**Recht und Datenschutz**

Universität Zürich
Fachbereich Datenschutz
Hirschengraben 56
CH-8001 Zürich
privacy@rud.uzh.ch

www.rud.uzh.ch

Version August 2018

# Checkliste – Datenschutz im Büroalltag

Die nachstehende Checkliste gibt Ihnen grundlegende Hinweise darüber, wie Sie im Büroalltag mit Personendaten an der UZH umgehen müssen[1].

## 1. Datenschutzrechtliche Grundlagen

☐ Mir ist bewusst, dass die **Bearbeitung von Personendaten datenschutzrechtlichen Restriktionen unterliegt**, die sich für die UZH insbesondere aus dem **Gesetz über die Information und den Datenschutz** (IDG[2]) und der **Verordnung über die Information und den Datenschutz** (IDV[3]) ergeben.

☐ Ich weiss, dass **Datenschutz** den **Schutz** von Personen **vor dem Missbrauch ihrer Daten** und gleichzeitig das **Recht jeder Person** beinhaltet**, selbst darüber zu entscheiden, was mit den Daten über ihre Person geschieht**.

☐ Ich weiss, dass **Personendaten** sich auf eine **bestimmte oder auf eine nur bestimmbare natürliche oder juristische Person** beziehen.

- **Bestimmt** ist eine Person, wenn sich ihre Identität direkt aus der Information ergibt. Dies ist meist bei Informationen der Fall, bei welchen der Name, die Anschrift oder das Geburtsdatum des Betroffenen konkret mitgenannt sind oder ein Foto mitgeliefert wird, z. B. bei einem Personaldossier, einem Reisepass, einer Steuerakte oder einem Zeugnis.

- **Bestimmbar** ist eine Person, wenn ihre Identität durch die Kombination der Information mit anderen Informationen ohne einen unverhältnismässigen Aufwand feststellbar ist, z. B. bei einer Ausweisnummer, einer Matrikelnummer, einer Kontonummer, einer Versichertennummer, einer Telefonnummer, einer E-Mail-Adresse oder einer IP-Adresse. Zu diesen Angaben existieren Verzeichnisse, welche die Bestimmbarkeit ermöglichen.

☐ Ich weiss, dass unter eine **Datenbearbeitung** faktisch **jeder Umgang mit Personendaten** fällt, wie das Beschaffen, das Aufbewahren, das Verwenden, das Umarbeiten, das Bekanntgeben oder das Vernichten. Als Bekanntgabe ist jedes Zugänglichmachen wie das Einsichtgewähren, das Weitergeben oder das Veröffentlichen von Personendaten zu verstehen.

☐ Als Mitarbeitender der UZH **darf ich nur solche Personendaten bearbeiten, die für mein Aufgabengebiet erforderlich** sind.

☐ Mein **Wissen** zu datenschutzrechtlichen Grundlagen kann ich nach Bedarf **anhand** des **Lernprogramms des Datenschutzbeauftragten des Kantons Zürich[4] vertiefen**.

---

[1] Diese Checkliste basiert auf Materialien des Lernprogramms des Datenschutzbeauftragten des Kantons Zürich (https://review.datenschutz.ch/datenschutz/) sowie des Magazins für IT-Sicherheit „backUp Nr. 4“ des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (https://www.datenschutzzentrum.de/uploads/it/backup04.pdf).

[2] IDG: http://www.zhlex.zh.ch/Erlass.html?Open&Ordnr=170.4.

[3] IDV: http://www.zhlex.zh.ch/Erlass.html?Open&Ordnr=170.41.

[4] Lernprogramm des DSB ZH: https://review.datenschutz.ch/datenschutz/.

## 2. Mein Rechner und mein Arbeitsplatz

☐ Ich **erstelle mein Passwort entsprechend den mir von der IT vorgegebenen Kriterien**[5]. Ich **halte mein Passwort geheim und gebe es an keine andere Person weiter**, weder an einen Arbeitskollegen, noch an meinen Vorgesetzten und auch nicht an den IT-Betreuer oder den IT-Administrator.

☐ Ich **halte meine Daten, Unterlagen** (z. B. Korrespondenz oder Ausdrucke) **und Datenträger** (z. B. CDs, USB-Sticks, Speicherkarten oder externe Festplatten), welche Personendaten beinhalten, **unter Verschluss** (z. B. im Aktenschrank oder in der Schreibtischschublade), wenn ich nicht unmittelbar daran arbeite.

