Dienstvereinbarung

zwischen

dem Thüringer Justizministerium

und dem Hauptpersonalrat des Thüringer Justizministeriums

§ 1 Gegenstand und Geltungsbereich

1. Diese Dienstvereinbarung regelt die Rahmenbedingungen für die Einführung und den Betrieb eines HAUSHALTSMANAGEMENTSYSTEMS (HAMASYS). Sie gilt für alle Beschäftigten im Geschäftsbereich des Thüringer Justizministeriums, die Nutzer von HAMASYS sind.
2. Mit dem Abschluss der Dienstvereinbarung stimmt der Hauptpersonalrat dem Einsatz von HAMASYS zu. Für die tatsächliche Einführung der Module, die Erhebung und Verarbeitung personenbezogener Daten der Beschäftigten, die Regelung für den Datenzugriff, die Überwachung der Nutzer des Systems und die daraus folgenden organisatorischen Änderungen gelten die folgenden Bestimmungen.

§ 2 Ziele

Ziele des Einsatzes von HAMASYS sind die Optimierung und Stärkung der wirtschaftlichen Leistungsfähigkeit, die Steigerung der Dienstleistungsqualität und die Verbesserung der Arbeitsbedingungen der Beschäftigten.
Es ist nicht Ziel beim Einsatz von HAMASYS, die Leistung und das Verhalten der Mitarbeiterinnen und Mitarbeiter zu kontrollieren oder die Wertigkeit der Arbeitsplätze zu verringern.

§ 3 Grundsätze für die Einführung des Systems, seiner Module und deren Änderungen

1. Das Aktivieren und Betreiben von Komponenten unterliegen der Mitbestimmung des Hauptpersonalrates gemäß § 74 Abs. 2 Nr. 11 des Thüringer Personalvertretungsgesetzes (ThürPersVG). Das Thüringer Justizministerium legt dem Hauptpersonalrat vor Aktivieren und Betreiben neuer Module mindestens folgende Angaben vor:

   - Bezeichnung, Aufgabenstellung und Zielsetzung des Moduls
   - Technische Ausstattung der Arbeitsplätze
   - Schulungsplan, Qualifizierungsmaßnahmen
   - Angaben über die Erhebung, Verarbeitung, Nutzung und Auswertung personenbezogener Daten
   - Schnittstellenkonzept
   - Berechtigungskonzept

2. Soweit im Rahmen der Einführung Projekt-, Arbeits- bzw. Koordinierungsgruppen gebildet werden, können jeweils bis zu zwei Vertreter des örtl. Personalrates und des Hauptpersonalrates teilnehmen.
3. Bei den diese Dienstvereinbarung berührenden Änderungen und Erweiterungen von Modulen ist der Hauptpersonalrat über Art, Umfang und Folgen der Änderung rechtzeitig zu informieren.
4. Die Anwender und der Hauptpersonalrat sind über jede Maßnahme, die mit einer wesentlichen Änderung des Verfahrens HAMASYS verbunden ist, rechtzeitig, fortlaufend und umfassend zu informieren. Dazu gehören insbesondere Informationen über die geplante Einführung von zusätzlichen Modulen, Auswirkungen auf die Arbeitsplätze, Arbeitsinhalte und Qualifikationsanforderungen.

§ 4 Systemdokumentation

Die Systemdokumentation einschließlich der Einführungs-, Schulungs-, Benutzer-, Installations- und Betriebshandbücher liegt ab der Produktivsetzung des Verfahrens vor und ist Bestandteil dieser Dienstvereinbarung.

§ 5 Leistungs- und Verhaltenskontrolle

Es werden nur solche personenbezogenen Daten erfasst, die zur Erfüllung der vereinbarten Zweckbestimmung von HAMASYS einschließlich der dafür notwendigen Sicherungsmaßnahmen erforderlich sind. Individuelle Leistungs- und/oder Verhaltenskontrollen bezogen auf Anwender oder eine Gruppe von Anwendern sind verboten, es sei denn, der Hauptpersonalrat stimmt in Abstimmung mit dem örtlichen Personalrat im begründeten Ausnahmefall zu. Auswertungen von Logdateien sind nur bei sicherheitsrelevanten Vorgängen zulässig. Der Personalrat ist unverzüglich zu informieren.
Eine persönliche Identifizierung der Anwender an den Systemen dient nur zur Überprüfung der Zugriffsberechtigung, der Zuordnung von Arbeitsvorgängen im Rahmen der Arbeitsorganisation sowie der Identifikation von Bearbeitern bei laufenden oder abgeschlossenen Vorgängen zum Zwecke erforderlicher Rückfragen.
Alle personenbezogenen Daten werden durch technische und/oder organisatorische Maßnahmen vor Zugriffen unbefugter Personen und vor einer Nutzung, die nicht der vereinbarten Zielsetzung entspricht, geschützt.
Beschäftigte erhalten auf Antrag im Rahmen der gesetzlichen Vorschriften vollständige Informationen über alle sie betreffenden, gespeicherten und personenbezogenen Daten im Zusammenhang mit der Einführung und dem Einsatz von HAMASYS.

