Universität Innsbruck

Richtlinie für die Verwendung personenbezogener Daten

1. Einleitung

Die Nutzung von IT-Systemen zur Informationsbeschaffung und -verarbeitung und zur Kommunikation ist zur alltäglichen Routine geworden und durchdringt die Geschäftstätigkeit der Universität Innsbruck weitgehend. Bei ordnungsgemäßer Benützung erleichtert dies viele Tätigkeiten; manche Arbeiten sind ohne den Einsatz von Computern nicht mehr denkbar.

Fahrlässige oder gesetzeswidrige Verwendung kann zum Verlust der Vertraulichkeit, Verfügbarkeit und Integrität von personenbezogenen oder andern vertraulichen Informationen führen, die IT-Sicherheit bedrohen und die Rechte anderer Personen verletzen. Die Universität Innsbruck verlangt daher von allen Mitarbeiterinnen und Mitarbeitern einen sorgfältigen und verantwortungsvollen Umgang mit Daten und IT-Systemen.

Ziel dieser Richtlinie ist es, Mindeststandards für die Nutzung und den Betrieb von IT-Systemen zu etablieren und die rechtskonforme Verarbeitung personenbezogener und vertraulicher Daten durch die zuständigen Stellen der Universität Innsbruck zu gewährleisten.

Die Universität Innsbruck will insbesondere erreichen, dass

- nur Befugte die Daten zur Kenntnis nehmen können (Vertraulichkeit),
- die Daten während der Bearbeitung unversehrt, vollständig und aktuell bleiben (Integrität),
- die Daten jederzeit ihrem Ursprung zugeordnet werden können (Authentizität),
- festgestellt werden kann, wer zu einem Zeitpunkt welche Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit),
- die Verfahrensweisen bei der Verarbeitung von Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Weise nachvollzogen werden können (Transparenz).

Dabei ist der Grundsatz zu beachten, dass der Aufwand in einem angemessenen Verhältnis zum Schutzzweck zu stehen hat.

Diese Richtlinie gilt für alle Anwendungen und IT-Systeme mit personenbezogenen und vertraulichen Daten und für alle Systeme, auf denen Benutzerinnen- und Benutzerdaten (insbesondere Benutzerkennung und Passwort) verwendet werden, mit denen auf solche Daten zugegriffen werden kann.

Bezüglich der Begriffsbestimmungen wird auf die „Rahmenbetriebsvereinbarung zur automatisationsunterstützten Verwendung personenbezogener Daten“ und das Datenschutzgesetz 2000 verwiesen.

A Endbenutzerinnen und Endbenutzer

2. Wie informiere ich mich über Datenschutz und IT-Sicherheit?

1. Alle Beschäftigten sind verpflichtet, sich über die Bestimmungen des Datenschutzes und der IT-Sicherheit zu informieren, sowie die einschlägigen Richtlinien, Betriebsvereinbarungen und Gesetze einzuhalten. Die Universität Innsbruck hat dafür Sorge zu tragen, dass entsprechende Schulungsmöglichkeiten bei Bedarf organisiert werden.

2. Der ZID und die Stabstelle für Personalentwicklung bieten Schulungen zur IT-Infrastruktur, zur Daten- und IT-Sicherheit und zu zahlreichen anderen Themen an. Es wird empfohlen, diese Kurse bei Bedarf zu besuchen.

3. Der ZID kündigt betriebliche Änderungen und Unterbrechungen auf der Mailingliste betrieb@lists.uibk.ac.at an. Es wird allen Mitarbeiterinnen und Mitarbeitern empfohlen, diese Mailingliste zu abonnieren.

3. Wie sichere ich meinen IT-Arbeitsplatz?

1. Räume mit IT-Systemen und Arbeitsplätze, an denen personenbezogene Daten verarbeitet werden, sind so zu sichern, dass Unbefugte keinen Einblick in oder Zugriff auf die Daten erlangen können.

2. In Bereichen mit Publikumsverkehr sind Monitore, Drucker und Faxgeräte so aufzustellen, dass das Risiko der Einsichtnahme Dritter möglichst ausgeschlossen wird.

3. Bereiche, in denen hoch vertrauliche und sensible Informationen verarbeitet werden, sind besonders zu sichern. Nur berechtigte, namentlich bekannte Personen haben Zugang zu diesen Bereichen.

4. Der Arbeitsplatz ist „aufgeräumt“ zu hinterlassen, sodass Unbefugten kein Zugriff auf Daten und IT-Anwendungen ermöglicht wird.

