Dienstvereinbarung zur Verarbeitung systemimmanenter Daten und der Einsichtnahme in Nutzdaten an der Universität Regensburg

Präambel

Beim Einsatz technischer Systeme erfolgen die verschiedenartigsten Aufzeichnungen, die es ermöglichen, Aspekte der Leistung oder des Verhaltens der Beschäftigten sichtbar oder kontrollierbar zu machen oder die sogar in das Persönlichkeitsrecht der Einzelnen eingreifen können. Das Recht auf informationelle Selbstbestimmung der Beschäftigten und ein verantwortungsvoller Umgang mit deren Daten sind ein hohes Gut.
Die Universität Regensburg will durch diese Regelung unter Beteiligung des behördlichen Datenschutzbeauftragten und nach Anhörung der Vertrauensperson der schwerbehinderten Menschen sowie der Gleichstellungsbeauftragten im Sinne der vertrauensvollen Zusammenarbeit mit der Personalvertretung die schutzwürdigen Belange der Beschäftigten bei gleichzeitiger Nutzung der Möglichkeiten moderner Technik wahren.

Art. 1 Geltungsbereich

(1) Diese Dienstvereinbarung gilt für alle an der Universität Regensburg tätigen Personen.

(2) Änderungen an der Organisation, den Zuständigkeiten oder der Aufgabenverteilung lassen diese Dienstvereinbarung unberührt.

(3) Innerhalb des Regelungsbereiches dieser Dienstvereinbarung können die Dienststelle und die Personalvertretung der Universität Regensburg weitere Festlegungen oder Ausführungsdienstvereinbarungen treffen.

(4) Personen, die nicht unter § 1 Abs. 1 fallen und die Zugang zu auf den IT-Systemen gespeicherte Daten haben, sind auf die Einhaltung der Regelungen dieser Dienstvereinbarung zu verpflichten.

(5) Die Dienstvereinbarung gilt für den Einsatz aller IT-Systeme, die im universitären Kontext verwendet werden.

Art. 2 Begriffsbestimmung

(1) Systemimmanente Daten im Sinne dieser Dienstvereinbarung sind Daten von Betriebssystemen, Netzwerken, Anwendungen, Entwicklungssystemen, Datenbanken und Verwaltungssystemen, Sicherheitssystemen oder ähnlichen Systemen, die entweder automatisch durch entsprechende Konfiguration oder als Nebenprodukt erzeugt werden und für sich oder in ihrer Summe oder Verknüpfung eine Identifikation von Beschäftigten oder Beschäftigtengruppen ermöglichen. Hierzu zählen insbesondere Accounting und Auditingdateien, Logdateien, Logbücher, Identifikations- und Authentifizierungsdaten, Transaktionsdaten, Daten der Lizenz/Netzwerküberwachung sowie Netzwerkprotokolldaten, Fehlerlisten, Daten der technischen Ressourcenverwaltung usw.

(2) Nutzdaten im Sinne dieser Vereinbarung sind alle Daten, die Beschäftigten zuzuordnen sind, deren Kenntnisnahme für Dritte durch technische Maßnahmen erschwert oder verhindert werden soll und die von Beschäftigten selbst oder durch Systemprozesse in dazu zur Verfügung gestellten Speicherbereichen abgelegt werden.

(3) Fernwartungs-\Fernzugriffsmaßnahmen (Remote Control) sind alle Maßnahmen und Möglichkeiten, mit denen unter Nutzung von Übertragungswegen auf Geräte, deren Bestandteile,

Netzwerke, Programme oder Daten Einsicht oder Einfluss genommen werden kann, wie z.B. Überwachung\Übertragung der Bildschirmausgabe oder der Tastatureingaben.

(4) Administrator/in im Sinne dieser Vereinbarung ist jede Person, die Zugriff auf systemimmanente Daten, Nutzdaten anderer Beschäftigter der Universität Regensburg oder auf Daten aus Fernwartungs-/Fernzugriffsmaßnahmen hat.

(5) Betriebseinheit im Sinne dieser Vereinbarung ist die jeweilige organisatorische Einrichtung (z.B. Rechenzentrum, Bibliothek, weitere zentrale Einrichtungen, Verwaltungs-DV, Fakultäten, Lehrstühle etc.), welche die Systeme betreibt, auf denen Daten im Sinne von (1) bis (3) anfallen bzw. bei welcher der/die Administrator/in beschäftigt ist.

