LEUPHANA
UNIVERSITÄT LÜNEBURG

DV-SAP-HR Anlage 8 - Datenschutzkonzept

Datenschutzkonzept für SAP-HR

0. Zustimmung des Datenschutzbeauftragten

Dieses Datenschutzkonzept ist mit dem Datenschutzbeauftragten der Leuphana Universität Lüneburg abgestimmt.

1. Allgemeines zum Konzept

Personenbezogene Daten sind nach der Begriffsbestimmung des niedersächsischen Datenschutzgesetzes Einzelangaben über persönliche oder sachliche Verhältnisse von bestimmten oder bestimmbaren natürlichen Personen (Betroffene).
Aufgrund des in Verbindung mit der Verarbeitung von HR-Daten entstehenden hohen Risikos erfolgt der SAP-HR Einsatz lediglich zentral in der Personalverwaltung (Modul Personaladministration) und im Finanzservice (Modul Organisationsmanagement). Die speziellen Risiken werden des Weiteren durch ein spezifisches Berechtigungskonzept, restriktives Customizing des SAP-Systems und ein Protokollierungskonzept für den Bereich HR berücksichtigt. Alle nicht technisch zu lösenden Problemfälle werden mittels der Dienstvereinbarung und der Dienstanweisung für die Handhabung des SAP R/3 Systems Modul HR geregelt.

2. Auftragskontrolle

2.1. Gemäß der datenschutzrechtlichen Spezialregelung des § 101 Abs. 2 NBG ist allen Anwendern/innen, die personenbezogene Daten verarbeiten, untersagt, diese Daten zu einem anderen als dem zur jeweiligen Aufgabenerfüllung gehörenden Zweck zu verarbeiten. Das Datengeheimnis besteht auch nach Beendigung der Tätigkeit fort.

2.2. Alle Anwender, die personenbezogene Daten verarbeiten, werden bei der Aufnahme ihrer Tätigkeit über ihre Pflichten nach Abs. 2.1 unterrichtet und auf deren Einhaltung verpflichtet.

3. Sicherungsmaßnahmen

Die in HR zu verarbeitenden personenbezogenen Daten sind der Schutzstufe C zugeordnet (vgl. Anhang). Zur Gewährung des Datenschutzes sind daher folgende Sicherungsmaßnahmen zu beachten:

3.1. Zugangskontrolle

Unbefugten ist der Zugang zur Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren. Deshalb sind:

3.1.1. Räume oder Datenverarbeitungsanlagen, in/mit denen personenbezogene Daten verarbeitet werden, bei Abwesenheit der berechtigten Personen auch wenn dies nur vorübergehend ist, zu verschließen/zu sichern. Gleichzeitig sollte ein Passwortschutz eingerichtet werden.

3.1.2. Datenträger mit personenbezogenen Daten (elektronische Datenträger, Ausdrucke), sofern nicht mit ihnen gearbeitet wird, unter Verschluss zu halten.

Die Datenbankserver stehen in einem gesonderten und gesicherten Systembetriebsraum, zu dem nur mit der Systemverwaltung betraute Personen Zugang haben (Einzelheiten hierzu sind im „Betriebskonzept zum SAP-Einsatz an den niedersächsischen Hochschulen im Rahmen des SAP-Referenzmodells“ beschrieben).

3.2. Speicher-, Zugriffs-, Benutzer- und Datenträgerkontrolle

Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Weiterhin ist zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert, gelöscht oder entfernt werden können oder dass durch Unbefugte Eingaben vorgenommen werden. Durch ein Berechtigungskonzept ist gewährleistet, dass die HR-berechtigten Sachbearbeiter/innen nur Zugriff auf die für ihre Aufgabenerfüllung notwendigen Bereiche innerhalb von SAP HR haben.

3.2.1. Speicherung, Übermittlung, Veränderung und Löschung von Daten sowie deren Auswertung und Ausdruck sind nur bei Aufgabenerfüllung und dienstlichen Anforderungen, soweit sie datenschutzmäßig korrekt sind, zulässig.

3.2.2. Die Fertigung der Kopie einer Datenauswertung mit personenbezogenen Daten (z. B. Diskette) ist nur zulässig, wenn dies für die Aufgabenerfüllung oder zum Zweck der Datensicherung erforderlich ist. Bei Herstellung einer Kopie sind Zeitpunkt und Anlass aufzuzeichnen. Die Kopien sind getrennt von dem Originalbestand aufzubewahren.

3.2.3. Der Zugang zu personenbezogenen Daten ist nur für die Mitarbeiter/innen des Personaldezernats und des Finanzdezernates zulässig. Genaue Ausgestaltungen sind in einem Berechtigungskonzept (Anlage 5 der Dienstvereinbarung) geregelt.

3.2.4. Eine Koppelung von Datenverarbeitungsanlagen, die zu Lehr- und Forschungszwecken eingesetzt werden, ist unzulässig.

3.3. Eingabekontrolle

Es ist sicherzustellen, dass nachträglich feststellbar ist, welche personenbezogenen Daten in welcher Zeit von wem in ein Datenverarbeitungssystem eingegeben worden sind. Deshalb sind Eingabe, Veränderung und Löschung solcher Daten automatisiert zu protokollieren. Ist dies aus technischen Gründen nicht möglich, sind sie in anderer Weise zu protokollieren.

3.4. Übermittlungskontrolle

Die Übermittlung personenbezogener Daten an Dritte ist unter Angabe des Empfängers und des Anlasses festzuhalten. Werden personenbezogene Daten als Ausdruck, per CD, per E-Mail etc. weitergegeben, ist auf die Geheimhaltungsvorschriften hinzuweisen.

3.5. Transportkontrolle

Die Versendung von Datenträgern mit personenbezogenen Daten (z. B. CD) ist in einem verschlossenen Umschlag durchzuführen. Die Versendung bzw. die Übergabe ist schriftlich festzuhalten. Die Übergabe von Hand zu Hand ist vorzuziehen.

3.6. Ausmusterung von Computern und Datenträgern

EDV-Systeme werden bei Ausmusterung vollständig und irreversibel gelöscht.