§ 6 Datenschutz- und Sicherheitsmaßnahmen

6.1 Technische Maßnahmen
Es werden alle angemessenen technischen Möglichkeiten der eingesetzten PC- und Netzwerktechnik genutzt, um sicherzustellen, dass nur die nach § 5 zulässigen Daten gespeichert werden.

6.2 Organisatorische Maßnahmen
Weil die Einhaltung der Datenschutz- und Datensicherheitsmaßnahmen auch abhängig vom Verantwortungs- und Datenschutzbewusstsein der betroffenen Anwender ist, muss sich jeder Anwender, insbesondere jeder Vorgesetzte, mit den Bestimmungen des Da-

tenschutzgesetzes, den erforderlichen Sicherheitsbestimmungen und den Bestimmungen dieser Dienstvereinbarung vertraut machen. Dies ist bei der Qualifizierung in besonderem Maße zu berücksichtigen.

Folgende organisatorische Maßnahmen, die auch im Zusammenhang mit dem Berechtigungskonzept stehen, werden getroffen:

1. Die Vergabe der Zugriffsberechtigungen für einzelne Anwender wird ausschließlich gemäß den dienstlichen Aufgaben erteilt. Das Berechtigungskonzept ist nach Tätigkeitsgebieten und Funktionen festzulegen.
2. Die Einstellung der Berechtigungen erfolgt in Funktionstrennung zwischen Programmierung und Administration der Berechtigungen. Veränderungen der Berechtigungen werden durch das System protokolliert.
3. Bei Einrichtung/Änderung der Berechtigung während des Produktivsystems sind Veränderungen der Rollen zu definieren und mit dem Hauptpersonalrat abzustimmen.
4. Die Dienststelle benennt verantwortliche Personen, die für die Einhaltung und Weiterentwicklung der technischen und organisatorischen Maßnahmen bei der Verarbeitung von Mitarbeiterdaten zuständig sind. Der Hauptpersonalrat ist davon zu informieren.

Im Übrigen gelten die Bestimmungen des Thüringer Datenschutzgesetzes in der jeweils gültigen Fassung.

6.3 Einsatz von Sicherheitskomponenten; digitale Signatur und Verschlüsselung
Der Einsatz des Verfahrens wird durch technische Einrichtungen hochwertig gesichert:

1. Mindestens jeder anordnende Arbeitsplatz wird mit einer Sicherheitseinrichtung, bestehend aus einem Chipkartenlesegerät und darauf abgestimmten Programmen, ausgestattet. Die Beschäftigten erhalten für Zwecke der Identifikation und Verschlüsselung sog. Chipkarten. Die im bisherigen Verfahren erforderliche Unterschrift auf Papierunterlagen wird durch eine rechtsgültige „elektronische Unterschrift“ (digitale Signatur) ersetzt. Maßgebliche Rechtsgrundlage hierfür ist das Gesetz zur digitalen Signatur (Signaturgesetz - SigG) und die Signaturverordnung (SigV). Die eingesetzten Chipkarten entsprechen den Vorgaben des Signaturgesetzes. Sie werden von einer nach den Vorgaben des Signaturgesetzes genehmigten Zertifizierungsstelle bereitgestellt.
2. Die Verwaltung stellt sicher, dass
   - ausschließlich personenbezogene Daten an die Zertifizierungsstelle weitergegeben werden, die nach dem SigG erforderlich sind,
   - Beschäftigte schriftlich über die digitale Signatur und das Antragsverfahren sowie den Umgang mit der Chipkarte in Verbindung mit der persönlichen Identitätsnummer (PIN) aufgeklärt werden.
   - keine unmittelbaren dienstlichen vertraglichen Bindungen zwischen Beschäftigten und der Zertifizierungsstelle bestehen,
   - Beschäftigte von sämtlichen Ansprüchen freigestellt werden, die durch die Zertifizierungsstelle verursacht werden,
   - die öffentliche Bekanntgabe gültiger und gesperrter Zertifikate anonymisiert erfolgt und
   - Aufgaben der Systemverwaltung und -pflege grundsätzlich nicht zusammen mit Anwendungsaufgaben in einer Rolle vereinigt werden dürfen.

3. Der Beschäftigte ist darüber aufzuklären, dass
   - der Verlust oder der Verdacht der missbräuchlichen Nutzung der Signaturkarte durch Dritte dem Beauftragten für den Haushalt (BfdH) sofort anzuzeigen sind,
   - bei Verlust oder missbräuchlicher Nutzung der Signaturkarte durch Dritte der Beschäftigte bei grob fahrlässigem oder vorsätzlichem Verhalten durch den Dienstherrn in Regress genommen werden kann und
   - ein Zuwiderhandeln gegen diese Dienstvereinbarung mit arbeits- bzw. disziplinarrechtlichen Maßnahmen geahndet werden kann.

