Recht und Datenschutz

Universität Zürich
Fachbereich Datenschutzrecht
Künstlergasse 15
CH-8001 Zürich

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

Datenschutz @ UZH

Merkblatt
Datenschutzvorfälle / Data Breach Notification

1. Was ist ein Datenschutzvorfall?

Für die Datenbearbeitung verantwortliche Organe müssen mit technischen und organisatorischen Massnahmen die Einhaltung des Datenschutzes sicherstellen. Diese Massnahmen müssen insbesondere dem Stand der Technik, der Art und dem Umfang der Datenbearbeitung sowie den Risiken, welche die Bearbeitung für die Rechte der betroffenen Personen mit sich bringt, angemessen sein (§ 7 IDG). Eine der zentralen Komponenten der Datensicherheit ist neben der Fähigkeit, Datenschutzvorfälle soweit möglich zu verhindern, diese möglichst frühzeitig zu erkennen und zügig darauf zu reagieren.

Um einen Datenschutzvorfall (data breach / Datenschutzverletzung / unbefugte Datenbearbeitung) handelt es sich, wenn *personenbezogene* Daten

- unwiederbringlich *vernichtet* werden oder *verloren* gehen;
- unbeabsichtigt oder unrechtmässig *verändert* oder *offenbart* werden;
- Unbefugten *zugänglich* werden.

Öffentliche Organe wie die UZH sind gesetzlich verpflichtet, gewisse Datenschutzvorfälle an die kantonale Datenschutzbeauftragte zu melden (§ 12a IDG).

2. Was sind personenbezogene Daten?

Personenbezogene Daten sind Informationen, die sich auf eine bestimmte oder bestimmbare Person beziehen:

- Eine Person ist *bestimmt*, wenn sich ihre Identität unmittelbar aus den Daten selbst ergibt (i.d.R. Name, Gesichtsfoto).
- Eine Person ist *bestimmbar*, wenn sich ihre Identität aus dem Kontext der Daten durch Kombination mit anderen Daten/Verzeichnissen ergibt, solange dies ohne unverhältnismässigen Aufwand möglich ist (etwa Matrikelnummer, AHV-Nummer, IP-Adresse, Kontonummer, Kundennummer, Autokennzeichen).

  Der Aufwand ist unverhältnismässig, wenn nach der allgemeinen Lebenserfahrung nicht damit gerechnet werden muss, dass ein Interessent diesen auf sich nimmt. Ein allfälliges spezifisches Interesse, das der Interessent an der Identifizierung der Person hat, ist dabei mit zu berücksichtigen.

3. Was sind Beispiele eines Datenschutzvorfalls?

Beispiele, wie sich ein Datenschutzvorfall ereignen könnte (Liste nicht abschliessend):

- Verlust eines Datenträgers mit Personendaten (z.B. Forschungsdatensatz), insbesondere an einem öffentlich zugänglichen Ort;
- versehentliche Übermittlung von Personendaten an unberechtigte Dritte (z.B. aufgrund falscher E-Mail-Adresse);
- versehentliches Zugänglichmachen von Personendaten übers Internet (z.B. fehlender Passwortschutz);
- Eindringen eines Dritten in einen Netzwerkbereich, in dem Personendaten abrufbar bzw. gespeichert sind;

- Infizierung mit Spyware, Malware oder Ransomware (Viren, Trojaner etc.), wobei hinreichende Anhaltspunkte vorliegen müssen, dass Personendaten zerstört oder Dritten bekannt worden sind.

4. Wer ist für den Datenschutz bzw. Datenschutzvorfälle verantwortlich?

Innerhalb der UZH sind diejenigen Personen für Datenbearbeitungen und damit zusammenhängende Vorfälle verantwortlich, welche *Inhaber der Datensammlung* sind, d.h. welche *über Zweck und Inhalt* der Datenbearbeitungen *entscheiden* (Art. 3 lit. i DSG analog; üblicherweise wäre das bei Forschungsvorhaben der/die verantwortliche Professor*in, innerhalb der ZDU der/die Projektverantwortliche).

Die Verantwortung verbleibt auch dann bei der entsprechenden Person, falls Datenbearbeitungen an Dritte (Cloud-Service-Anbieter, Hosting-Provider, Marktforschungsunternehmen etc.) übertragen wurden (§ 6 Abs. 2 IDG). In solchen Fällen muss vertraglich nicht nur sichergestellt sein, dass der Dritte die übertragenen Informationen angesessen schützt, sondern auch die an der UZH für die Datenbearbeitung verantwortliche Person über allfällige Datenschutzvorfälle sofort informiert.

5. Was ist bei einem mutmasslichen Verdacht auf einen Datenschutzvorfall zu unternehmen?

- Involvieren Sie umgehend Ihre IT-Verantwortliche oder Ihren IT-Verantwortlichen und stellen Sie sicher, dass unmittelbar damit begonnen wird, die Umstände, die zum Datenschutzvorfall geführt haben, soweit als möglich zu beheben. Der IT-Verantwortliche kann weitere Stellen wie die IT-Sicherheitsstelle der Zentralen Informatik oder den Fachbereich Datenschutz beiziehen.
- Klären Sie zeitgleich mit der oder dem IT-Verantwortlichen ab, was für Daten betroffen sind.
- Treffen Sie eine Ersteinschätzung, ob es sich um personenbezogene Daten handelt und eruieren Sie die allfälligen Betroffenen.
- Falls personenbezogene Daten involviert oder Sie sich unsicher sind, informieren Sie umgehend den Fachbereich Datenschutzrecht.
- Der Fachbereich Datenschutzrecht prüft insbesondere, wie gravierend mögliche Folgen der Datenschutzverletzung für betroffene Personen sind und ob allfällige Sofortmassnahmen zur Behebung des Datenlecks zu ergreifen sind. Bei Bedarf informiert er die Universitätsleitung und veranlasst die gesetzlich vorgeschriebene Meldung an die kantonale Datenschutzbeauftragte oder andere zuständige Datenschutzaufsichtsbehörden, sofern ein meldepflichtiger Sachverhalt vorliegt.
- Die zuständige Aufsichtsbehörde kann weitere Massnahmen anordnen.

6. Müssen auch allfällige betroffene Personen informiert werden?

Die betroffenen Personen müssen dann benachrichtigt werden, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten von Personen zur Folge hat. Diese Beurteilung hängt vom Einzelfall ab und wird in Absprache mit dem Fachbereich Datenschutzrecht sowie ggf. der kantonalen Datenschutzbeauftragten eruiert.

7. Was ist zur Verhinderung von Datenschutzvorfällen zu unternehmen?

Bitte beachten Sie die Richtlinien und Sicherheitsregeln zur IT-Sicherheit auf der Webseite der Zentralen Informatik. Sie finden dort einschlägige Vorschriften, Weisungen und Merkblätter.

Die Juristinnen und Juristen des Fachbereichs Datenschutzrecht stehen bei Fragen gerne zur Verfügung (privacy@rud.uzh.ch).