Universität Zürich[UZH]

Recht und Datenschutz

Universität Zürich
Fachbereich Datenschutzrecht
Hirschengraben 56
CH-8001 Zürich

privacy@rud.uzh.ch
www.rud.uzh.ch

Version Januar 2020

Merkblatt – Datenschutzrechtliche Grundsätze

1. Gesetzmässigkeit und der Verhältnismässigkeit (§ 8 IDG)

Die UZH darf nur diejenigen Personendaten bearbeiten, die zur Erfüllung der ihr gesetzlich übertragenen Aufgaben geeignet und erforderlich sind. Zweck und Auftrag der UZH ergeben sich im Allgemeinen aus § 2 Universitätsgesetz (UniG vom 15. März 1998):

- Leistung von wissenschaftlicher Arbeit und Erbringung von Dienstleistungen in Forschung und Lehre im Interesse der Allgemeinheit;
- Vermittlung wissenschaftlicher Bildung und damit zusammenhängender Schaffung von Grundlagen zur Ausübung von akademischen Tätigkeiten und Berufen;
- Pflege der akademischen Weiterbildung und Förderung des wissenschaftlichen Nachwuchses.

Auf einer Einwilligung sollte eine Datenbearbeitung innerhalb der UZH nur ausnahmsweise basieren (z. B. wenn unklar ist, ob eine Datenbearbeitung geeignet und erforderlich ist).

2. Datenvermeidung und Datensparsamkeit (§ 11 IDG)

Datenbearbeitungssysteme und -programme müssen so gestaltet sein, dass

- keine Personendaten anfallen, die zur Aufgabenerfüllung nicht notwendig sind (§ 11 Abs. 1 IDG);
- Personendaten sobald und soweit möglich, gelöscht, anonymisiert oder teilanonymisiert werden (§ 11 Abs. 2 IDG) und
- soweit eine Anonymisierung oder Teilanonymisierung nicht möglich ist, sobald und soweit möglich Personendaten pseudonymisiert werden.

3. Transparenz bzw. Erkennbarkeit (§ 12 IDG)

Die Beschaffung von Personendaten an sich sowie auch der Zweck ihrer Bearbeitung müssen für die betroffenen Personen aus den Umständen erkennbar sein. Andernfalls müssen sie entsprechend informiert werden. Ein Verstoss gegen diesen Grundsatz sowie gegen den Grundsatz der Gesetzmässigkeit liegt beispielsweise im Rahmen von unerlaubten verdeckten Datenbeschaffungen durch Programmmanipulationen oder unerlaubten Telefonüberwachungen vor.

Bei der Beschaffung von besonderen Personendaten (für eine Definition siehe unser Glossar) ist der Inhaber der Datensammlung grundsätzlich verpflichtet, die betroffene Person über den Zweck der Bearbeitung zu informieren.

Aus dem Grundsatz der Transparenz folgt auch, dass eine betroffene Person benachrichtigt werden sollte, soweit deren Personendaten unrechtmässig bekanntgegeben, verändert, oder vernichtet worden sind und der betroffenen Person dadurch eine Beeinträchtigung ihrer Rechte oder schutzwürdigen Interessen droht (d. h. materieller oder immaterieller Schaden, wie beispielsweise wirtschaftliche Nachteile oder Reputationsschaden). Dabei ist es ausreichend, wenn anhand von tatsächlichen Anhaltspunkten mit einer gewissen Wahrscheinlichkeit davon ausgegangen werden kann, dass Dritte von den

Personendaten Kenntnis erlangt haben (z. B. wenn Laptops oder andere Datenträger an Orten verlorengehen, wo sie Dritten zugänglich sind, oder wenn Daten gestohlen oder illegal aus IT-Systemen abgerufen werden und die Daten respektive die Datenträger nicht verschlüsselt waren).

In solchen Fällen muss die Benachrichtigung der betroffenen Person eine Auskunft darüber beinhalten

- wann, welche Daten bekanntgegeben, verändert oder vernichtet worden sind, und
- wann dies festgestellt worden ist, und
- welche Sofortmassnahmen eingeleitet worden sind, um beispielsweise die Ursache eines Datenlecks zu beheben, und
- welche Vorsorge- oder Schadensabwehrmassnahmen zur Minderung weiterer nachteiliger Folgen empfohlen werden, wie beispielsweise die Änderung von Passwörtern.

Soweit und solange Ermittlungen der Strafverfolgungsbehörden gefährdet werden, muss die Benachrichtigung der betroffenen Person unterbleiben.

