MITTEILUNGSBLATT

DER

Medizinischen Universität Innsbruck

Internet: http://www.i-med.ac.at/mitteilungsblatt/

Studienjahr 2008/2009 | Ausgegeben am 25. November 2008 | 12. Stück

Das Mitteilungsblatt erscheint jeweils am 1. und 3. Mittwoch jeden Monats.
Eigentümer, Herausgeber, Vervielfältigung, Vertrieb und für den Inhalt verantwortlich:
O. Univ.-Prof. Dr. Manfred P. Dierich, Rektor-Stellvertreter der Medizinische Universität Innsbruck, Innrain 52, A-6020 Innsbruck.

44. Rahmenbetriebsvereinbarung über die Verwendung personenbezogener Daten

Rahmenbetriebsvereinbarung

über die Verwendung personenbezogener Daten

abgeschlossen zwischen

1. der Medizinischen Universität Innsbruck als Arbeitgeber, vertreten durch das Rektorat,

2. und als Vertretung der Arbeitnehmerinnen und Arbeitnehmer
   a. dem Betriebsrat für das allgemeine Universitätspersonal der Medizinischen Universität Innsbruck (§ 135 Abs. 5 UG 2002) und
   b. dem Betriebsrat für das wissenschaftliche Personal an der Medizinischen Universität (§ 135 Abs. 4 UG 2002)

als Grundsatzvereinbarung über die Regelung der Verwendung von personenbezogenen Daten aller Beschäftigten in Datenverarbeitungssystemen, die sich an der Medizinischen Universität Innsbruck im Einsatz befinden oder geplant sind.

§ 1 Terminologie

Zur einheitlichen Formulierung und Übersichtlichkeit wird die in Anhang 1 angeführte Terminologie in Anlehnung an das DSG 2000 festgeschrieben.

§ 2 Geltungsbereich

(1) Diese Betriebsvereinbarung gilt:
   a. Personell für alle von den abschließenden Betriebsräten vertretenen Arbeitnehmerinnen und Arbeitnehmer der Medizinischen Universität Innsbruck und Mitarbeiterinnen und Mitarbeiter des Amtes der Medizinischen Universität Innsbruck, im Folgenden als Mitarbeiterinnen und Mitarbeiter zusammengefasst.
   b. Sachlich für personenbezogene Daten der Mitarbeiterinnen und Mitarbeiter bei der Planung, Einführung, Verwendung und Veränderung bestehender und zukünftiger Datenverarbeitungssysteme.

(2) Die Grundsätze dieser Betriebsvereinbarung gelten sinngemäß für alle (auch zukünftige) Detail-(Zusatz)-Betriebsvereinbarungen, die den konkreten Einsatz von Datenverarbeitungssystemen beschreiben (Betriebsvereinbarungen im Sinne der §§ 96, 96a und 97 ArbVG).

§ 3 Rechtsgrundlagen

Die rechtliche Basis bilden insbesondere die Bestimmungen
1. des Universitätsgesetzes 2002,
2. des Arbeitsverfassungsgesetzes (ArbVG; im Besonderen die §§ 91, 92, 96, 96a und 97),
3. des ArbeitnehmerInnenschutzgesetzes (ASchG),
4. des Datenschutzgesetzes 2000 (DSG 2000),
5. des Gesundheitstelematikgesetzes (GTelG), und
6. des Telekommunikationsgesetzes (TKG).

§ 4 Zielsetzung

(1) Diese Betriebsvereinbarung dient zur Qualitätssicherung und Transparenz der Verwendung personenbezogener Daten beim Einsatz von Datenverarbeitungssystemen.

(2) Es besteht Übereinstimmung darüber, dass der Einsatz von Datenverarbeitungssystemen dazu dient, die sich aus Gesetzen, Kollektivverträgen, Betriebsvereinbarungen oder Arbeitsverträgen ergebenden Aufgaben der Medizinischen Universität Innsbruck zu unterstützen und zu erleichtern.

(3) Es besteht darüber hinaus Konsens, dass bei Verwendung von personenbezogenen Daten bzw. bei vernetzten Datenverarbeitungssystemen allen Mitarbeiterinnen und Mitarbeitern entsprechender Schutz geboten wird vor
1. einer systematischen, die Menschenwürde des Einzelnen berührenden Kontrolle,
2. unrichtigen und subjektiven Interpretationen,
3. Leistungs- und Verhaltenskontrollen aus eventuellen Auswertungen jeglicher Art, wobei Evaluierungen gem. § 14 Universitätsgesetz 2002 ausdrücklich ausgenommen sind,
4. unberechtigter Speicherung von personenbezogenen Daten auf jeder Art von Medien (insbesondere auf beweglichen Medien),
5. unberechtigter Übermittlung personenbezogener Daten in andere, sich außerhalb der Medizinischen Universität Innsbruck befindende Systeme, und
6. falschen Daten.

