PRG aktuell Garching

Informationen des Personalrats Garching der TUM

Ausgabe
Oktober 2012

Liebe Kolleginnen und Kollegen,

das Datenschutzgesetz soll den Einzelnen davor schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Beeinträchtigungen seiner Persönlichkeit können zur Verletzung seiner Privatsphäre, zu Belästigungen, zu Ruf- oder Geschäftsschädigungen und zur Verletzung existenzieller Grundlagen führen. Laut dem Art. 7 BayDSG haben alle öffentlichen Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, geeignete technische und organisatorische Maßnahmen zum Schutz dieser Daten zu treffen.

Als Personalrat einer Technischen Universität sind wir natürlich nicht daran interessiert neue Technologien und ihre Vorteile zu verhindern. Aber wir sind angehalten nach Art. 75a BayPVG im Gespräch mit der Dienststelle Beeinträchtigungen des Persönlichkeitsrechtes und unerlaubte Leistungskontrollen der Beschäftigten mit Einführung derselben zu verhindern.

In diesem Sinne wäre es für alle Beteiligten von großem Vorteil, wenn die Universitätsleitung mit den zuständigen Fachreferaten ein Verfahren bzw. Richtlinien entwickeln würde, nach dem solche Technologien verbindlich in den einzelnen Fakultäten eingeführt werden müssen. Dann würde sich das Verfahren mit dem jedes eingeführte System datenschutzrechtlich überprüft werden muss stark vereinfachen, und eine eigene Dienstvereinbarung eventuell überflüssig. Dem bayerischen Obersten Rechnungshof wird das im Übrigen bei der anstehenden Überprüfung der IT-Verfahren an der TU bestimmt auch gefallen.

Bei besonders sicherheitssensiblen Technologien, wie z.B. Cloud-Computing, sollten bestehende Partner der öffentlichen Hand (z.B. LRZ), mit denen schon Verträge bestehen, bevorzugt werden. Dies würde allen Beteiligten viel Arbeit, Zeit und auch Geld sparen.

Mit kollegialen Grüßen,

Peter Kämmerer

In dieser Ausgabe:

Outsourcing und Cloud -Computing	2
VoIP und Unified Messaging	4
U6: MVG Information	4
JAV Garching	5
Lohnsteuer-Freibeträge für 2013	5
Impressum	5

Für gute und für schlechte Zeiten -

Tipps gibt´s auf den Personalrats-Seiten.

http://www.prg.tum.de

Termine für die Grippeschutzimpfung am Campus Garching

- 19.11.2012, 8:30 - 11:45 Uhr
- 21.11.2012, 13:00 - 16:15 Uhr

In den Räumen der Betriebsärztin, Geb. H1, Bereich IPP.
Es ist eine rechtzeitige, verbindliche Terminvereinbarung unter Tel. 32991410 erforderlich.

Problemkreis: Outsourcing und Cloud-Computing

Gleichwohl es sich bei Outsourcing (Auslagern von IT-Diensten) und Cloud-Computing (Nutzen von IT-Diensten aus der Internet-„Wolke“) um zwei verschiedene Dinge handelt, treten sie oft gemeinsam auf, und die dabei auftretenden Probleme und Risiken sind vergleichbar.

Vor allem der Erfolg der Smartphones brachte auch den Durchbruch bei der privaten Anwendung von sogenannten Cloud-Diensten. Haben diese Geräte doch nur begrenzten Speicher und begrenzte Leistungsfähigkeit, sind aber durch die Datenverbindung ständig mit dem Internet verbunden. Was liegt da näher, als diese Verbindung zu nutzen, um Daten auf externen Rechnern zu lagern oder Programme und Dienste auf diesen zu nutzen? Viele nutzen diese Dienste (Google Drive, Microsoft SkyDrive, Apple iCloud, DropBox usw.) ohne sich dessen richtig bewusst zu sein, oft auch in Verbindung mit sozialen Netzwerken (Google+, Facebook etc.).

Was ist das? (mit Wikipedia-Links)

VoIP oder **Internet-Telefonie**
Das Telefonieren über Computernetzwerke, welche nach Internet-Standards aufgebaut sind. Im Unterschied zur klassischen Telefonie werden bei VoIP aber keine dedizierten „Leitungen“ durchgeschaltet, sondern die Sprache wird digitalisiert und in kleinen Daten-Paketen transportiert.