6.4 Sorgfaltspflicht der Beschäftigten und der Dienststellen

1. Die Anwenderkennung (Kennwort, Benutzername, Zugangscode) ist nicht übertragbar. Der Beschäftigte ist verantwortlich für den Schutz der ihm zugeordneten Anwenderkennung.
2. Die Dienststellen sind für die Sicherheit der Hardware verantwortlich. Es werden geeignete Verfahren gegen Missbrauch eingesetzt. Der Hauptpersonalrat und die Beschäftigten werden über die eingesetzten Verfahren informiert. Die Beschäftigten sind verpflichtet, die Dienststellen dabei, soweit es ihnen möglich und zumutbar ist, zu unterstützen.
3. Die Verwendung der Signierkomponenten wird auf dienstliche Zwecke beschränkt. Eine Nutzung für private Zwecke ist untersagt.

6.5 Aufbewahrungsfrist

Die Aufbewahrungsfristen der Dateien und Listen richten sich nach der Thüringer Landeshaushaltsordnung und den dazu erlassenen Bestimmungen und dem Thüringer Datenschutzgesetz in der jeweils gültigen Fassung.

§ 7 Schulungsmaßnahmen

1. Alle Anwender, deren Arbeitsplatz durch die Einführung von HAMASYS betroffen ist, sind zeitnah zum Einführungstermin durch entsprechende Fort- und Weiterbildung zu qualifizieren. Diese Maßnahmen finden innerhalb der Arbeitszeit statt.
2. Für alle Module und für alle Anwender werden entsprechende Schulungspläne erstellt. Der Schulungsplan enthält mindestens folgende Bestandteile:

   - Überblick über den Aufbau des Systems, die eingesetzten Module, die Arbeitsweise und Bedienung
   - konkrete Arbeitsabläufe und praktische Übungen
   - Aufbauschulungen und Erfahrungsaustausche

§ 8 Arbeits- und Gesundheitsschutz

Bei der Einrichtung oder Umrüstung von Arbeitsplätzen sind die neuesten arbeitswissenschaftlichen und arbeitsmedizinischen Erkenntnisse anzuwenden.

§ 9 Informations- und Prüfungsrechte

Der Hauptpersonalrat hat das Recht,

1. sich alle Funktionen anzeigen und ausdrucken zu lassen, die Aufschluss über den Systemzustand geben und

2. Einsicht in sämtliche System-, Überwachungs- und Änderungsprotokolle, Schnittstellendateien, Dokumentationen der Stapelprozesse, System- und Anwendungsunterlagen zu erhalten.

§ 10 Beschwerderecht und Konfliktregelung

1. Soweit sich Beschäftigte über die Nichteinhaltung dieser Dienstvereinbarung, über Folgen von getroffenen Maßnahmen und Regelungen im Gegenstandsbereich dieser Dienstvereinbarung beschweren, ist der Hauptpersonalrat zu informieren, sofern der Beschäftigte damit einverstanden ist.
2. Bei Streitigkeiten über die Auslegung und Anwendung dieser Dienstvereinbarung sind diese zwischen den Vertretern des Hauptpersonalrates und dem Dienststellenleiter des Thüringer Justizministeriums mit dem Ziel einer einvernehmlichen Einigung in einem gemeinsamen Gespräch zu erörtern. Der Rechtsweg zu den zuständigen Gerichten wird hierdurch nicht berührt.

§ 11 Kündigung

Diese Dienstvereinbarung kann mit einer Frist von 3 Monaten zum Schluss eines Kalenderjahres von beiden Seiten gekündigt werden. Die einvernehmliche Änderung ist jederzeit möglich. Kündigung und Änderung bedürfen der Schriftform.

§ 12 Gleichstellungsbestimmung

Status- und Funktionsbezeichnungen in dieser Vereinbarung gelten jeweils in männlicher und weiblicher Form.

§ 13 In-Kraft-Treten

1. Diese Dienstvereinbarung tritt am Tage ihrer Unterzeichnung in Kraft und ist den Beschäftigten rechtzeitig bekannt zu geben.
2. Sind Teile dieser Dienstvereinbarung nichtig, so bleiben die anderen Teile dieser Vereinbarung unberührt.

Erfurt, im Juli 2006

Thüringer Justizministerium	Hauptpersonalrat des
Der Staatssekretär	Thüringer Justizministeriums
In Vertretung	Die Vorsitzende
11.07.2006	
gez. Stefan Kaufmann	gez. Barbara Zwinkau
Stefan Kaufmann	Barbara Zwinkau