4. Zweckbindung (§ 9 Abs. 1 IDG)

Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde oder der aus den Umständen ersichtlich oder gesetzlich vorgesehen ist. (beispielsweise dürfen Stammdaten der Mitarbeiter, die für die Anstellung erhoben wurden, nicht zu kommerziellen Zwecken weiterverwendet werden).

Personendaten müssen gelöscht respektive vernichtet oder anonymisiert werden, wenn:

- die Daten nicht mehr für die ursprünglich erhobenen Zwecke benötigt werden, und
- die gesetzlichen Aufbewahrungsfristen, die für die Akten gelten, abgelaufen sind, und
- die Daten nicht (mehr) als Beweismittel im Rahmen eines rechtlichen respektive gerichtlichen Verfahrens benötigt werden, und
- das zuständige (End-)Archiv, dem die Daten nach Ablauf der Aufbewahrungsfrist angeboten worden sind, die Daten nicht übernommen und archiviert hat.

Für einen anderweitigen Zweck dürfen die Daten nur dann bekanntgegeben werden, wenn eine rechtliche Bestimmung eine anderweitige Zweckverwendung vorsieht oder im Einzelfall eine Einwilligung der betroffenen Person vorliegt.

5. Daten- bzw. Informationssicherheit (§ 7 IDG)

Die zu treffenden organisatorischen und technischen Massnahmen haben sich an den folgenden Schutzzielen zu orientieren:

- Informationen dürfen nicht unrechtmässig zur Kenntnis gelangen, d. h. müssen vertraulich bleiben und vor zufälligen oder unrechtmässigen Zugriffen, Veränderungen oder Bekanntgaben geschützt werden; daraus folgt auch, dass ein Zugriff auf Personendaten ausschliesslich nach dem Grundsatz der Erforderlichkeit («need to know») denjenigen Personen erteilt werden darf, die aufgrund ihrer Funktion und Aufgabe auf die Personendaten zugreifen müssen.
- Informationen müssen richtig und vollständig sein; daraus folgt, dass falsche oder unvollständige Personendaten gelöscht, berichtigt oder aktualisiert werden müssen.

- Informationen müssen bei Bedarf vorhanden sein, d. h. vor Verlusten sowie Zerstörung geschützt werden.
- Informationsbearbeitungen müssen einer Person zugerechnet werden können.
- Veränderungen von Informationen müssen erkennbar und nachvollziehbar sein.
- Die zu treffenden Massnahmen richten sich nach der Art der Information, nach Art und Zweck der Verwendung und nach dem jeweiligen Stand der Technik.

6. Datenbearbeitung im Auftrag (§ 6 IDG)

Das Bearbeiten von Informationen kann Dritten übertragen werden, sofern keine rechtliche Bestimmung oder vertragliche Vereinbarung entgegensteht.

Die Aufträge müssen schriftlich und unter Einbezug der einschlägigen AGB (sogenannte UZH-Paketlösung) ergehen.

Es muss kontrolliert werden, dass die Anforderungen aus den Verträgen erfüllt werden und, falls nötig, Korrekturen eingeleitet werden.

7. Grenzüberschreitende Bekanntgabe von Personendaten (§ 19 IDG)

Personendaten dürfen an Empfängerinnen und Empfänger, die dem Europarats-Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten nicht unterstehen, bekannt gegeben werden, wenn:

- der Empfängerstaat ein angemessenes Datenschutzniveau gewährleistet (siehe Staatenliste des EDÖB), oder
- eine gesetzliche Grundlage dies erlaubt, um bestimmte Interessen der betroffenen Person oder überwiegende öffentliche Interessen zu schützen, oder
- vom öffentlichen Organ angemessene vertragliche Sicherheitsvorkehrungen getroffen wurden.

8. Gewährleistung von Betroffenenrechten und des Informationszugangs (§§ 20, 21, 22, 28 IDG)

Betroffene Personen können von der UZH verlangen (§§ 21, 22 IDG), dass:

- unrichtige Personendaten berichtigt oder vernichtet werden,
- das widerrechtliche Bearbeiten von Personendaten unterlassen wird,
- die Folgen des widerrechtlichen Bearbeitens beseitigt werden,
- die Widerrechtlichkeit des Bearbeitens festgestellt wird,
- die Bekanntgabe von Personendaten an Private gesperrt wird, wenn das öffentliche Organ aufgrund einer spezialgesetzlichen Bestimmung Personendaten voraussetzungslos bekannt geben kann.

Folgendes muss die UZH grundsätzlich innert 30 Tagen behandeln und beantworten:

- Gesuch um Zugang zu Informationen im Sinne des Öffentlichkeitsprinzips (§ 20 Abs. 1 IDG) und
- Gesuch um Zugang zu den bei der UZH vorhandenen eigenen Personendaten (§ 20 Abs. 2 IDG).