(4) Aufzeichnungen und Auswertungen der System- oder systemnahen Software über Benutzerinnen- bzw. Benutzeraktivitäten dürfen nur zu folgenden Zwecken verwendet werden:
1. Einhaltung der Bestimmungen des § 14 DSG 2000 zur Datensicherheit,
2. Gewährleistung der Systemsicherheit,
3. Analyse und Korrektur von technischen Fehlern in Datenverarbeitungssystemen,
4. Optimierung von Datenverarbeitungssystemen,
5. Leistungsverrechnung für den Betrieb der Datenverarbeitungsinfrastruktur.

(5) Zur Konkretisierung einzelner Regelungen dieser Vereinbarung werden personenbezogene Daten in vier Kategorien unterteilt. Da idente Datenfelder in verschiedenen Systemen unterschiedliche Bedeutung besitzen können, hat diese Unterteilung für jedes Datenverarbeitungssystem, für das eine Zusatzvereinbarung abgeschlossen wird, zu erfolgen. Die Entscheidung, welches Datenfeld in welche Kategorie fällt, ist Gegenstand der innerbetrieblichen Datenschutzkommission (vgl. § 5):
1. **Kategorie A**: Mitarbeiterinnen- bzw. mitarbeiterbezogene Daten zur geschäftlichen Kommunikation. Diese Daten umfassen die geschäftlichen Kommunikationsdaten (z.B.: Name, Organisationseinheit, Anschrift in der Organisationseinheit, Büroraum, Telefonnummer, E-Mail-Adresse). Diese Daten können als Einzeldatensätze frei, z.B. via Internet, kommuniziert werden. Eine Massenübermittlung dieser Daten bedarf jedenfalls der Zustimmung der innerbetrieblichen Datenschutzkommission.
2. **Kategorie B**: Persönliche Geschäftsdaten. Diese Daten müssen von der Medizinischen Universität Innsbruck bzw. dem Amt der Medizinischen Universität Innsbruck verarbeitet werden. In vielen Fällen werden die Daten benötigt, um gesetzlichen Forderungen bzw. vertraglichen Verpflichtungen nachkommen zu können. Diese Daten dürfen intern und extern nur im Rahmen der gesetzlichen Forderungen bzw. vertraglichen Verpflichtungen und zur Erfüllung der Aufgaben der Medizinischen Universität Innsbruck verwendet werden. Ob und in welchem Ausmaß diese Daten intern und extern kommuniziert werden dürfen, ist durch die innerbetriebliche Datenschutzkommission detailliert festzulegen (z.B.: Dienstzeitregelung, Urlaubsanspruch, Qualifikationen).
3. **Kategorie C**: Private Geschäftsdaten. Diese Daten gehören zwar zum Teil zu den Stammdaten (werden daher z.B. zur Entgeltberechnung benötigt), sind aber dem Privatbereich der Mitarbeiterin bzw. des Mitarbeiters zuzuordnen und stehen nicht direkt mit der Universität in Verbindung (z.B: Familienstand, Bankverbindung). Hierunter fallen auch Daten, die aus Sicht der betroffenen Mitarbeiterin bzw. des betroffenen Mitarbeiters einem erweiterten Schutzinteresse unterliegen (z.B.: Pfändungen, betriebliche Darlehen).
4. **Kategorie D**: Sensible Daten, insb. im Sinn des § 4 Z 2 DSG 2000. Darunter fallen Daten der Mitarbeiterin bzw. des Mitarbeiters über ihre bzw. seine rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder Sexualleben.

§ 5 Innerbetriebliche Datenschutzkommission

(1) Zur Beratung aller Fragen, die sich im Zusammenhang mit der Einführung, dem Betrieb und den Änderungen von Datenverarbeitungssystemen ergeben, bildet die Medizinische Universität Innsbruck eine innerbetriebliche Datenschutzkommission.

(2) Die Entscheidungskompetenzen des Rektorats als Organ der Medizinischen Universität Innsbruck und die der Betriebsräte als Körperschaften gemäß ArbVG bleiben davon unberührt.

(3) Die Beratungen und Ergebnisse der innerbetrieblichen Datenschutzkommission dienen für das Rektorat und die Betriebsräte als Entscheidungsgrundlagen.