5. Räume mit IT-Systemen sind beim Verlassen grundsätzlich zu verschließen. Räume mit mehr als einem Arbeitsplatz sind von der letzten Person zu verschließen, die den Raum verlässt.

6. IT-Endgeräte sind bei Dienstschluss nach vorschriftsmäßiger Programmbeendigung abzuschalten. Bei kurzfristiger Abwesenheit ist das Gerät mit einem passwortgeschützten Bildschirmschoner zu sperren, der beim Verlassen des Arbeitsplatzes oder automatisch aktiv wird.

7. Ausdrucke mit vertraulichen Informationen sind umgehend aus dem Drucker zu entfernen.

8. Nicht mehr benötigte schriftliche Unterlagen sind so zu vernichten, dass ihr Inhalt nicht mehr erkennbar ist (zum Beispiel durch Einsatz eines Aktenvernichters).

9. Bei von mehreren Personen verwendeten EDV-Arbeitsplätzen ist sicherzustellen, dass personenbezogene oder vertrauliche Daten anderen Benutzern nicht zugänglich gemacht werden (zum Beispiel durch Setzen von Zugriffsrechten oder automatisiertes Löschen temporärer Dateien).

4. Was muss ich bei der Verarbeitung von Daten allgemein beachten?

1. Es ist sicherzustellen, dass Daten unversehrt, vollständig, aktuell und zeitgerecht zur Verfügung stehen.

2. Alle Daten sind so aufzubewahren, dass sie problemlos wiedergefunden werden können. Insbesondere sind geeignete Dateinamen und Verzeichnis- oder Ordnerstrukturen zu wählen.

3. Personenbezogene und vertrauliche Daten sind grundsätzlich auf zentralen, vom Zentralen Informatikdienst (ZID) betreuten Systemen zu verarbeiten. Ist dies nicht möglich, hat die verarbeitende Stelle eine zumindest gleichwertige Qualität der Datensicherheit und -verfügbarkeit sicherzustellen.

4. Auf zentralen, vom ZID betreuten Systemen wird eine automatische Datensicherung tagesaktuell durchgeführt. Existieren besondere Anforderungen an die Datensicherung, ist dies mit dem ZID zu vereinbaren.

5. Werden Daten auf nicht vom ZID betreuten Systemen gespeichert, hat die datenverarbeitende Organisationseinheit die Datensicherung sicherzustellen. Die Sicherung hat dabei bevorzugt am zentralen Datensicherungssystem des ZID zu erfolgen.

5. Wie sichere ich Datenträger?

1. Personenbezogene Daten dürfen nur auf den dafür vorgesehenen Systemen verarbeitet werden. Jede Übertragung von Daten der Kategorien B, C und D iSd „Rahmenbetriebsvereinbarung zur automatisationsunterstützten Verwendung personenbezogener Daten“ auf andere Datenträger ist grundsätzlich untersagt.

2. Datenträger mit personenbezogenen oder vertraulichen Daten dürfen nur in Abstimmung mit der oder dem Vorgesetzten aus dem Dienstbetrieb entfernt werden (z.B. für häusliche Arbeiten oder sonstige dienstliche Zwecke außer Haus).
   In diesem Fall sind die Daten möglichst durch Verschlüsselung zu schützen.

3. Mobile Datenträger (z.B. CD-ROM, Memory Sticks oder mobile Festplatten) mit personenbezogenen oder vertraulichen Daten sind eindeutig zu kennzeichnen.

4. Mobile Datenträger sind so zu verwahren, dass sie vor einem Zugriff Unberechtigter geschützt sind.

5. Datenträger mit personenbezogenen oder vertraulichen Daten, die nicht mehr benötigt werden, sind vor der Entsorgung so zu löschen, dass die Daten keinesfalls mehr zu-

gänglich sind. Falls dies nicht möglich ist, sind die Datenträger in geeigneter Weise unbrauchbar zu machen.

6. Die Aufbewahrungsfristen gespeicherter Daten und Datenträger richten sich nach den für die einzelnen Bereiche vorgeschriebenen gesetzlichen Aufbewahrungspflichten.

6. Darf ich Daten weitergeben?

1. Allen Mitarbeiterinnen und Mitarbeitern ist es untersagt, schutzwürdige Daten unbefugt zu einem anderen als dem zur jeweiligen rechtskonformen Auftragserfüllung gehörenden Zweck zu verarbeiten, bekannt zu geben, zugänglich zu machen oder sonst zu nutzen.