Unified Messaging
„Vereinheitlichtes Nachrichten System“. Bei Unified Messaging Systemen vereint man verschiedenste Kommunikationsdienste (Email, Fax, Video, Telefon etc.) in eine einzige Kommunikationsplattform auf die von jedem Nutzer mittels eines Programmes (oft Browser und/oder Emailprogramm) zugegriffen werden kann.

Cloud-Computing
Das Nutzen von Programmen, Rechenleistung, Speicherplatz usw. auf fremden Rechnern über das Netzwerk / Internet. Da der Nutzer i.d.R. nicht weiß, welche Rechner im Netzwerk er nutzt, erscheint ihm das ganze wie eine „Wolke“ (engl. cloud) von Rechnern in die er seine Daten gibt, bzw. aus der er seine Daten bekommt.

(**IT-)Outsourcing**
Die Abgabe von Unternehmensaufgaben und -strukturen, bzw. von bisher intern erbrachter Leistung, an Drittunternehmen.

Bei einer dienstlichen Nutzung, oder einer Nutzung durch eine Behörde müssen aber andere Rahmenbedingungen gelten als bei privater. Es kommt zu Problemen und Risiken, wenn

- die Nutzung und Kontrolle externer Dienstleistungen nicht vertraglich geregelt ist,
- dadurch neue, dem Informationssicherheitsmanagement unbekannte und damit unkontrollierte Datenflüsse entstehen,
- vertrauliche Daten unautorisiert an Dritte gegeben werden und damit interne Sicherheitsvorgaben oder Datenschutzbestimmungen verletzt werden,
- technische Sicherheitsmaßnahmen wie Virenschutz und Firewall unterlaufen werden.

Ein besonders heikler Punkt ist hierbei die datenschutzrechtliche Verantwortlichkeit, die natürlich NICHT mit Outsourcing auf den externen Dienstleister abgeschoben werden kann:

… „Das europäische und deutsche Datenschutzrecht knüpft die rechtliche Verantwortlichkeit für die Datenverarbeitung personenbezogener Daten an die inhaltliche Verantwortlichkeit über die Entscheidung des Umgangs mit den Daten. Danach ist verantwortliche Stelle jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt und allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, § 3 Abs. 7 BDSG, Art. 2 Buchst. d) 4 Richtlinie 95/46/EG. Der Cloud-Anwender ist verantwortliche Stelle in diesem Sinne. Ein Cloud-Anbieter kann jedoch dann ausnahmsweise verantwortliche Stelle sein, wenn er selbst Dienstleistungen anbietet.

Nimmt der Cloud-Anwender von einem Cloud-Anbieter IT-Dienstleistungen für Cloud-Services in Anspruch, so wird Letzterer als Auftragnehmer nach § 11 Abs. 2 BDSG tätig. Der Cloud-Anwender bleibt hingegen nach § 11 Abs. 1 BDSG für die Einhaltung sämtlicher datenschutzrechtlicher Bestimmungen

verantwortlich. Weiterhin muss der Cloud-Anwender einen schriftlichen Auftrag an den Cloud-Anbieter erteilen und dabei die inhaltlichen Anforderungen nach § 11 Abs. 2 BDSG erfüllen." … (aus Orientierungshilfe Cloud Computing (Version 1.0/Stand 26.09.2011) der Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder)

aus dem Bundes Datenschutzgesetz (BDSG):

…

§ 11 Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

(1) …

(2) Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei insbesondere im Einzelnen festzulegen sind:

1. der Gegenstand und die Dauer des Auftrags,
2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
3. die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen,
4. die Berichtigung, Löschung und Sperrung von Daten,
5. die nach Absatz 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,
6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
7. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Er kann bei öffentlichen Stellen auch durch die Fachaufsichtsbehörde erteilt werden. Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren.

(3) …

Bei der Entscheidung für das Auslagern von IT-Diensten sollte eine objektive Wirtschaftlichkeitsrechnung durchgeführt werden, die auch Datenschutz und Datensicherheit berücksichtigt. Eine umfassende Wirtschaftlichkeitsrechnung berücksichtigt nicht nur die Kosten, die der Dienstleister in Rechnung stellt, sondern alle relevanten Kosten, wie z.B. auch mögliche Kosten für eine zum externen Dienstleister verbindungshaltenden (retained) Organisation oder für die Beendigung eines Projekts bzw. der Zusammenarbeit mit dem Dienstleister. Des Weiteren :