(4) Aufgaben der innerbetrieblichen Datenschutzkommission:
1. Grundsätzliche Aufgabe der innerbetrieblichen Datenschutzkommission ist es, einen Interessenausgleich zwischen Rektorat und den Betriebsräten herbeizuführen. Auch Nichteinigung in Fragen, die im Zusammenhang mit dieser Rahmenbetriebsvereinbarung stehen, ist vorerst in der innerbetrieblichen Datenschutzkommission zu behandeln.
2. Die innerbetriebliche Datenschutzkommission hat die zu dieser Rahmenbetriebsvereinbarung notwendigen Detail-(Zusatz-)Betriebsvereinbarungen vorzubereiten. Dies gilt ebenso für die Revisionen dieser und von Detail-(Zusatz-)Betriebsvereinbarungen.
3. Die innerbetriebliche Datenschutzkommission hat bei allen eingesetzten Datenverarbeitungssystemen zu klären, bei welchen der verarbeiteten Daten ein Personenbezug vorliegt.
4. Im Besonderen hat die innerbetriebliche Datenschutzkommission sensible Daten (= personenbezogene Daten der Kategorien C und D in Anlehnung an § 4 Abs. 5 dieser Rahmenbetriebsvereinbarung) zu definieren.
5. Die innerbetriebliche Datenschutzkommission hat über geplante Systeme, die Verwendung von personenbezogenen Daten möglich machen, zu beraten. Dazu ist die innerbetriebliche Datenschutzkommission bereits in der Planungsphase, d.h. vor Einführung bzw. Veränderung des Systems gemäß Anlage 2 detailliert zu informieren.
6. Die innerbetriebliche Datenschutzkommission hat im Einvernehmen mit dem Rektorat und den Betriebsräten ein Datenschutzkonzept zu entwickeln und jährlich einen Datenschutzreport zu erstellen, in dem der aktuelle Stand und die wesentlichen Problembereiche betreffend Datensicherheit und Datenschutz dargestellt sind. Dieser Datenschutzreport dient dem Rektorat und den Betriebsräten im Hinblick auf interne und externe Qualitätssicherung, Mitarbeiter/innen/zufriedenheit, sowie Informations- und Kommunikationsqualität zur Diskussion, Zukunftsorientierung und Weiterentwicklung.
7. In mehrjährigen Abständen soll überprüft werden, ob die Datenschutzkonzepte für bereits bestehende Datenverarbeitungssysteme ausreichen. Die innerbetriebliche Datenschutzkommission hat Empfehlungen hierfür zu erstellen.

(5) Das Rektorat und die Betriebsräte verpflichten sich, im Konfliktfall erst dann den Rechtsweg zu beschreiten, wenn nach Beratung in der innerbetrieblichen Datenschutzkommission keine Einigung zustande gekommen ist bzw. ein innerbetrieblicher Schlichtungsversuch erfolglos blieb. Dies wird dann als gegeben angenommen, wenn im Zuge der Beschlussfassung keine Einigung vorliegt oder ein Beschluss innerhalb sechs Wochen ab der ersten Befassung in der innerbetrieblichen Datenschutzkommission nicht zustande gekommen ist.

(6) Der innerbetrieblichen Datenschutzkommission gehören an:
1. Zwei Vertreterinnen bzw. Vertreter des Rektorates, davon eine Juristin bzw. ein Jurist. Im Falle, dass eine Datenschutzbeauftragte bzw. ein Datenschutzbeauftragter an der Medizinischen Universität Innsbruck bestellt ist, ist diese Person grundsätzlich Mitglied der Datenschutzkommission und in die Zahl der Vertreterinnen bzw. Vertreter des Rektorates einzurechnen.
2. Je eine Vertreterin bzw. ein Vertreter der beiden Betriebsräte.
3. Für jedes Mitglied der Datenschutzkommission ist eine Stellvertreterin bzw. ein Stellvertreter zu benennen.

(7) Rektorat und Betriebsräte haben jeweils das Recht, bei Bedarf Auskunftspersonen ihrer Wahl zur Beratung beizuziehen.

(8) Zur Bewältigung der organisatorischen Abläufe hat die innerbetriebliche Datenschutzkommission (nach ihrer Konstituierung) eine Geschäftsordnung mit folgendem Mindestinhalt festzulegen, die in ihrer jeweils gültigen Fassung dieser Betriebsvereinbarung angehängt wird, ohne integrierter Bestandteil zu sein.
1. Vorsitzführung
2. Protokollführung
3. Art der Beschlussfassung
4. Art der Einberufung
5. Tagungsintervall

(9) Die innerbetriebliche Datenschutzkommission ist beschlussfähig, wenn alle Mitglieder anwesend sind. Gültige Beschlüsse können nur einstimmig gefasst werden und sind zu protokollieren. Das Votum eines betriebsrätlichen Mitglieds nach Abs 6 Z 2 kann durch einen Beschluss dieses Betriebsrates ersetzt werden.

(10) Die innerbetriebliche Datenschutzkommission kann hinsichtlich der an sie gestellten Fragestellungen
1. eine grundsätzliche oder einzelfallbezogene Zustimmung geben,
2. ihre Zustimmung an bestimmte Auflagen knüpfen (z.B. zusätzliches Passwort),
3. die Verarbeitung ablehnen.

(11) Zustimmungen und Ablehnungen der innerbetrieblichen Datenschutzkommission bedürfen der Schriftform.

(12) Die innerbetriebliche Datenschutzkommission tagt zumindest vierteljährlich. Zwischenzeitliche Einberufungen durch die Vorsitzende bzw. den Vorsitzenden sind möglich.

(13) Die bzw. der Vorsitzende hat auch auf Verlangen eines Kommissionsmitgliedes, unter Angabe des Grundes, binnen fünf Arbeitstagen eine Sitzung einzuberufen. Jede Einberufung hat eine schriftliche Tagesordnung zu enthalten und ist spätestens zwei Arbeitstage vor der Sitzung allen Kommissionsmitgliedern zu übermitteln.