☐ Beim Verlassen meines Arbeitsplatzes während der Arbeitszeit **sperre ich den Bildschirm meines Rechners**. Nach Dienstschluss **melde ich meinen Computer mittels „Herunterfahrens" vom Netzwerk ab** und schalte den Bildschirm aus.

☐ Ich habe einen **passwortgeschützen Bildschirmschoner installiert, der sich nach Inaktivität automatisch** nach einer bestimmten Zeit **einschaltet**.

☐ Beim Verlassen meines Büros **schliesse ich die Tür ab**.

☐ Ich habe meinen **Badge sowie die Schlüssel** zu meinem Büro, zu meinem Aktenschrank und zu meiner Schreibtischschublade **sicher verwahrt**. Ich stelle sicher, dass der **Bildschirm meines Rechners so ausgerichtet ist, dass kein Unbefugter den Bildschirminhalt lesen** kann.

☐ Ich stelle sicher, dass sich meine **Besucher nur in meiner Anwesenheit in meinem Büro aufhalten** und sie **dort befindliche Personendaten** (z. B. in Unterlagen oder auf dem Bildschirm meines Rechners) **nicht unbefugt zur Kenntnis nehmen** können.

☐ Ich **drucke keine Personendaten über einen unbewachten Drucker** aus und **lasse keine Ausdrucke unnötig lange in einem Drucker liegen**.

## 3. Behandlung dienstlicher und privater Daten

☐ Ich bin mir bewusst, dass **alle Personendaten, die ich mittels der dienstlichen Infrastruktur respektive auf dienstlichen Geräten der UZH bearbeite, grundsätzlich als Daten der UZH und damit als dienstliche Daten gelten**.

☐ Ich bin mir bewusst, dass **Daten der UZH**:

- **grundsätzlich** dem **Amtsgeheimnis** und unter Umständen zusätzlich einem **Berufsgeheimnis** (z. B. für Ärzte, für Zahnärzte und für Psychologen) oder einem **Fabrikations- oder Geschäftsgeheimnis unterliegen**;
- **nur zu dienstlichen Zwecken bearbeitet** werden dürfen;

[5] Passwortkriterien: https://www.zi.uzh.ch/de/support/identitaet-zugang/manage-password.html.

- nur **auf solchen Geräten bearbeitet** und **gespeichert** werden dürfen, **die vor einem Zugriff Unbefugter geschützt** sind; dies gilt sowohl bei einem Zugriff mittels dienstlicher Geräte wie auch bei einem Zugriff mittels privater Geräte; dies ist auch zu beachten, soweit ich auf dienstliche E-Mails nicht per Webmail der UZH, IBM Notes oder IBM Verse[6] zugreife.
- **nicht über die Infrastruktur externer Anbieter** (z. B. Cloud-Dienste-Anbieter) **bearbeitet** oder **gespeichert** werden dürfen, **soweit nicht die datenschutzrechtlichen Vorgaben** der UZH **eingehalten** werden[7].

☐ Ich **leite keine dienstlichen E-Mails auf mein privates E-Mail-Konto um oder weiter**; ich leite eine **dienstliche E-Mail nur dann an eine externe E-Mail-Adressen** weiter, **soweit der Empfänger** zum Erhalt der Nachricht **über die externe E-Mail-Adresse autorisiert** ist.

☐ Zur **Gewährleistung der Verfügbarkeit und besseren Wiederauffindbarkeit**:

- **verschiebe ich geschäftsrelevante dienstliche E-Mails** von meinem mir persönlich zugewiesenen E-Mail-Konto **in ein sog. „Funktionskonto“** (Mail-In-Konto) sofern eine solche für die Funktion erforderlich und vorhanden ist und die E-Mails für die Stellvertretung zugreifbar sein müssen;
- **verschiebe ich geschäftsrelevante dienstliche elektronische Unterlagen in einen mir zugewiesenen Ordner** (auf einem UZH-eigenen Serverlaufwerk oder auf einem Server eines autorisierten externen Auftragsdatenbearbeiters der UZH), sofern die Unterlagen für die Stellvertretung zugreifbar sein müssen;
- **stelle ich sicher, dass mein Stellvertreter Zugriff auf das Funktionskonto und den zugewiesenen Ordner hat**.

