Dienstvereinbarung

Zwischen der Hochschulleitung der Ludwig-Maximilians-Universität München (LMU),
vertreten durch den Präsidenten, Herrn Prof. Dr. Dr. h.c. Bernd Huber,
und den Vizepräsidenten für den Bereich der Wirtschafts- und Personalverwaltung,
Herrn Dr. Christoph Mülke
und
dem Personalrat der LMU,
vertreten durch die Vorsitzende, Frau Grit Kermes,
wird folgende Dienstvereinbarung über den
Umgang mit systemimmanenten Daten zur Gewährleistung der Informationssicherheit an der LMU
geschlossen.

Gemeinsam im Folgenden: „Vertragspartner"

Präambel

Durch diese Dienstvereinbarung sollen die schutzwürdigen Belange der Beschäftigten beim notwendigen Einsatz von Maßnahmen zur Gewährleistung der IT-Sicherheit an der LMU geregelt werden.

1. Geltungsbereich

1.1 Diese Dienstvereinbarung gilt für alle Personen, die die dienstlich bereitgestellte Informationstechnologie der LMU nutzen.

1.2 Änderungen an der Organisation, den Zuständigkeiten, der Aufgabenverteilung oder der Rechtsform lassen diese Dienstvereinbarung unberührt.

2. Begriffsbestimmung

2.1 Systemimmanente Daten im Sinne dieser Dienstvereinbarung sind erzeugte Daten von IT-Bausteinen, wie bspw. Betriebssystemen, Netzwerkkomponenten, Anwendungen, Entwicklungssystemen, Datenbanken, Verwaltungs- oder Sicherheitssystemen, die für sich oder in ihrer Summe oder Verknüpfung eine Identifikation von Personen oder Personengruppen ermöglichen. Hierzu zählen insbesondere Logdateien, in denen bspw. Identifikations- und Authentifizierungsvorgänge protokolliert sind oder Daten der Lizenz- oder Netzwerküberwachung.

2.2 Personenbezogene Benutzerdaten im Sinne dieser Vereinbarung sind alle Daten i.S.v. Art. 4 Nr. 1 DSGVO, die Beschäftigten zuzuordnen sind.

2.3 Fernüberwachungsmaßnahmen sind alle Maßnahmen und Möglichkeiten, mit denen unter Nutzung von Übertragungswegen auf Geräte, deren Bestandteile, Netzwerke, Programme oder Daten Einsicht oder Einfluss genommen werden können.

2.4 Mit Systemadministration im Sinne dieser Vereinbarung ist die Gruppe der Beschäftigten an der LMU gemeint, die Zugriff auf systemimmanente Daten sowie auf

personenbezogene Benutzerdaten oder auf Daten aus Fernüberwachungsmaßnahmen hat.

2.5 Dienststelle im Sinne dieser Vereinbarung ist die organisatorische Einheit (z. B. Zentrale Universitätsverwaltung, Fakultät, Department, Institut, Lehrstuhl usw.), welche die Systeme betreibt, auf der Daten im Sinne von 2.1 bis 2.3 anfallen bzw. bei welcher der Systemadministrator oder die Systemadministratorin beschäftigt ist.

3. Zweckbestimmung

3.1 Das Protokollieren und Auswerten personenbezogener systemimmanenter Daten sowie personenbezogener Daten aus Fernüberwachungsmaßnahmen ist nur für folgende Zwecke zulässig:

- Gewährleistung der maßgeblichen Schutzziele der Informationssicherheit, z.B. Herstellung und Sicherstellung der Betriebssicherheit und Integrität der Systeme, Sicherstellung und Aufrechterhaltung der Betriebsbereitschaft der Systeme, technische Fehlerfindung in den Systemen,
- Nachweis über die Einhaltung maßgeblicher datenschutzrechtlicher und informationssicherheitsrechtlicher Bestimmungen.

3.2 Protokollierungen und Auswertungen für die unter 3.1 genannten Zwecke haben den Erfordernissen des ordnungsgemäßen Betriebs Rechnung zu tragen.

4. Verarbeitung

4.1 Die Verarbeitung systemimmanenter Daten sowie Daten aus Fernüberwachungsmaßnahmen zu den unter 3.1 genannten Zwecken ist ausschließlich durch die Systemadministration durchzuführen.

4.2 Nimmt die Systemadministration über diese Tätigkeit hinaus noch andere Aufgaben wahr, dürfen die aus der Administrationstätigkeit gewonnenen Erkenntnisse nicht für diese anderen Tätigkeiten weitergegeben oder verwendet werden.

4.3 Die in 4.1 genannten Daten werden grundsätzlich für die Dauer bis zu 7 Werktage aufbewahrt und dann automatisch gelöscht oder wirksam anonymisiert. Eine längere Speicherung der personenbezogenen Daten ist für die in Ziffer 3.1 genannten Zwecke zulässig, soweit dies geltender Rechtslage entspricht und die Speicherung auf getrennten, nach dem Stand der Technik gesicherten Systemen[1] erfolgt. Für diese Systeme ist ein Rechte- und Rollenkonzept zu erstellen und mit dem behördlichen Datenschutzbeauftragten sowie der Personalvertretung, soweit Beschäftigte gemäß Art. 4 BayPVG betroffen sind, abzustimmen.

4.4 Die jeweilige Dienststelle, der behördliche Datenschutzbeauftragte sowie die Personalvertretung haben im Rahmen ihrer Zuständigkeiten Kontrollrechte im Hinblick auf die Einhaltung der Bestimmungen dieser Dienstvereinbarung.