(14) Die Konstituierung hat innerhalb von drei Monaten nach Abschluss dieser Betriebsvereinbarung durch Wahl einer bzw. eines Vorsitzenden zu erfolgen.

§ 6 Grundregeln zur Verwendung personenbezogener Daten

(1) Vor der Verwendung von personenbezogenen Daten ist zu prüfen, ob die angestrebten Ergebnisse auch ohne personenbezogene Daten effizient und mit vertretbarem Aufwand zu erzielen sind. Ist dies nicht der Fall, so ist die innerbetriebliche Datenschutzkommission zu befassen.

(2) Verarbeitungen von personenbezogenen Daten, die im Rahmen des gesetzlich festgeschriebenen Rahmens und im Rahmen geltender Detail-(Zusatz-)Betriebsvereinbarungen erfolgen, werden ohne vorheriges Einverständnis der innerbetrieblichen Datenschutzkommission durchgeführt. Jeder Betriebsrat bzw. die Betriebsräte gemeinsam können jedoch deren Rechtmäßigkeit durch Einholung einer Information (z.B. Gutachten) bei ihrer jeweiligen gesetzlichen Interessenvertretung überprüfen lassen. In allen anderen Fällen (keine Notwendigkeit, negatives Gutachten der Interessenvertretung, …) ist die innerbetriebliche Datenschutzkommission damit zu befassen.

(3) Wurde durch die innerbetriebliche Datenschutzkommission die Zustimmung zu einer Verarbeitung gegeben, so gilt diese ausschließlich für den angegebenen Verarbeitungszweck, jede andere Verwendung der Daten ist unzulässig.

(4) Für alle im Rahmen dieser Betriebsvereinbarung verwendeten personenbezogenen Daten ist in der jeweiligen Detail-(Zusatz-)Betriebsvereinbarung eine Frist zu vereinbaren, in der diese Daten aufbewahrt werden können bzw. gelöscht werden müssen.

(5) Bei einzelfallbezogener Zustimmung ist die Verarbeitung innerhalb einer zu vereinbarenden Frist zu beenden. Die personenbezogenen Daten sind unmittelbar nach Ablauf dieser Frist zu löschen. Besteht die begründete Vermutung, dass die Daten für die zulässige Verarbeitung (z.B. zur Fehlerkorrektur) noch benötigt werden, kann eine längere Speicherfrist vereinbart werden. Werden diese Fristen überschritten, ist neuerlich die innerbetriebliche Datenschutzkommission zu befassen.

(6) Bei der Übermittlung von personenbezogenen Daten zwischen verschiedenen betriebsinternen Datenverarbeitungssystemen gilt im Hinblick auf Daten der Kategorie A und B eine besondere Obsorgepflicht. Für Daten der Kategorie C und D ist die innerbetriebliche Datenschutzkommission zu befassen.

(7) Für die Übermittlung von personenbezogenen Daten in andere, sich außerhalb der Medizinischen Universität Innsbruck befindliche Datenverarbeitungssysteme ist grundsätzlich die innerbetriebliche Datenschutzkommission zu befassen.

(8) Vor der Speicherung von personenbezogenen Daten auf bewegliche Speichermedien (USB-Stick, Datenbänder, CD-ROM, DVD, etc.) ist die innerbetriebliche Datenschutzkommission zu befassen.

(9) Bei Bildschirmarbeitsplätzen kann vom Grundsatz ausgegangen werden, dass sämtliche personenbezogenen Daten (unabhängig vom Format) sowie sämtliche Transaktionen von dritter Seite (andere Beschäftigte, Vorgesetzte, organisationsfremde Personen) ohne Zustimmung der innerbetrieblichen Datenschutzkommission weder eingesehen noch aus-gewertet werden dürfen. Ausnahmen davon – wie zum Beispiel im Rahmen der Systemadministration bzw. bei personeller Vertretung im Falle einer Abwesenheit – müssen in den jeweiligen Detail-(Zusatz-)Vereinbarungen festgehalten werden.

(10) Es wird vereinbart, dass für bestehende Datenverarbeitungssysteme gemäß § 2 Abs 1 lit b innerhalb von zwölf Monaten nach Abschluss dieser Betriebsvereinbarung der innerbetrieblichen Datenschutzkommission und den Betriebsräten die Informationen gemäß Anhang 2 zur Verfügung zu stellen sind, damit für das jeweilige Datenverarbeitungssystem eine Detail-(Zusatz-)Betriebsvereinbarung abgeschlossen werden kann; Kommt es innerhalb von zwei Jahren nicht zum Abschluss einer entsprechenden Detail-(Zusatz-)Betriebsvereinbarung, so darf dieses Datenverarbeitungssystem nicht mehr weiter betrieben werden. Diese Verpflichtung kann jedoch durch einen Beschluss der innerbetrieblichen Datenschutzkommission aufgehoben werden, wenn das entsprechende Datenverarbeitungsystem in absehbarer Zeit ausgetauscht wird, oder nur kumulierte bzw. indirekt personenbezogene Daten verwendet werden.