**Geschäftsrelevant** sind solche Unterlagen und Informationen, die **für die Nachvollziehbarkeit des Geschäftsverlaufs unverzichtbar** sind; **die Entscheidung**, ob Unterlagen und Informationen in diesem Sinne unverzichtbar sind, **trägt der jeweilige Mitarbeitende der UZH.**

☐ Ich **überführe sämtliche dienstlichen Informationen und Unterlagen, die geschäftsrelevant sind, in eine** (elektronische oder physische) **Akte** entsprechend den Vorgaben, sofern meine Dienststelle/Organisationseinheit solche zur strukturierten Ablage und Verwaltung von Akten erstellt hat[8].

☐ Um **eine Vermischung von privaten mit dienstlichen Daten** und daraus resultierend z. B. eine **ungewollte Offenlegung von Details aus meinem Privatleben** im Falle des Zugriffs des IT-Betreuers oder des IT-Administrators **zu vermeiden**, **nutze** ich die dienstliche Infrastruktur respektive die dienstlichen Geräte der UZH **nur restriktiv für private Zwecke**.

☐ **Soweit** ich dennoch **private Daten auf dienstlichen Geräten der UZH bearbeite**, **kennzeichne ich diese Daten sichtbar als private Daten**. Hierzu **verschiebe** ich:

---

[6] Verse: https://www.zi.uzh.ch/de/support/e-mail-kollaboration/mobiles.html.

[7] Datenbearbeitung im Auftrag: http://www.dsd.uzh.ch/de/outsourcing.html.

[8] Merkblatt Aktenführung: http://www.archiv.uzh.ch/dam/jcr:ffffffff-e406-9649-0000-000046c958ba/2014_04_01_uaz_merkblatt_aktenfuehrung.pdf.

- **private E-Mails in einen Unterordner** meines persönlich zugewiesenen E-Mail-Kontos, den ich mit dem Namen „**PRIVAT**“ kennzeichne;
- **private Informationen respektive Unterlagen in einen mir zum persönlichen Gebrauch zugewiesenen Ordner**; den ich mit dem Namen „**PRIVAT**“ kennzeichne.

## 4. Bekanntgabe von Personendaten

☐ Ich **schalte bei Informationszugangsgesuchen** nach § 20 Abs. 1 und Abs. 2 IDG **und** bei **Amts- und Rechtshilfegesuchen**, die bei mir eingehen, **den Datenschutzdelegierten der UZH ein**. Dieser entscheidet über das weitere Vorgehen.

☐ Ich **überprüfe E-Mail-Empfängerlisten** vor Versand auf Richtigkeit.

☐ Ich **versende Informationen, die besondere Personendaten**[9] beinhalten **oder** die **einem Berufsgeheimnis**[10] **unterliegen**, sowohl an UZH-interne wie auch an UZH-externe Adressaten:

- in elektrischer Form **nur per verschlüsselter E-Mail**;
- in physischer Form **nur im verschlossenen Umschlag**, mit der Aufschrift “Vertraulich”;
- **niemals per Fax** (im Ausnahmefall ist eine telefonische Absprache zur Sicherstellung der sofortigen Anwesenheit des Empfängers am Faxgerät notwendig, um den Ausdruck an sich zu nehmen).

## 5. Ausserhalb der Büroräumlichkeiten

☐ Soweit ich aufgrund meiner Funktion und Aufgabenstellung **dienstliche Daten** und hierbei insbesondere Personendaten **ausserhalb meines Büros** bearbeite (z. B. aufgrund eines Auswärtstermins, einer Geschäftsreise oder einer Tätigkeit am Heimarbeitsplatz), nehme ich **nur solche Daten** mit mir mit respektive greife ich von ausserhalb des Büros nur auf solche Daten zu, **die zur Erfüllung der konkreten Aufgabe erforderlich sind** und **stelle sicher, dass die Daten gegen Zugriff und Kenntnisnahme Unbefugter geschützt** sind.

☐ **In der Öffentlichkeit**, wie insbesondere in Flughäfen oder Bahnhöfen oder in öffentlichen Transportmitteln, wie Bussen oder Grossraumwaggons:

- führe ich **keine vertraulichen Gespräche** (unter Anwesenden oder per Telefon);

[9] 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. Hierzu gehören Informationen über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten und Tätigkeiten, die Gesundheit, die Intimsphäre, die Rassenzugehörigkeit oder die ethnische Herkunft, Massnahmen der sozialen Hilfe, administrative oder strafrechtliche Verfolgungen oder Sanktionen. Zu den besonderen Personendaten gehören auch Zusammenstellungen von Informationen, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit natürlicher Personen (Persönlichkeitsprofil) erlauben.