- Die Qualität und die Sicherheit der ausgelagerten Prozesse, die nur indirekt beeinflusst werden kann. Oft sind solche Dienstleistungen auch mit Cloud-Diensten und/oder Funktionen von sozialen Netzwerken gekoppelt (z.B. Microsoft SharePoint u.a.; wann werden vorgehaltene Daten gelöscht?).
- Abhängigkeit von Drittunternehmen (Was, wenn die Firma insolvent oder aufgekauft wird? Gibt es alternative Anbieter am Markt? Werden Daten vom Dienstleister weitergegeben?).
- Oft ist der Schutz des Knowhows bei der Vergabe von Leistungen an Dritte nicht sichergestellt. Auch informelle Kontakte z. B. zwischen Lehrstühlen und Arbeitsgruppen, aus denen neue Ideen für Verbesserungen entstehen, werden beim Outsourcing einzelner Prozesse oft unterbunden, wenn hierfür kein einheitliches, universitätsweites retained Management organisiert ist.

Zurzeit erscheint noch Vieles im Bereich von Datensicherheit und Datenschutz an der TU zufällig und heterogen. Es gibt zwar schon mit dem ITSZ (IT-Servicezentrum) und dem ITZ-Steuerkreis eine Stelle, welche die IT-Dienste universitätsweit organisiert und plant, doch scheint das Thema Datensicherheit und Datenschutz, mangels Kapazitäten, nur eine untergeordnete Rolle zu spielen. Wünschenswert wäre vielleicht ein Referat im ITSZ, das mit dem Datenschutzbeauftragten zusammenarbeitet und alle IT-Projekte der TU und ihrer Untereinheiten mit Beratung und Planung begleitet.

Problemkreis: VoIP und Unified Messaging-Systeme

Viele Telekommunikationsanwendungen arbeiten mit personenbezogenen Daten und reichen diese unter Umständen an andere Anwendungen des Systems und / oder einen Provider weiter. Besonders hervorzuheben sind Unified Messaging-Systeme (z.B. Microsoft Lync Server u.a.), bei denen die Auswirkungen eines Vertraulichkeitsverlustes aufgrund der zentralen Sammlung unterschiedlicher Nachrichtentypen gravierend sein können. Personenbezogene Daten sind beispielsweise Gebührendaten, Konfigurationsdaten, Berechtigungen und elektronische Telefonbücher, Passwörter und Verrechnungsnummern. Für die Rechnungserstellung zeichnen TK-Anlagen, und auch VoIP-Systeme, oft Verbindungsdatensätze auf, die mindestens Informationen über die angerufene Teilnehmernummer, den Anrufzeitpunkt und die Dauer des Gesprächs enthalten. Hieraus lassen sich Kommunikationsprofile für einzelne Endgeräte oder Nutzer ableiten, welche natürlich nicht zur Arbeits- und Verhaltenskontrolle genutzt werden dürfen.
Es beabsichtigen alleine an der TU in Garching mittlerweile mindestens 3 Dienststellen schon solche VoIP- bzw. Unified Messaging-Systeme einzurichten (zwei davon in Betrieb!?), ohne dass ein Gesamtkonzept und Sicherheitsmanagement an der TU bzw. dem Standort für diese Fälle schon vorhanden ist. Problematisch ist, dass damit kein homogenes, hohes Sicherheitsniveau mehr gewährleistet ist. Fehlende, standortübergreifende strategische und konzeptionelle Vorgaben im Sicherheitsmanagement führen hier zu Wildwuchs, welche die allgemeine Datensicherheit beeinträchtigen. Zudem erfordert das Fehlen einer TU-weiten Regelung die „Einzelabnahme“ jedes Systems, eine datenschutzrechtliche Prüfung und Freigabe und eine eigene Dienstvereinbarung über die Nutzung mit dem Personalrat.
Wünschenswert wäre daher, dass die Dienststelle hier verbindliche Vorgaben erarbeitet, die möglichst für alle installierten bzw. noch zu installierenden Systeme einen Rahmen setzt, so dass unbürokratisch und zügig eine datenschutzrechtliche Freigabe und Dienstvereinbarung erfolgen kann.