(11) Es wird vereinbart, dass für künftige Datenverarbeitungssysteme gemäß § 2 Abs 1 lit b vor der Produktivstellung (Echtbetrieb, Abschluss der Implementierung, Ende des Roll-outs) eine entsprechende Detail-(Zusatz-)Betriebsvereinbarung abgeschlossen wird.

(12) Auf die Bestimmungen der §§ 17 und 18 des DSG 2000 wird ausdrücklich verwiesen.

§ 7 Simulationsdaten (Testdaten)

Bei der Entwicklung und Wartung von Auswertungsprogrammen muss mit speziellen Simulationsdaten (Testdaten) gearbeitet werden. Falls eine Anonymisierung nicht möglich ist, werden diese Daten wie Echtdaten behandelt.

§ 8 Fernwartung

Bei der Installierung von Fernwartungskonzepten (etwa im Rahmen von Wartungsverträgen) und dem Betrieb von Fernwartungseinrichtungen (Modemanschlüssen, Internetverbindungen, etc.) ist dafür Sorge zu tragen, dass personenbezogene Daten nicht missbräuchlich verwendet werden können. Der innerbetrieblichen Datenschutzkommission und, wenn bestellt, der bzw. dem Datenschutzbeauftragten ist über den Stand der Fernwartungseinrichtungen auf Verlangen, mindestens aber einmal jährlich, Bericht zu erstatten.

§ 9 Rechte und Pflichten der Betriebsräte

(1) Jeder Betriebsrat für sich hat bzw. die Betriebsräte gemeinsam haben das Recht, jederzeit die Einhaltung der Betriebsvereinbarung zu kontrollieren und Auskünfte über die einzelnen Systeme zur Verarbeitung personenbezogener Daten zu erhalten.

(2) Jeder Betriebsrat für sich hat bzw. die Betriebsräte gemeinsam haben das Recht in sämtliche Protokolle und Auswertungen, unter Einhaltung der jeweils geltenden gesetzlichen Bestimmungen, Einsicht zu nehmen bzw. solche anzufordern.

(3) Den Betriebsräten ist die Kontrolle der Verwendungen von Datenverarbeitungssystemen zu ermöglichen. Die jeweiligen Detail-(Zusatz-)Betriebsvereinbarungen regeln die genaue Art und den Einsatz bestimmter Werkzeuge, um diese Kontrolle ausüben zu können.

(4) Um die notwendigen Qualifikationen zur Wahrnehmung ihrer Kontrollrechte zu erlangen, werden den Betriebsräten von der Medizinischen Universität Innsbruck geeignete Informationsmittel zur Verfügung gestellt.

(5) Wenn erforderlich, ist es den Betriebsräten gestattet, externe Experten ihres Vertrauens hinzuzuziehen, wobei diese zur Geheimhaltung und zur Einhaltung datenschutzrechtlicher Bestimmungen zu verpflichten sind.

(6) Jeder Betriebsrat für sich hat bzw. die Betriebsräte gemeinsam haben weiters das Recht, während der Arbeitszeit unter Fortzahlung des Entgeltes an Anwenderschulungen bezüglich der einzelnen Systeme zur Verarbeitung personenbezogener Daten teilzunehmen. Diese Bildungsveranstaltungen sind nicht auf die Bildungsfreistellung anzurechnen.

§ 10 Information der Betriebsräte

(1) Die Medizinische Universität Innsbruck verpflichtet sich, den Betriebsräten folgende Informationen zur Verfügung zu stellen, die laufend aktualisiert werden:
1. Übersicht über alle Systeme, die automationsunterstützt personenbezogene Daten verwenden, inklusive einer allgemein verständlichen Kurzbeschreibung,
2. Übermittlung personenbezogener Daten von oder zur Medizinischen Universität Innsbruck,
3. Einladungen zu Veranstaltungen/Sitzungen, in denen über die Speicherung, Übertragung und Verwendung von personenbezogenen Daten in Datenverarbeitungssystemen gemäß § 2 Abs 1 lit b beraten und entschieden wird.
4. Protokolle aller Sitzungen und Unterlagen zur allen Veranstaltungen, die in Zusammen-hang mit der Einführung oder Änderung von Datenverarbeitungssystemen zur personenbezogenen Datenverwendung stehen.

(2) Bei allen eingesetzten Systemen sind den Betriebsräten unaufgefordert folgende Informationen zur Verfügung zu stellen:
1. die jeweiligen Systembeschreibungen,
2. die Verwendungszwecke, zumindest im Hinblick auf die Datenkategorien C und D,
3. alle Systembenutzer und deren Zugriffsberechtigungen (zumindest im Hinblick auf die Datenkategorien C und D),
4. der Standort und Vernetzung der verwendeten Hardware, und
5. ein taxatives Verzeichnis personenbezogener Auswertungen mit Beispielen (zumindest im Hinblick auf die Datenkategorien C und D).

(3) Diese Informationen sollen sich an der in Anhang 2 definierten Checkliste orientieren und auch die Ziele der Personaldatenverwendung, die zeitliche Einführungsplanung, die jeweiligen Zuständigkeiten (Kompetenzen) für die Einführung und den Betrieb des Systems sowie die Auswirkungen (Veränderungen) auf die Mitarbeiterinnen und Mitarbeiter enthalten.

