Universität Zürich[UZH]

Recht und Datenschutz

Universität Zürich
Fachbereich Datenschutzrecht
Künstlergasse 15
CH-8001 Zürich

www.rud.uzh.ch

Datenschutz @ UZH

Merkblatt
Datenschutz und korrekter Umgang mit Personendaten von Mitarbeiter*innen der UZH (Personaldaten)

1. An wen richtet sich dieses Merkblatt?

Dieses Merkblatt richtet sich an alle Mitarbeiter*innen der Abteilungen Personal (nachfolgend PA) und Professuren, welche Personendaten von Mitarbeiter*innen bearbeiten. Zudem gilt es auch für Vorgesetzte und für Personalverantwortliche der Abteilungen, Institute und weiteren Organisationseinheiten. Alle Mitarbeiter*innen, die Personaldaten bearbeiten, haben damit sorgfältig umzugehen und insbesondere im Verkehr mit Drittpersonen das Amtsgeheimnis zu beachten.

2. Was sind Personendaten, besondere Personendaten und Personaldaten?

In diesem Merkblatt werden folgende Begriffe verwendet:

- **Personendaten**:
  Personendaten sind sämtliche Angaben und Informationen, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen[1]. Sie werden auch als **normale oder gewöhnliche Personendaten** bezeichnet.
  Beispiele im HR-Kontext: Name, Wohnadresse, AHV-Nr., Personal-Nr., Bankverbindung, Lohneinreihung, Bewerbungsunterlagen, Mitarbeiterinnenbeurteilung.

- **Besondere Personendaten:**
  Besondere Personendaten sind Informationen, bei denen wegen ihrer Bedeutung, der Art ihrer Bearbeitung oder der Möglichkeit ihrer Verknüpfung mit anderen Informationen die besondere Gefahr einer Persönlichkeitsverletzung besteht, wie Informationen über: religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, die Gesundheit, Intimsphäre, ethnische Herkunft, genetische und biometrische Daten, Massnahmen der sozialen Hilfe, administrative oder strafrechtliche Verfolgungen oder Sanktionen, automatisierte Auswertungen (Profiling)[2]. Auf Bundesebene werden sie als **besonders schützenswerte Personendaten**[3] bezeichnet.
  Beispiele im HR-Kontext: Arztzeugnisse, vertrauensärztliche Gutachten, Schlussbericht einer Administrativuntersuchung.

- **Personaldaten:**
  Personaldaten sind sämtliche normalen und besonderen Personendaten von Mitarbeiter*innen, die während eines Anstellungsverhältnisses (von der Bewerbung bis zum Austritt) bei der Arbeitgeberin anfallen.

- **HR-Community:**
  Zur HR-Community an der UZH gehören alle Mitarbeiter*innen der Abteilungen Personal und Professuren sowie die Personalverantwortlichen der Abteilungen, Institute und weiteren Organisationseinheiten.

---

[1] Vgl. § 3 Abs. 3 IDG
[2] Vgl. § 3 Abs. 4 IDG
[3] Vgl. Art. 5 lit. c DSG

3. Was bedeutet das «Need-to-know-Prinzip»?

Personenbezogene Daten müssen so bearbeitet werden, dass ihre Integrität und Vertraulichkeit (ein Grundsatz der Datenbearbeitung) hinreichend gewährleistet sind. Dazu gehört auch, dass Unbefugte keinen Zugang zu den Daten haben. Um den Grundsatz der Integrität und Vertraulichkeit gewährleisten zu können, sind technische und organisatorische Massnahmen (TOM) einzuführen. Eine solche Massnahme ist die Beschränkung des Zugriffs auf Personaldaten auf diejenigen Angestellten, die diesen Zugriff zur Wahrnehmung ihrer Aufgaben benötigen. Diese Vorgehensweise wird auch «Need-to-know-Prinzip» genannt.

Zugriffsbeschränkungen dürfen allerdings nicht dazu führen, dass die betriebliche Zusammenarbeit (abteilungsintern oder abteilungsübergreifend) behindert wird. Auch der informelle Austausch im Arbeitsalltag darf deswegen nicht verloren gehen: so sollen sich Personen der HR-Community über Personalgeschäfte oder konkrete Fragen mündlich austauschen können, um diese gemeinsam zu reflektieren und von der Erfahrung / dem Praxiswissen ihrer Kolleg*innen in ihrer eigenen Arbeit zu profitieren.

4. Was ist eigentlich Vertraulichkeit?

Vertraulichkeit ist ein Schutzziel der Informationssicherheit: Informationen dürfen ausschliesslich befugten Personen in der zulässigen Weise zugänglich sein. Dazu dienen insbesondere TOM: Definition und Vergabe restriktiver Berechtigungen mittels Berechtigungskonzept, ggf. Verschlüsselung oder Anonymisierung bei der Übermittlung. [4]

5. Was sind Rollen- und Berechtigungskonzepte?

Rollen- und Berechtigungskonzepte geben namentlich auf folgende Fragen eine Antwort:

- Wer darf zu welchem Zweck auf welche Daten zugreifen?
- Wer benötigt welche Daten für welche Aufgabenerfüllung?
- Wer trägt letztlich die Verantwortung für die Datenbearbeitungsvorgänge innerhalb der Abteilung?

M.a.W. sollen die Rollen- und Berechtigungskonzepte den Zugriff von Unberechtigten auf Daten verhindern.
Welche Person tatsächlich Zugriff auf die Daten erhält, wird am Need-to-know-Prinzip gemessen.