[10] Das Berufsgeheimnis ist eine gesetzliche Geheimhaltungspflicht, welche für bestimmte Berufsgruppen, die auch an der UZH vorhanden sind, und deren Hilfspersonen gilt. Zu diesen Berufsgruppen zählen z. B. Ärzte, Zahnärzte und Psychologen.

- bearbeite ich **vertrauliche Daten nur dann mit meinem Laptop, soweit dessen Bildschirm mit einem Sichtschutzfilter** (z. B. „3M Blickschutzfilter“) **versehen** ist, um den Bildschirminhalt insbesondere vor unerwünschten Seitenblicken des Sitznachbarn zu schützen.

☐ Meinen dienstlichen **Laptop**, mein dienstliches **Mobiltelefon** oder **dienstliche Unterlagen:**

- gebe ich **nicht unbeaufsichtigt** aus der Hand;
- lasse ich **nicht sichtbar im Auto** liegen;
- nehme ich **im Hotel** (z. B. Hotelsafe) **oder zuhause unter Verschluss**.

## 6. Vertrauen ist gut, Kontrolle ist besser

☐ Ich bin mir bewusst, dass ich **als Mitarbeitender der UZH über vertrauliche Informationen verfüge**, die für andere Personen von Interesse sein können. Solche Personen können verschiedenste Methoden benutzen, um an solche Informationen zu gelangen, angefangen vom Mithören eines Gesprächs, über Mitlesen einer E-Mail oder Kenntnisnahme vom Inhalt einer Unterlage, bis hin zu Lauschangriffen über das Internet, wie z. B. durch Spyware und Phishing-Angriffen.

☐ Bei **vertraulichen Themen kläre ich die Identität von mir unbekannten Personen**:

- die mich anrufen, indem ich z. B. einen Rückruf vereinbare;
- die mich persönlich aufsuchen, bevor ich ihnen Zugang zu Räumen oder Zugriff auf Unterlagen der UZH verschaffe, indem ich deren Namen erfrage und indem ich mich z.B. nach deren Dienststelle/Organisationseinheit erkundige und den Dienstausweis vorzeigen lasse.

☐ Ich **kontaktiere einen** (angeblichen) **Absender persönlich**, indem ich diesen z.B. anrufe, wenn ich:

- **E-Mails mit überraschendem oder ungewöhnlichem Inhalt** erhalte, bevor ich handle;
- **E-Mails mit Dateianhängen erhalte, die ich nicht erwartet habe**, bevor ich die Anhänge öffne.

☐ **Falls** ich **im Unklaren** bin, **kläre** ich:

- mit meinem Vorgesetzten die **Vertraulichkeit einer Information**;
- mit meinem Vorgesetzten **die Autorisation einer externen Person wie auch eines UZH-internen Kollegen**; und
- bei meinem IT-Betreuer **einen computertechnischen Aspekt**.

☐ Ich **schliesse gefundene oder von Unbekannten geschenkte elektronische Datenträger**, wie insbesondere USB-Sticks oder Speicherkarten, **niemals an einen dienstlichen Rechner an**.

## 7. Löschung respektive Vernichtung von Personendaten

☐ Ich **überprüfe regelmässig, welche Daten** ich zur Erfüllung meiner Aufgabenstellung **nicht mehr benötige**.

☐ Ich **lösche respektive vernichte Personendaten**, soweit:

- diese **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 UZH-Archiv**, dem ich die Daten nach Ablauf der Aufbewahrungsfrist angeboten habe, **die Daten nicht übernommen und archiviert hat**.

☐ Ich **lösche respektive vernichte Personendaten** in der Art, dass **keine missbräuchliche Verwendung mehr möglich** ist. Daher werfe ich:

- **Fehldrucke oder Unterlagen mit Personendaten nicht in den Papierkorb**. Solche Fehldrucke und Unterlagen müssen in ein verschlossenes Sammelbehältnis, welches zur ordnungsgemässen Aktenvernichtung vorgesehen ist, entsorgt respektive sofort in einem Schredder vernichtet werden;
- **Datenträger (z.B. CDs, USB-Sticks, Speicherkarten, Festplatten),** welche ausgesondert oder vernichtet werden sollen, **nicht in den Papierkorb**, sondern gebe diese zur sicheren zentralen Entsorgung bei der für mich zuständigen IT-Abteilung ab. Die IT-Abteilung sorgt dafür, dass die auf den Datenträgern gespeicherten Daten nicht mehr lesbar sind respektive die Datenträger vernichtet werden.