§ 11 Rechte und Pflichten der Mitarbeiterinnen und Mitarbeiter

(1) Alle Mitarbeiterinnen und Mitarbeiter sind unter Fortzahlung des Entgeltes während der Arbeitszeit über ihre Rechte und Pflichten in Bezug auf diese Rahmenbetriebsvereinbarung und etwaige Detail-(Zusatz-)Vereinbarungen zu den jeweiligen Datenverarbeitungssystemen gemäß § 2 Abs 1 lit b zu informieren.

(2) Personelle Konsequenzen, die auf Informationen beruhen, die unter Verletzung dieser Rahmenbetriebsvereinbarung gewonnen werden, sind rechtsunwirksam.

(3) Werden von Mitarbeiterinnen und Mitarbeitern personenbezogene Daten verwendet, haben die Dienstvorgesetzten dafür Sorge zu tragen, dass die Mitarbeiterinnen und Mitarbeiter vorher durch Unterschrift dokumentieren, dass sie über ihre Rechte und Pflichten im Sinne dieser Vereinbarung informiert wurden.

(4) Darüber hinaus haben die Dienstvorgesetzten dafür Sorge zu tragen, dass die für die einzelnen Datenverarbeitungssysteme gemäß den jeweiligen Detail-(Zusatz-)Betriebsvereinbarungen zugriffsberechtigten Personen durch ihre Unterschrift bestätigen, über die Sensibilität der Daten (resultierend aus der Kategorisierung), über die vereinbarten Regelungen zwischen Rektorat und Betriebsräten (Betriebsvereinbarungen) und die daraus resultierenden Datenschutzbestimmungen informiert worden zu sein.

(5) Im Falle des Verdachts eines Verstoßes gegen die Regelungen dieser Rahmenbetriebsvereinbarung sowie der davon abhängigen Detail-(Zusatz-)Betriebsvereinbarungen ist dieser Verdacht dem Rektorat, den Betriebsräten sowie, wenn bestellt, der oder dem Datenschutzbeauftragten anzuzeigen. Im folgenden Verfahren wird jeweils eine Beauftragte bzw. ein Beauftragter des Rektorats, der Betriebsräte sowie, wenn bestellt, die bzw. der Datenschutzbeauftragte Untersuchungen zur Aufklärung des angezeigten Verdachts auf Datenmissbrauch anstellen. Zu diesem Zweck sind alle Beteiligten zu hören, wobei die bzw. der eines Missbrauchs Beschuldigte Anspruch auf einen rechtsfreundlichen Beistand oder zumindest das Hinzuziehen einer Vertrauensperson hat. Aus diesen Untersuchungen und Anhörungen resultiert eine Empfehlung an das Rektorat, das die tatsächliche Entscheidung über Konsequenzen zu treffen hat. Eine deutliche Abweichung von der Empfehlung ist ausführlich zu begründen. Mögliche Konsequenzen bei nachgewiesenem Fehlverhalten sind die Verpflichtung zur Nachschulung, eine Einschränkung oder ein temporärer/dauerhafter Entzug der Berechtigungen, sowie eine Dokumentation im Personalakt. Eine Verhängung disziplinärer Maßnahmen im Sinne von § 96 Abs 1 Z 1 ArbVG ist damit nicht verbunden.

(6) Ist eine Mitarbeiterin oder ein Mitarbeiter über die Zulässigkeit einer Verarbeitung oder Übermittlung personenbezogener Daten im Zweifel, ist sie oder er berechtigt, vor Durchführung den Arbeitsauftrag schriftlich zu dokumentieren und, wenn bestellt, bei der bzw. dem Datenschutzbeauftragten, ansonsten bei der innerbetrieblichen Datenschutzkommission Information einzuholen. Der Mitarbeiterin bzw. dem Mitarbeiter dürfen hierdurch keine Nachteile entstehen. Die Stellungnahme der bzw. des Datenschutzbeauftragten oder der inner-betrieblichen Datenschutzkommission hat schriftlich zu erfolgen.

(7) Alle Mitarbeiterinnen und Mitarbeiter erhalten auf Anforderung einmal jährlich eine kurze, allgemein verständliche Auflistung im Sinne des § 26 DSG 2000. Die innerbetriebliche Datenschutzkommission kann für die jeweiligen Systeme Standardanfragen ausarbeiten und diese den Mitarbeiterinnen und Mitarbeitern zwecks Anfrage zur Verfügung stellen.

(8) Alle Mitarbeiterinnen und Mitarbeiter haben das Recht, Daten richtig stellen bzw. löschen zu lassen, wenn
1. sie nicht berechtigt ermittelt wurden,
2. sie nicht richtig sind, oder
3. für den vorgesehenen Zweck nicht mehr erforderlich sind.