2. Um Missbrauch bei der Verarbeitung von schutzwürdigen Daten zu verhindern, sind alle Mitarbeiterinnen und Mitarbeiter, die Zugang zu solchen Daten haben, zur Verschwiegenheit über diese Daten verpflichtet. Dies gilt auch für Informationen, mit denen man sich Zugang zu schutzwürdigen Daten verschaffen kann. Im besonderen Maße gilt dies für Passwörter.

3. Die Weitergabe von personenbezogenen Daten zu anderen Zwecken als denen, für die sie erhoben wurden, ist nur dann erlaubt, wenn eine Rechtsvorschrift oder die Wahrnehmung einer durch Gesetz oder Rechtsvorschrift zugewiesene Aufgabe die Verarbeitung dieser Daten gestattet oder die oder der Betroffene schriftlich eingewilligt hat.

4. Auskunftsersuchen von Behörden oder sonstigen öffentlichen Stellen sind nur aufgrund gesetzlicher Regelungen möglich. In Zweifelsfällen ist vor Erteilung der Auskunft die oder der Datenschutzbeauftragte zu befragen.

5. Die Auskünfte werden grundsätzlich schriftlich erteilt, wobei die oder der Betroffene entsprechend zu informieren ist. Telefonische Auskünfte dürfen nicht gegeben werden.

6. Ist ausnahmsweise aufgrund dringender Notwendigkeit eine elektronische Form der Datenübermittlung erforderlich (z.B. per E-Mail), sind die Daten in geeigneter Form vor unberechtigtem Zugriff zu schützen.

7. Personenbezogene oder vertrauliche Daten dürfen nur dann übermittelt werden, wenn die Vertraulichkeit bei der Übermittlung gewährleistet ist (Wahl geeigneter Versandsmethoden, sicherer Protokolle und Verschlüsselung).

8. Es sind keine vertraulichen Inhalte auf Anrufbeantworter zu sprechen.

9. Beim Faxversand schutzbedürftiger Dokumente ist mit der Gegenseite ein Sendezeitpunkt zu vereinbaren.

7. Wie gehe ich mit Benutzerkennung und Passwörtern um?

1. Alle Zugangsdaten, Passwörter und sonstige Authentisierungs(hilfs)mittel sind vertraulich zu halten und nicht weiterzugeben. Auch eine Weitergabe an Vorgesetzte, System- und Netzwerkadministratorinnen und -administratoren oder anderes IT-Personal ist nicht zulässig.

2. Es ist untersagt, die Zugangsdaten anderer Personen zu verwenden.

3. Passwörter dürfen nicht unverschlüsselt in Dateien abgelegt werden.

4. Sämtliche schriftlichen Unterlagen, aus denen Rückschlüsse auf Zugangsmöglichkeiten zum System gezogen werden können, sind sorgfältig und für Unbefugte unzugänglich aufzubewahren.

5. Wenn der Verdacht besteht, dass die eigenen Zugangs- und Zugriffsberechtigungen unberechtigt von Dritten genutzt werden, ist das Passwort umgehend zu ändern und die oder der IT-Sicherheitsbeauftragte des ZID zu verständigen.

6. Es sind die Zugangsregelungen und die vergebenen Berechtigungen zu beachten. Das Ausprobieren, ob weitere Dienste oder Zugriffsrechte als die erlaubten genutzt werden können, ist untersagt.

7. Passwörter dürfen nicht leicht zu erraten sein. Es dürfen keine Trivialpasswörter verwendet werden (z.B. 4711, 12345 oder andere naheliegende Tastenkombinationen). Vor- und Familiennamen oder Geburtstage sind beispielsweise zur Bildung von Passwörtern nicht geeignet.

8. Sofern Gruppenpasswörter zwingend erforderlich sind, sind diese jedenfalls zu ändern, wenn sich die Zusammensetzung der Gruppe ändert.

8. Wie gehe ich bei Tele- und Heimarbeit mit Daten um?

1. Eine Verarbeitung personenbezogener oder vertraulicher Daten ist nur in Absprache mit der oder dem Vorgesetzten zulässig.

2. Werden mobile Systeme (z.B. Laptops) oder IT-Systeme außerhalb der Universität für die Verarbeitung personenbezogener oder vertraulicher Daten verwendet, müssen sie zumindest den oben beschriebenen Standards für IT-Systeme genügen.

3. Überdies sind die vorhandenen Schutzmöglichkeiten des Systems (BIOS Passwort etc.) zu nutzen, um den Zugriff nicht autorisierter Personen zu verhindern.

