerin ihrer Anwaltskanzlei glättli partner in Winterthur. www.glattlipartner.ch

Alles richtig... dank prozessgeführter
HR- und Payroll-Administration



Wie bekommen Sie Ihre ELM-Prozesse in den Griff?

PerSal[®] **nearo**
silver edition

mehr zu den intelligenten Daten-Assistenten auf www.persal.ch



Fragen & Antworten

So erstellen Sie ein Nutzungsreglement

Viele Unternehmen erlassen eigene Weisungen zur Nutzung der IT-Infrastruktur. Wir sagen Ihnen, welche Punkte unbedingt in ein solches Reglement gehören und was es im Hinblick auf die DSGVO zu beachten gilt.

■ Von Elisabeth Glättli

Frage: Ist das Erstellen eines Reglements zur Nutzung der betrieblichen IT-Infrastruktur ein grosser Aufwand?

Antwort: Die Regelung der Nutzung der betrieblichen IT-Infrastruktur ist meist mit keinem sehr grossen Aufwand verbunden. Ein Arbeitgeber sollte sich namentlich fragen, welche privaten und geschäftlichen Nutzungen er als zweckmässig erachtet und welche Kontrollmöglichkeiten gewünscht und durchführbar sind. Ein grösserer Aufwand wäre für die Anpassung der Datenbearbeitung an die Regelungen der DSGVO erforderlich. Diese Regelungen betreffen die gesamte Geschäftstätigkeit des Unternehmens.

Frage: Was sollte in einem Reglement betreffend Nutzung von IT-Infrastruktur, E-Mail und Internet geregelt werden?

Antwort:

- 1) Richtlinien betreffend private Nutzung von E-Mail und Internet
 - a. Zulässigkeit oder Verbot der Nutzung des betrieblichen Internets und E-Mail-Accounts für private Zwecke
 - b. Nutzungsvorschriften in zeitlicher und inhaltlicher Art: Welche Nutzungen sind eingeschränkt, welche verboten? (Missbrauchsbestimmungen)
 - c. private E-Mails: Bezeichnung, Vertraulichkeit und Verpflichtung zur Löschung bei Austritt
- 2) Regelung betreffend geschäftliche E-Mails
 - a. Regeln für Betreff, Absender, Inhalt, Verschlüsselung, Speicherung sowie Weiterleitung bei Abwesenheit, Stellvertretung und Austritt
 - b. Evtl. Meldepflicht bei verdächtigen E-Mails
- 3) Evtl. Regelung betreffend Soziale Medien
- 4) Regelung betreffend Geschäftsdaten im Allgemeinen:
 - a. Weisungen betreffend Einhaltung von Zugangs- und anderen Sicherheits-

massnahmen (z.B. Passwortschutz, Sicherung des Arbeitsplatzes)

- b. Ablageort, Verbot der anderweitigen Speicherung (insbesondere auf Peripheriegeräten), sofern diese nicht erlaubt sind, Weiterleitung jeglicher Geschäftsdaten per E-Mail zu eigenen Zwecken
- c. Verfahren bei Austritt

5) Kontrollmöglichkeiten und Sanktionen

Frage: Braucht ein solches Reglement die Zustimmung der Mitarbeitenden? Wie kann es geändert werden?

Antwort: Grundsätzlich braucht es die Zustimmung der Mitarbeitenden nicht, da der Arbeitgeber berechtigt ist, Weisungen zu erlassen. Änderungen müssen daher den Mitarbeitenden lediglich zur Kenntnis gebracht werden.

Frage: Was sieht die DSGVO vor?

Antwort: Die DSGVO sieht einerseits ausgebauten Rechten zugunsten der betroffenen Person vor (Information bei der Datenerhebung und anderen Datenbearbeitungen, Auskunft- und Einsichtsrecht, Berichtigungs-/Löschungsrecht, Recht auf Einschränkung

der Bearbeitung und Datenübertragbarkeit, Widerspruchsrecht, Recht auf Verzicht auf eine automatisierte Entscheidung im Einzelfall, Recht auf Benachrichtigung über Datenschutzverletzungen). Zum anderen muss unter Umständen ein EU-Vertreter oder Datenschutzbeauftragter bestellt werden. Vorgeschrieben sind im Weiteren Datenschutzfolgenabschätzungen bei Tätigkeiten mit grösseren Risiken, Datenschutzmassnahmen im Zeitpunkt der Planung von Datenbearbeitung oder durch Voreinstellungen (privacy by design/by default) sowie Dokumentations- und Meldepflichten.

Frage: Wann muss mein Unternehmen die Vorschriften für die DSGVO beachten?

Antwort: Die DSGVO ist anwendbar, wenn im Zusammenhang mit einer Niederlassung des Unternehmens (oder eines Auftragsbearbeiters) in der EU Personendaten bearbeitet werden. Besteht keine Niederlassung in der EU, so genügt es, wenn beispielsweise über eine Website Waren oder Dienstleistungen bewusst in Ländern der EU angeboten werden oder das Surfverhalten von Personen in der EU auf einer Website aufgezeichnet wird. Die EU-DSGVO ist nicht anwendbar, wenn eine Unternehmung HR-Daten von in der Schweiz tätigen Arbeitnehmern in der Schweiz oder in einem Drittland bearbeitet. Auch bei Online-Bewerbungen sind die Voraussetzungen für die Anwendung der DSGVO regelmässig nicht erfüllt. Hingegen würde eine Verhaltensüberwachung von Arbeitnehmern in der EU unter die DSGVO fallen.



Weisungen betreffend IT-Nutzung brauchen nicht die Zustimmung der Mitarbeitenden.