Diesen Mitarbeiterinnen und Mitarbeitern und dem zuständigen Betriebsrat ist eine Überprüfungsmöglichkeit über die Korrektur bzw. Löschung einzuräumen. Entsteht Uneinigkeit über die Richtigkeit von Daten und kann das Rektorat die Richtigkeit nicht nachweisen, so sind diese Daten zu löschen.

(9) Alle mit und an Datenverarbeitungssystemen gemäß § 2 Abs 1 lit b arbeitenden Mitarbeiterinnen und Mitarbeiter sind ihrer Aufgabe entsprechend zu schulen. Dafür kann jeweils systembezogen in den Detail-(Zusatz-)Betriebsvereinbarungen ein Qualifizierungskonzept definiert werden.

§ 12 Inkrafttreten und Vertragsdauer

(1) Die Geltungsdauer dieser Rahmenbetriebsvereinbarung ist unbefristet; sie kann jedoch bei Übereinstimmung zwischen dem Rektorat der Medizinischen Universität Innsbruck und den Betriebsräten jederzeit durch eine neue ersetzt werden.

(2) Diese Rahmenbetriebsvereinbarung tritt mit Ablauf des Tages ihrer Veröffentlichung im Mitteilungsblatt der Medizinischen Universität in Kraft.

Innsbruck, am 06.11.2008

Für das Rektorat der Medizinischen Universität Innsbruck:

Ao. Univ.-Prof. Dr. Margarethe Hochleitner eh
Vizerektorin für Personal, Personalentwicklung und Gleichstellung

Ao. Univ. Prof. Dr. Martin Tiefenthaler eh
Vorsitzender des BR für das wissenschaftliche Personal
Gemäß Beschluss des Betriebsrates vom: 18.12.2006

ADir Monika Viehweider eh
Vorsitzende des BR für das allgemeine Universitätspersonal
Gemäß Beschluss des Betriebsrates vom: 05.11.2008

Anhänge

Anhang 1

Terminologie

(1) Datenverarbeitungssystem: jede Datenanwendung;

(2) ,,Daten'' (,,personenbezogene Daten''): Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist; ,,nur indirekt personenbezogen'' sind Daten dann, wenn der Personenbezug der Daten derart ist, dass die Identität der bzw. des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmt werden kann;

(3) ,,sensible Daten'' (,,besonders schutzwürdige Daten''): Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben;

(4) ,,Betroffene/Betroffener'': jede natürliche oder juristische Person oder Personengemeinschaft, deren Daten verwendet werden;

(5) ,,Auftraggeberin bzw. Auftraggeber'': natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie allein oder gemeinsam mit anderen die Entscheidung getroffen haben, Daten für einen bestimmten Zweck zu verarbeiten, und zwar unabhängig davon, ob sie die Verarbeitung selbst durchführen oder hiezu einen anderen heranziehen. Als Auftraggeberin bzw. Auftraggeber gelten die genannten Personen, Personengemeinschaften und Einrichtungen auch dann, wenn sie einem Anderen Daten zur Herstellung eines von ihnen aufgetragenen Werkes überlassen und die Auftragnehmerin bzw. der Auftragnehmer die Entscheidung trifft, diese Daten zu verarbeiten. Wurde jedoch der Auftragnehmerin bzw. dem Auftragnehmer anlässlich der Auftragserteilung die Verarbeitung der überlassenen Daten ausdrücklich untersagt oder hat die Auftragnehmerin bzw. der Auftragnehmer die Entscheidung über die Art und Weise der Verwendung, insbesondere die Vornahme einer Verarbeitung der überlassenen Daten, auf Grund von Rechtsvorschriften, Standesregeln oder Verhaltensregeln gemäß § 6 Abs. 4 DSG 2000 eigenverantwortlich zu treffen, so gilt die bzw. der mit der Herstellung des Werkes Betraute als datenschutzrechtliche Auftraggeberin bzw. datenschutzrechtlicher Auftraggeber;

(6) ,,Dienstleisterin bzw. Dienstleister'': natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie Daten, die ihnen zur Herstellung eines aufgetragenen Werkes überlassen wurden, verwenden;

(7) ,,Datei'': strukturierte Sammlung von Daten, die nach mindestens einem Suchkriterium zugänglich sind;

(8) ,,Datenanwendung'' (früher: ,,Datenverarbeitung''): die Summe der in ihrem Ablauf logisch verbundenen Verwendungsschritte, die zur Erreichung eines inhaltlich bestimmten Ergebnisses (des Zweckes der Datenanwendung) geordnet sind und zur Gänze oder auch nur teilweise automationsunterstützt, also maschinell und programmgesteuert, erfolgen (automationsunterstützte Datenanwendung);

(9) ,,Verwenden von Daten'': jede Art der Handhabung von Daten einer Datenanwendung, also sowohl das Verarbeiten als auch das Übermitteln von Daten;

(10) ,,Verarbeiten von Daten'': das Ermitteln, Erfassen, Speichern, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Benützen, Überlassen, Sperren, Löschen, Vernichten oder jede andere Art der Handhabung von Daten einer Datenanwendung durch die Auftraggeberin bzw. den Auftraggeber oder die Dienstleisterin bzw. den Dienstleister mit Ausnahme des Übermittelns von Daten;