Art. 3 Zweckbestimmung

(1) Das Aufzeichnen und Auswerten systemimmanenter Daten sowie Daten aus Fernwartungs-\Fernzugriffsmaßnahmen ist nur für folgende Zwecke zulässig:

a. Herstellung und Aufrechterhaltung der IT-Sicherheit und Integrität der Systeme
b. Nachweis über die Einhaltung datenschutzrechtlicher Bestimmungen
c. technische Fehlerfindung in den Systemen
d. Sicherstellung und Aufrechterhaltung der Betriebsbereitschaft des Systems sowie der Weiterentwicklung der Dienste in technischer Hinsicht

(2) Notwendige Auswertungen für die unter (1) genannten Zwecke haben den Erfordernissen der Dienststelle und den datenschutzrechtlichen Interessen der Beschäftigten Rechnung zu tragen.

Art. 4 Erhebung, Nutzung und Verarbeitung

(1) Die Erhebung, Nutzung und Verarbeitung systemimmanenter Daten sowie Daten aus Fernwartungs-\Fernzugriffsmaßnahmen zu den unter Art. 3 Abs. (1) genannten Zwecken sind ausschließlich durch die Administratorin/ den Administrator oder mit der technischen Problemlösung betraute Personen durchzuführen.

(2) Nimmt die Administratorin/der Administrator über diese Tätigkeit hinaus noch andere Aufgaben wahr, dürfen die aus der Tätigkeit als Administrator/in gewonnenen Erkenntnisse nicht für diese anderen Tätigkeiten weitergegeben oder verwendet werden. Selbiges gilt auch für die mit der technischen Problemlösung betrauten Personen.

(3) Alle in Art 4 Abs. (1) genannten Daten sind nicht länger aufzubewahren, als für die unter Art. 3 Abs. (1) genannten Gründe erforderlich ist.

(4) Bei Fremdvergaben von Administrator-Aufgaben an Dritte oder andere Dienststellen ist durch die Dienststelle die Einhaltung der Vorgaben dieser Dienstvereinbarung durch Vereinbarung sicherzustellen.

(5) Alle an der Erhebung, Nutzung und Verarbeitung Beteiligten haben die hierbei erlangten Kenntnisse vertraulich zu behandeln.

(6) Eine Weitergabe oder zur Verfügungstellung solcher Daten und Erkenntnisse, außer zu den in Art. 3 genannten Zwecken und abgesehen von den in Art. 5 und 6 geregelten Sachverhalten, ist ausgeschlossen. Eine Leistungs- und Verhaltenskontrolle mit Hilfe dieser Daten findet nicht statt.

Art.5 Auswertung in Sonderfällen

(1) Eine Auswertung systemimmanenter Daten sowie Daten aus Fernwartungs-\Fernzugriffsmaßnahmen darf, abgesehen von Art. 3, nur bei sicherheitsrelevanten Ereignissen und Ereignissen von strafrechtlicher Relevanz sowie bei schweren arbeitsrechtlichen Vergehen mit Begründung der Dienststelle und mit vorheriger Zustimmung der Personalvertretung erfolgen, sofern keine milderen Mittel zur Verfügung stehen. Sofortmaßnahmen zur Verhinderung des Missbrauchs oder der Beweissicherung bei offensichtlich strafrechtlicher Relevanz sind vor der Beteiligung der Personalvertretung zulässig, jedoch auch hier nur bei begründetem Verdacht. Der Personalrat ist im Nachgang darüber zu informieren. Gesetzliche Bestimmungen der Sicherheits- und Ermittlungsbehörden bleiben durch diese Dienstvereinbarung unberührt.

(2) Die Auswertung erfolgt gemeinsam durch den Datenschutzbeauftragten sowie eine Vertreterin/einen Vertreter der Dienststelle, der Systemverwaltung und der Personalvertretung.

(3) Die Auswertung ist zu protokollieren.

(4) Sollte sich der Tatverdacht nicht erhärten, sind das Protokoll sowie die im Zuge dieses Prozesses entstandenen Daten unverzüglich datenschutzrechtlich konform zu vernichten.

(5) Die Daten sind insbesondere auch zur Entlastung heranzuziehen.

Art.6 Einsicht in Nutzdaten

(1) Für die private Nutzung freigegeben sind die lokale Festplatte sowie das „persönliche Netzlaufwerk". Eine Einsichtnahme in die dort gespeicherten Nutzdaten ist grundsätzlich, abgesehen von den nachfolgend erläuterten Umständen, unzulässig. Nur aufgrund einer richterlichen Anordnung hin darf eine Einsichtnahme durch die Strafverfolgungsbehörden erfolgen. Sofortmaßnahmen zur Verhinderung des Missbrauchs, zur Sicherung der Betriebsbereitschaft oder der Beweissicherung sind vor der richterlichen Anordnung und vor der Beteiligung der Personalvertretung durch den Systemadministrator zulässig. Um einen reibungslosen Dienstbetrieb zu gewährleisten, soll, soweit es in den jeweiligen Betriebseinheiten möglich ist, Projektspeicherplatz zur Verfügung gestellt werden.