U6: MVG Information vom 6.7.2012

„… Wegen Gleis- und Brückenbauarbeiten fahren im Sommer 2013 und 2014 Busse anstelle von Zügen zwischen Studentenstadt und Kieferngarten. 2013 wird die Baumaßnahme vsl. am 20. Mai (Pfingstferien) beginnen und bis in den August dauern; ein ähnlicher Zeitraum ist für 2014 vorgesehen. Die U6 wird in dieser Zeit durch Gelenkbusse ersetzt, die in kurzen Abständen zwischen Studentenstadt und Kieferngarten sowie zusätzlich vom U-Bahnhof Nordfriedhof über die A9 nach Fröttmaning fahren. Kapazitätsengpässe sind dabei unvermeidlich, weil noch so viele Gelenkbusse (ca. 100 Plätze) keine U-Bahn (ca. 900 Plätze) ersetzen können. Die MVG hat deswegen auch schon Kontakt mit den Fußball-Verantwortlichen aufgenommen, denn bis zum Bahnhof Studentenstadt kann die U-Bahn nicht – wie sonst bei Fußballverkehr üblich – verdichtet werden und auch die Ersatzbusse könnten den üblichen Fußballverkehr mit bis zu 30.000 Fahrgästen nicht bewältigen. Die notwendige Dauer der Bauarbeiten lässt leider keine Abwicklung ausschließlich in den Schulferien und der fußballfreien Zeit zu.
Die Baustelle auf der U6 Nord umfasst die Erneuerung der Gleise zwischen Studentenstadt und Kieferngarten sowie Sanierungsarbeiten und vertiefende Bauwerksprüfungen an der U-Bahnbrücke über der Heidemannstraße, für die die Gleise ohnehin entfernt werden müssten. Dabei wird in jedem Jahr jeweils eine Brückenhälfte bearbeitet und das jeweils zugehörige Gleis erneuert. Das andere Gleis dient jeweils für die Bereitstellung der Baulogistik (Bauzüge und -maschinen) und die unverzichtbare Anbindung des Betriebshofs in Fröttmaning. Ein Fahrgastbetrieb über den jeweils verbleibenden Schienenstrang ist aus Sicherheits- und Kapazitätsgründen jedoch ausgeschlossen. Zudem werden im U-Bahnhof Kieferngarten die Bahnsteige erneuert und um ca. 5 Zentimeter angehoben, um die Barrierefreiheit zu verbessern. …“

Die letzte Seite ...

News von der JAV Garching

Ergebnis der konstituierenden Sitzung:

Vorsitzende:

Sabine Fölsner, Chemielaborantin, CH, Tel: 13020, sabine.foelsner@tum.de

Stellvertreter:

Erik Faber, Feinwerkmechaniker, PH, Tel: 12496, erik.faber@tum.de

Weitere Mitglieder:

Lino Krause, Feinwerkmechaniker, MW, Tel: 16205, linokrause@inbox.com
Jesko Petersen, Feinwerkmechaniker, MW, Tel: 15954, jeskoo@gmx.de
Sebastian Grüll, Systemelektroniker, MW, Tel: 15870, gruell@ftm.mw.tum.de

Ersatz:

Caner Yanbaz: Feinwerkmechaniker, MW, Tel: 15324, c.yanbaz@gmail.com
Tobias Krist: Feinwerkmechaniker, MW
Martin Schellerer Chemielaborant, CH

Lohnsteuer-Freibeträge für 2013 neu beantragen!

Wer will, dass 2013 Freibeträge schon beim Lohnsteuerabzug berücksichtigt werden, beispielsweise Freibeträge bei Berufspendlern oder für volljährige Kinder, kann ab Oktober 2012 beim zuständigen Wohnsitzfinanzamt einen entsprechenden Antrag stellen. Denn für 2012 beantragte Freibeträge verlieren 2013 ihre Gültigkeit. Sie müssen daher für 2013 neu beantragt werden.

Die Pressemitteilung des BayLfSt

Die Antragsformulare

§ Wichtiger Hinweis: Wir geben unsere Auskünfte nach bestem Wissen und Gewissen, aber ohne Gewähr. Rechtsauskünfte dürfen wir nicht erteilen. Bitte fragen Sie für rechtssichere Auskünfte bei den zuständigen Stellen nach (Dienststelle, Landesamt für Finanzen u.s.w.) Rechtsverbindliche Auskünfte können Ihnen auch zugelassene Anwälte und die Rechtsberatungen der Gewerkschaften erteilen.

Herausgeber:
Personalrat Garching
Technische Universität München
Boltzmannstr. 15
85748 Garching

Telefon: 089-289-16382/5
Fax: 089-289-16390
E-Mail: personalrat@mw.tum.de
http://www.mw.tum.de/Personalrat
Red.: Kämmerer, Hoyer, Tögel, Wittner