[1] Für den Stand der Technik gelten z.B. nationale und internationale Sicherheitsstandards wie DIN, ISO, DKE oder ISO/IEC oder die jeweils aktuellen Empfehlungen des Arbeitskreis „Stand der Technik" des Teletrust (https://www.teletrust.de/arbeitsgremien/ak-stand-der-technik/).

4.5 Sämtliche aus der Verarbeitung und Auswertung erlangten Kenntnisse über systemimmanente oder personenbezogene Daten sind vertraulich zu behandeln.

4.6 Die personenbezogene Verarbeitung, insbesondere Auswertung, von Daten der Beschäftigten zur Überwachung ihres Verhaltens oder ihrer Leistung ist unzulässig.

4.7 Eine Weitergabe oder Zurverfügungstellung solcher Daten und Erkenntnisse außerhalb gesetzlicher Vorschriften ist untersagt.

4.8 Besondere Regelungen können einvernehmlich zwischen Dienststelle, Personalvertretung und dem behördlichen Datenschutzbeauftragten im Rahmen ihrer Zuständigkeiten getroffen werden.

5. Personenbezogene Auswertung

5.1 Eine personenbezogene Auswertung systemimmanenter Daten, personenbezogener Benutzerdaten sowie personenbezogener Daten aus Fernüberwachungsmaßnahmen darf nur in Ausnahmefällen, wie z.B.

- zur unmittelbaren Abwehr eines bevorstehenden erheblichen Angriffs auf die IT-Infrastruktur,
- bei Gefahr im Verzug,
- zur Bekämpfung einer konkreten Gefahr oder
- bei hinreichendem Verdacht auf einen Missbrauch

unter Beachtung des Verhältnismäßigkeitsgrundsatzes und – soweit Beschäftigte gemäß Art. 4 BayPVG betroffen sind – im Benehmen mit der Personalvertretung erfolgen. Der Zugriff aufgrund Gesetzes, z.B. durch Strafverfolgungsbehörden, bleibt hiervon unberührt.
Sofortmaßnahmen, die zur Verhinderung des Missbrauchs und zur Beweissicherung dienen sollen, sind ausschließlich im „Mehraugenprinzip“ und – soweit deren Zuständigkeit gegeben ist – auch vor der Beteiligung der Personalvertretung zulässig.

5.2 Die Auswertung erfolgt gemeinsam durch eine Vertretung der Dienststelle, der Systemadministration, des behördlichen Datenschutzbeauftragten oder der für den jeweiligen Bereich zuständigen Datenschutzkontaktperson und der Personalvertretung.

5.3 Die Auswertung ist zu protokollieren.

5.4 Die Daten der Auswertung sind auch zur Entlastung heranzuziehen.

6 Rechte der Beschäftigten und der Personalvertretung

6.1 Den Beschäftigten stehen unter den jeweils geltenden gesetzlichen Voraussetzungen folgende Datenschutzrechte zu:

- Auskunftsrecht (Art. 15 DSGVO)
- Recht auf Datenberichtigung (Art. 16 DSGVO)
- Recht auf Löschung personenbezogener Daten und Recht auf Vergessen (Art. 17 DSGVO)
- Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO)
- Widerspruchsrecht (Art. 21 DSGVO)
- Recht auf Datenübertragbarkeit (Art. 20 DSGVO)

6.2 Die Personalvertretung kann im Rahmen ihrer Zuständigkeit bei hinreichendem Verdacht auf Missbrauch systemimmanenter Daten, personenbezogener Benutzerdaten sowie Daten aus Fernüberwachungsmaßnahmen die Offenlegung der protokollierten Daten und eine Erläuterung der Sachlage verlangen, soweit dem keine gesetzlichen Vorschriften entgegenstehen. Alle Kenntnisse über den Inhalt der Daten unterliegen der Verschwiegenheit.

7 Schlussvorschriften

7.1 Diese Dienstvereinbarung tritt mit der Unterzeichnung in Kraft.

7.2 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, soweit die Regelungen nicht gegen höherrangiges Recht verstoßen.

7.3 Einzelne Bestimmungen können im gegenseitigen Einvernehmen jederzeit geändert, aufgehoben oder ergänzt werden.

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

7.5 Auslegungen über den Umgang mit systemimmanenten Daten, personenbezogenen Benutzerdaten sowie Daten aus Fernüberwachungsmaßnahmen oder die Auslegung dieser Dienstvereinbarung sollen einvernehmlich beigelegt werden. Bis zur Entscheidung ist die Fortführung der strittigen Maßnahmen auszusetzen, sofern bzw. soweit diese nicht zur Erfüllung gesetzlicher Pflichten, für die Wahrung der unter Ziffer 3.1 genannten Zwecke, zur unmittelbaren Abwehr eines erheblichen Angriffs auf die IT-Infrastruktur, bei Gefahr im Verzug, zur Bekämpfung einer konkreten Gefahr oder bei hinreichendem Verdacht auf einen Missbrauch notwendig ist.

7.6 Den Beschäftigten und der Systemadministration ist diese Dienstvereinbarung in der jeweils gültigen Fassung durch den Vizepräsidenten für den Bereich der Wirtschafts- und Personalverwaltung in geeigneter Weise bekannt zu geben.

München, den 14.06.2024

Prof. Dr. Dr. h.c. Bernd Huber
Präsident

Dr. Christoph Mülke
Vizepräsident

Grit Kermes
Vorsitzende des Personalrats