



TECHNISCHE
UNIVERSITÄT
DRESDEN

Zentrum für Informationsdienste und Hochleistungsrechnen

Monitoring und Datenschutz

Ralph Müller-Pfefferkorn

Dresden, 27.Mai 2008

Bundesrepublik Deutschland

- Grundrecht auf informationelle Selbstbestimmung:
Der Betroffene kann grundsätzlich selbst darüber entscheiden, wem er welche persönlichen Informationen bekannt gibt.
- Gesetzliche Regelungen
 - ▶ steht nicht im Grundgesetz
 - ▶ Bundesdatenschutzgesetz regelt Belange für Bundesbehörden und Privatbereich (inkl. Wirtschaft)
 - ▶ Landesgesetze für öffentliche Landeseinrichtungen wie Universitäten
- Datenschutz bezieht sich auf die Erhebung, die Verarbeitung und die Nutzung personenbezogener Daten
- Im folgenden Erläuterung einiger grundlegender Prinzipien

Datensparsamkeit und Datenvermeidung

- möglichst keine oder so wenig personenbezogene Daten wie möglich erheben, verarbeiten oder nutzen
- nur so viele personenbezogene Daten sammeln, wie für den jeweilige Zweck unbedingt notwendig sind
- von Anonymisierung und Pseudonymisierung Gebrauch machen

Erforderlichkeit

- Was ist erforderlich, um den Zweck zu erreichen?
- Personenbezug eher vermeiden
- Nach Erreichen des Zwecks personenbezogene Daten in angemessenem Zeitraum löschen oder anonymisieren
- Anonymisierung darf nicht auf Person rückführbar sein
 - ▶ nicht einfach nur Namen entfernen
 - ▶ z.B.
 - durch Vergrößerung oder Entfernen von Zeitmarken
 - genügend große Personenzahl im Zeitraum
 - ▶ Gegenbeispiel: wenn nur ein Nutzer zu einer Zeit auf einer Ressource rechnet

Zweckbindung

- Einsatz der personenbezogenen Daten nur für den angegebenen Zweck
- Zweck muss vorher bekannt gegeben werden
- Zweck darf nicht einfach im Nachhinein neu definiert werden
- nicht erlaubt: "Daten auf Vorrat zu unbestimmten Zwecken"

Information der Nutzer

- Nutzer muss über Sammlung der Daten informiert werden
- genaue Angabe welche Daten erfasst werden
- genaue Angabe, zu welchem Zweck die Daten gesammelt werden
- Option zur Abwahl des Dienstes
 - ▶ kein Zwang zur Nutzung
- Recht des Nutzers auf Auskunft über die zu seiner Person gespeicherten Daten
 - ▶ Art, Umfang, Zweck

Datensicherheit

- Beschränkung des Zugriffs auf die Daten
- Einsicht in die personenbezogenen Daten darf nur nehmen:
 - ▶ die betroffene Person
 - ▶ wer die Daten für seine Aufgaben benötigt
 - aber NUR für diese Aufgabe und wie im Zweck definiert
- Zugriffsberechtigte können auf Datenschutz verpflichtet werden
 - ▶ z.B. Administratoren, die Zugang zu sensiblen Daten haben

Vorschlag des Datenschutzbeauftragten

- Aufnahme von Datenschutzbestimmungen in eine Ordnung / einen Vertrag, den der Nutzer akzeptieren / unterzeichnen muss
- z.B. in D-Grid oder VO User Policy
- Vorschlag eines Vertrages auf den folgenden Seiten

Ordnung zum Betrieb des ...

1. Zweck des Monitoring

Die Erhebung von Daten im Rahmen des Monitoring erfolgt

- ▶ zu Abrechnungszwecken,
- ▶ zur Information der Nutzer über ihre verbrauchte Rechenzeit,
- ▶ zur Gewährleistung eines ordnungsgemäßen Betriebs des D-Grid,
- ▶ für Zwecke der Systemadministration,
- ▶ zur Erkennung und Beseitigung von Störungen und Engpässen,
- ▶ zum Erkennen missbräuchlicher Nutzungen (z. B. DoS),
- ▶ zur Ressourcenplanung ...

Die Verwendung der gewonnenen Informationen zur Verhaltens- oder Leistungskontrolle der Nutzer ist unzulässig und findet nicht statt.

2. Überwachte Bereiche

Überwacht werden ... (Worker Nodes, Speicherressourcen ...)

3. Verantwortlichkeiten / Ansprechpartner

Namen oder Strukturen (Projektleiter, VO-Manager ...)

Kontaktperson im Falle von Problemen, Nachfragen

4. Erhobene Daten

Genaue Beschreibung

5. Zugriffsrechte

Wer darf die Daten sehen?

Müssen keine Namen sein, Strukturen (z.B. Administratoren, VO-Management ...)

6. Festlegungen zur allgemeinen Datensicherheit

Wie werden diese Daten vor unberechtigtem Zugriff und Verwendung geschützt ?

7. Löschfristen

Wann werden die Daten gelöscht ? KURZE FRISTEN ! (z.B. 3 Monate)

Einwilligung

Ich stimme den Regelungen und der damit evtl. verbundenen Verarbeitung personenbezogener Daten zu. Mir ist bekannt, dass ich diese Einwilligung jederzeit widerrufen kann.

Gültigkeit des Datenschutzes

- Datenschutz gilt für personenbezogene (d.h. auf eine Person zurückführbare) Daten
- Anonymisierte und nicht mehr rückführbare Daten dürfen veröffentlicht werden
- Nicht personenbezogene Daten dürfen vom Datenschutzgesichtspunkt aus veröffentlicht werden (sofern nicht politische Gründe dagegen sprechen)
- Vorherige klare Vereinbarung erspart Ärger hinterher!