B Administratorinnen und Administratoren

9. Wie ist der Zugriff auf Systeme zu regeln?

1. Es ist sicherzustellen, dass nur befugte Personen Zugang zu personenbezogenen und vertraulichen Daten haben. Dafür sind geeignete Identifikations- und Authentisierungsmethoden einzusetzen (z.B. Benutzerkennung und Passwort).

2. Berechtigungen für den Zugriff auf Daten sind nur in dem Umfang zu erteilen, wie dies für die Aufgabenerfüllung notwendig ist. Diese Rechte sind nach Möglichkeit schriftlich zu dokumentieren.

3. Es sind klare Vereinbarungen bezüglich des Zweckes, der Art und des Umfanges der Datenverarbeitung zu treffen und zu dokumentieren.

4. Bei Systemen und Anwendungen, die für den Betrieb der Universität Innsbruck oder eine ihrer Organisationseinheiten von geschäftswichtiger Bedeutung sind, muss im Vertretungsfall weiterhin ein administrativer Zugang möglich sein.

10. Wie sind IT-Systeme zu betreiben und zu warten?

1. Bei der Soft- und Hardwarebeschaffung sind neben fachlichen und technischen Maßnahmen sowie ergonomischen Aspekten auch Anforderungen an die IT-Sicherheit und an den Datenschutz zu berücksichtigen.

2. PC-Arbeitsplätze sind nach Möglichkeit standardisiert auszustatten, um die Verwaltung und Administration zu erleichtern.

3. Neue Soft- und Hardware ist vor dem Einsatz zu testen. Dabei sind nach Möglichkeit Test- und Produktivsystem zu trennen.

4. Es sind geeignete Vorkehrungen zu treffen, um den Zugriff anderer Systeme auf das erforderliche Maß zu reduzieren (z.B. Firewalls).

5. Alle IT-Systeme sind grundsätzlich mit einem Virenschutzprogramm zu versehen. Für dieses sind regelmäßig Updates durchzuführen und die Viren-Signaturen zu aktualisieren.

6. Alle verfügbaren Sicherheitsupdates sind zeitgerecht, regelmäßig und nach Möglichkeit automatisiert zu installieren. Dies gilt nicht nur für das Betriebssystem selbst, sondern für alle auf dem Rechner installierten Programme.

7. Alle IT-Systeme, auf denen personenbezogene oder vertrauliche Daten verarbeitet werden, sind so zu konfigurieren, dass ein Zugriff nur nach Authentifizierung möglich ist.

8. Die Regelungen für Zugangsdaten und Passwörter gelten besonders auch für administrative Zugänge, da diese meist Zugriff auf alle Daten auf einem IT-System haben.

9. IT-Systeme sind nach dem Prinzip der geringsten notwendigen Berechtigungen zu verwenden. Insbesondere sind nur dann Benutzerkennungen mit administrativen Berechtigungen zu verwenden, wenn dies erforderlich ist. Dies ist nach Möglichkeit auf einzelne Aktionen einzuschränken.

10. Um Sicherheitslücken zu schließen und Sicherheitsprobleme zu vermeiden, haben sich Administratorinnen und Administratoren laufend über aktuelle Vorfälle und Entwicklungen zu informieren.

11. Es ist eine regelmäßige Kontrolle der Funktionalität der IT-Systeme und Anwendungen durchzuführen.

C Protokollierung und Dokumentation

1. Es ist im Rahmen der technischen Möglichkeiten zu protokollieren, wer zu welchem Zeitpunkt welche Daten verarbeitet oder übermittelt hat. Wenn möglich hat die Protokollierung automatisch zu erfolgen.

2. Zur Sicherstellung der Datensicherheit und der Erfüllung der Grundanforderungen des Datenschutzes sind alle relevanten Systemereignisse einschließlich der Benutzerauthentifizierung zu protokollieren.

3. Alle Änderungen an Anwendungen und Systemen, mit denen personenbezogene und vertrauliche Daten verarbeitet werden, sind revisionssicher zu dokumentieren.

4. Die Auswertung von Protokollen ist grundsätzlich nicht zulässig und unterliegt den Regelungen der „Rahmenbetriebsvereinbarung zur automatisationsunterstützten Verwendung personenbezogener Daten“.

5. Die Anwendungen zur Verarbeitung personenbezogener und vertraulicher Daten sind vollständig, aktuell und nachvollziehbar zu dokumentieren. Alle Systemeinstellungen und Sicherheitsmaßnahmen sind so zu dokumentieren, dass sie für die Vertreterin oder den Vertreter und andere fachkundige Dritte verständlich sind.