Die Abteilungen Personal und Professuren sind verantwortlich für die Erstellung von Rollen- und Berechtigungskonzepten für die Bearbeitung von Personaldaten in sämtlichen von in ihrem Verantwortungsbereich verwendeten EDV-Systemen (bspw. SAP HR, eHR, eDossier). Bei der Übergabe von Personaldaten aus diesen EDV-Systemen prüfen die Abteilungen Personal und Professuren, dass für die Zielsysteme entsprechende Nutzungs-, Rollen- und Berechtigungskonzepte vorhanden sind.

6. Müssen E-Mails mit Personaldaten verschlüsselt werden?

Die meisten Personaldaten gehören zur Kategorie der normalen Personendaten. Im UZH-internen Verkehr müssen diese nicht verschlüsselt werden (z.B. die Mitteilung einer Lohneinreihung an den Vorgesetzten oder die Zustellung einer Mitarbeiterinnenbeurteilung an die PA zur Ablage im Personaldossier).

Die Verschlüsselung von E-Mails sollte zurückhaltend eingesetzt werden und sich auf wirklich heikle Dokumente beschränken (bspw. Versand des Schlussberichts einer Administrativuntersuchung). Zu

[4] Vgl. § 7 Abs. 2 IDG / § 13 IVSV

beachten ist, dass verschlüsselte E-Mails bei der Ablage in einer Geschäftsdokumentation (bspw. in Axioma) nicht mehr (oder nur noch eingeschränkt) geöffnet werden können.

Bei heiklen Dokumenten (z.B. Administrativuntersuchungs-Schlussbericht, umfangreiche Lohnlisten) ist ggf. die Datei selbst (anstelle der E-Mail) zu verschlüsseln und das Passwort den Adressat*innen auf separatem Weg bekanntzugeben.

7. Für die HR-Community

Die Ausführungen in Ziffer 7 betreffen nur die HR-Community.

a. Wie ist mit Coachings des Fachbereichs Personal- und Führungsentwicklung (PE/FE) umzugehen?

Coachings des Fachbereichs Personal- und Führungsentwicklung (nachfolgend PE/FE) mit führungsverantwortlichen Vorgesetzten sowie mit weiteren Angestellten können heikle Informationen beinhalten. Die Gespräche zwischen Coach und Coachee sind vertraulich. Die zuständigen HR Business Partner (nachfolgend HRBP) sind über Beginn und Ende eines Coachings, nicht aber über den Inhalt der Gespräche, zu informieren. Im Abschlussdokument sind die Erkenntnisse zu den einzelnen Coaching-Themen sowie die Entwicklung gegenüber der Ausgangslage schriftlich festzuhalten.

Der Fachbereich PE/FE hat die Coachings fallbezogen in einem dafür geeigneten Geschäftsverwaltungssystem zu führen. Der Zugriff auf fallbezogene Akten ist auf die fallführenden Mitarbeiter*innen des Fachbereichs zu beschränken (Zugriffs- und Berechtigungskonzept).

Einzelne Dokumente eines Coachings sind zusätzlich im Personaldossier der gecoachten Person abzulegen. Es sind dies: Coaching-Vereinbarung und Abschlussdokument.

b. Coachings des Fachbereichs PE/FE im Auftrag oder in Abstimmung mit der Abteilung Professuren

Führt der Fachbereich PE/FE im Auftrag oder in Abstimmung mit der Abteilung Professuren Coachings mit Professor*innen durch, ist die Abteilung Professuren analog zu den HRBP über Beginn und Ende eines Coachings zu informieren, und es sind ihr Coaching-Vereinbarung sowie Abschlussdokument für die Ablage im Personaldossier der gecoachten Person zur Verfügung zu stellen.

c. Zusammenarbeit mit UZH-internen Beratungsstellen

In der Zusammenarbeit mit Beratungsstellen für Mitarbeiter*innen (insbesondere Abteilung Gleichstellung und Diversität, Kommission RSB) hat die PA bei Bedarf im Einzelfall zu beurteilen, ob und inwieweit diesen Beratungsstellen Auskünfte erteilt werden können. Dabei ist das Need-to-know-Prinzip zu beachten (siehe Ziffer 3, Frage: Braucht die Beratungsstelle die Informationen für die gehörige Wahrnehmung ihrer Aufgaben?).

d. Zusammenarbeit mit der Abteilung Recht und Datenschutz (RuD)

Die Fachbereiche Personalrecht und Datenschutz der Abteilung Recht und Datenschutz (nachfolgend RuD) unterstützen als Fachstellen die PA bei ihrer Aufgabenerfüllung. RuD wird insbesondere bei heiklen oder komplexen Personalgeschäften sowie Datenschutzfragen beigezogen. Die Rechtsvertretung der UZH in Rekurs- und Beschwerdeverfahren obliegt ausschliesslich der Abteilung RuD. Wird RuD in einen Personalfall involviert, werden RuD sämtliche Personaldaten (bspw. gesamtes Personaldossier) zur Verfügung gestellt (resp. Zugriff gewährt).

e. Wie ist mit Personaldossiers von Mitarbeiter*innen der PA umzugehen?

Während die Mitarbeiter*innen der HR Administration (HRA), der HR Beratung (HRBP), der Personal- und Führungsentwicklung (PE/FE) sowie der HR Leitung in der Regel auf alle bei der PA geführten Personaldossiers zugreifen können, legt die HR Leitung den Zugriff auf Personaldossiers von Mitarbeiter*innen der PA selbst möglichst restriktiv fest (bspw. auf die HR Leitung, die zuständige HRBP und einzelne Personen der HR Administration).

f. An wen kann ich mich bei Fragen zum Datenschutz wenden?

Der Fachbereich Datenschutz von RuD steht für Fragen gerne zur Verfügung, sei dies telefonisch oder schriftlich über das Anfrageformular von RuD (www.rud.uzh.ch / Menu: *«Anfragen an Recht und Datenschutz»*).