(2) Eine Unterscheidung von dienstlicher und privater Nutzung auf technischem Weg ist verlässlich nicht möglich. Protokollierung der Zugriffe und Erstellen von Sicherungskopien (Backup) erstrecken sich somit auch auf den privaten Anteil der Nutzdaten. Die Beschäftigten erklären durch die private Nutzung der Speicherbereiche ihre Einwilligung in die Protokollierung und die Erstellung von Sicherungskopien auch für den Bereich der privaten Nutzung.

Art. 7 Meinungsverschiedenheiten

(1) Meinungsverschiedenheiten über den Umgang mit systemimmanenten Daten, Nutzdaten sowie Daten aus Fernwartungs-\Fernzugriffsmaßnahmen oder die Auslegung dieser Dienstvereinbarung sind einvernehmlich beizulegen. An diesen Gesprächen nehmen der/die Vorgesetzte des betroffenen Bereichs sowie ein/e Vertreter/in der Universität und zwei Vertreter/in der Personalvertretung teil. Auf Wunsch einer beteiligten Partei kann ein/e unabhängige/r Experte/in und/oder die/der zuständige Administrator/in hinzugezogen werden, allerdings nur in beratender Funktion.

(2) Eine Einigung kann nur einstimmig erreicht werden.

(3) Bis zur Einigung ist die Fortführung der strittigen Maßnahmen unzulässig, sofern dies nicht aufgrund der unter Art. 3 Abs. (1) genannten Punkte notwendig ist.

Art. 8 Rechte der Beschäftigten und Personalvertretungen

(1) Die Personalvertretung hat ein Kontrollrecht über die Einhaltung dieser Dienstvereinbarung. Die Personalvertretung kann bei Verdacht auf Missbrauch systemimmanenter Daten, Benutzerdaten sowie Daten aus Fernwartungs-/Fernzugriffsmaßnahmen die Offenlegung der protokollierten Daten und eine Erläuterung der Sachlage verlangen. Alle Kenntnisse über den Inhalt der Daten sind vertraulich zu behandeln.

(2) Vor Einführungen, Inbetriebnahme und der Umsetzung erheblicher Änderungen von Systemen, die von dieser Dienstvereinbarung erfasst werden, ist nach Art. 75a BayPVG der Personalrat mit einzubeziehen. Im Falle von Änderungen, die zur Sicherung der Betriebsbereitschaft dienen oder die IT-Sicherheit betreffen, kann der PR, sollte eine Information im Vorfeld nicht mehr möglich sein, ausnahmsweise im Nachgang informiert werden, z.B. Patchen im Fall von Zero-Day-Exploits.

(3) Den Beschäftigten und Administratorinnen/Administratoren ist diese Rahmendienstvereinbarung in geeigneter Weise bekannt zu geben.

(4) Zuwiderhandlungen sind den Vertragspartnern unverzüglich mitzuteilen und durch geeignete Maßnahmen abzustellen und zu ahnden.

Art. 9 Schlussvorschriften

(1) Diese Dienstvereinbarung tritt mit der Unterzeichnung in Kraft.

(2) Sie kann von jedem Vertragspartner unter Einhaltung einer Frist von 3 Monaten schriftlich gekündigt werden. Nach Eingang der Kündigung müssen unverzüglich Verhandlungen über eine neue Dienstvereinbarung aufgenommen werden. Bis zum Abschluss der neuen Dienstvereinbarung gilt diese Dienstvereinbarung weiter.

(3) Die Vertragspartner werden diese Dienstvereinbarung nach Ablauf von 3 Jahren nach ihrem Inkrafttreten evaluieren und erforderlichenfalls anpassen.
Einzelne Bestimmungen können im gegenseitigen Einvernehmen jederzeit geändert, aufgehoben oder ergänzt werden.

(4) Sind oder werden Regelungen dieser Dienstvereinbarung unzulässig oder ungeeignet, so sind diese durch Ausführungen zu ersetzen, die dem gedachten Zweck am nächsten kommen.

Regensburg, den 15/3/18

.....
Dr. Christian Blomeyer

Regensburg, den 27.03.18

.....
Thomas Grimm