(11) ,,Ermitteln von Daten'': das Erheben von Daten in der Absicht, sie in einer Datenanwendung zu verwenden;

(12) ,,Überlassen von Daten'': die Weitergabe von Daten von der Auftraggeberin bzw. vom Auftraggeber an eine Dienstleisterin bzw. einen Dienstleister;

(13) ,,Übermitteln von Daten'': die Weitergabe von Daten einer Datenanwendung an andere Empfänger als die Betroffene bzw. den Betroffenen, die Auftraggeberin bzw. den Auftraggeber oder eine Dienstleisterin bzw. einen Dienstleister, insbesondere auch das Veröffentlichen solcher Daten; darüber hinaus auch die Verwendung von Daten für ein anderes Aufgabengebiet der Auftraggeberin bzw. des Auftraggebers.

Anhang 2

Checkliste für die Informationsaufbereitung

(1) Für bestehende und neu einzuführende Datenverarbeitungssysteme oder für Änderungen an bestehenden Datenverarbeitungssystemen sind der innerbetrieblichen Datenschutzkommission bzw. den Betriebsräten nach Möglichkeit die nachfolgenden definierten Informationen ehestmöglich, d.h. schon im Planungsstadium (z.B. Istanalysen, Sollkonzept, Pflichtenheft, etc.) - schriftlich zur Verfügung zu stellen:

1. technische Systembeschreibung (Hard- und Softwarebeschreibung)
2. Datenverwendung (erfasste Daten): Alle mit EDV-Unterstützung verwendeten personenbezogenen Daten sind in einem Datenkatalog aufgelistet, der möglichst folgende Informationen zu enthalten hat:
    a. Dateiname/Tabellenname,
    b. Feldname,
    c. Feldinhalt (Beschreibung des Inhalts),
    d. Feldlänge,
    e. Lese- und Änderungsberechtigungen; rollenbezogene, benutzerbezogene Berechtigungen sind auf Anforderung der Datenschutzkommission bzw. den Betriebsräten nach Systemeinführung zur Verfügung zu stellen, zumindest jedoch am Beginn jedes Kalenderjahres;
    f. Hinweise auf die Aufbewahrungsverpflichtung der personenbezogenen Daten nach Austritt der Mitarbeiterin bzw. des Mitarbeiters,
    g. Sollten Datenfelder bzw. die Inhalte selbiger abgekürzt oder codiert werden, werden in einer separaten Tabelle die dazugehörigen Definitionen bzw. in Vollform zur Verfügung gestellt.
3. Systemdokumentation: Die Programmdokumentation hat möglichst folgende Informationen zu enthalten:
    a. Programmname, Versionsnummer
    b. Programminhalt (Produkt- und Leistungsumfang lt. Beschreibung der Herstellerin/ des Herstellers bzw. der Dienstleisterin/ des Dienstleisters, bei Eigenentwicklung durch die entsprechende Organisationseinheit, die mit der Entwicklung befasst ist),
    c. Programmeinsatz (kurze Beschreibung des vorgesehenen Einsatzes, ggf. genutzte Module, Berechtigungskonzept),
    d. Programmwartung (verantwortliche Stelle).
4. Verarbeitungsdokumentation (für standardisierte Verarbeitungen): Die durch die Programmanwendung durchgeführten standardisierten Verarbeitungen werden, soweit möglich, in einem Verarbeitungskatalog dokumentiert. Dieser Katalog enthält:
    a. Bezeichnung des Programmaufrufs,
    b. Beschreibung und Bezeichnung der standardisierten Auswertung,
    c. Verwendungszweck und ggf. Rechtsgrundlage bzw. Auftraggeber/in,
    d. Auflistung der in der Auswertung verarbeiteten Datenfelder,
    e. Muster von Bildschirm-Masken, Listen etc. (Druckerausgaben).

(2) Für zukünftige (geplante) Datenverarbeitungssysteme im Sinne von § 2 Abs 1 lit b sind neben der in Abs. 1 dargestellten Information zusätzlich folgende Informationen zur Verfügung zu stellen:

1. Zielsetzung des Projekts;
2. geplante Auswirkungen des Projekts auf die Verarbeitung von personenbezogenen Daten, Veränderung von Arbeitsabläufen und Arbeitsgestaltung;
3. Zeitplan des Projektablaufes bis zur Umsetzung;
4. Namen der Projektleiterin bzw. des Projektleiters, der System-Verantwortlichen und etwaiger Teilprojektleiterinnen bzw. Teilprojektleiter, sowie der involvierten Projektteam-Mitglieder;
5. Namen eventueller externer Beraterinnen bzw. Berater und Softwareentwicklerinnen bzw. Softwareentwickler und Firmen;
6. Gesamtkosten des Projekts;
7. Berechtigungskonzept;
8. Verwendete Hardware und Software (Technologien);
9. Standort und Vernetzung der verwendeten Hardware;
10. Übermittlung personenbezogener Daten von oder zur Medizinischen Universität Innsbruck.