dsb
datenschutzbeauftragter
kanton zürich

Leitfaden

Datenschutzlexikon Hochschule

Inhalt

1 Einleitung

Dieses Datenschutzlexikon richtet sich an Mitglieder der Hochschul- und Universitätsleitungen, Professorinnen und Professoren, Dozierende und Lehrbeauftragte, Mitarbeitende sowie Studierende, welche Fragen zu Datenbearbeitungen im kantonalen Hochschulbereich haben.

Beispiele:
- Welche Unterlagen gehören in das Personaldossier?
  Siehe unter Personaldossier.
- Dürfen Spenderinnen und Spender im Jahresbericht genannt werden?
  Siehe unter Spenderdaten.
- Dürfen Titel und akademische Grade bekannt gegeben werden?
  Siehe unter Bekanntgabe von Personendaten.
- Was muss beim Einsatz von Videokameras berücksichtigt werden?
  Siehe unter Videokameras.

Im Datenschutzlexikon finden Sie
- eine kurze Einführung zum Datenschutz
- Antworten zu den in der Praxis am häufigsten gestellten Fragen

Antworten auf Fragen, welche Sie nicht in diesem Datenschutzlexikon finden, erhalten Sie direkt beim Datenschutzbeauftragten unter der Nummer 043 259 39 99 oder via Kontaktformular unter www.datenschutz.ch.

2 Datenschutzlexikon Hochschule

2.1 Adressdaten

Siehe unter Bearbeiten von Personendaten durch die Hochschule.

2.2 Aktenaufbewahrung

Die Hochschule darf ihre Papier- und elektronischen Akten solange aufbewahren, wie sie diese für das Erfüllen ihrer Aufgaben benötigt (laufende Ablage). Die maximal folgende Aufbewahrungsfrist wird von der Hochschule gemäss IDG selbst festgelegt, es sei denn, es existieren spezialgesetzliche Regelungen.
Anschliessend müssen die für das Archiv bestimmten Akten aussortiert und archiviert werden. Die nicht ins Archiv überführten Akten sind zu vernichten. Ab diesem Zeitpunkt gelten die Bestimmungen des Archivgesetzes und nicht mehr diejenigen des IDG.

Es ist von Vorteil, Aufbewahrungsfristen zu definieren. Wie solche Fristen aussehen können, ist im Merkblatt Aktenaufbewahrung und Archivierung für die Zürcher Kantonsschulen der Schulleiterkonferenz des Kantons Zürich dokumentiert.

Die Akten müssen während der Aufbewahrung und Archivierung durch angemessene technische und organisatorische Massnahmen geschützt werden. Die Massnahmen richten sich nach dem Schutzbedarf, das heisst je sensibler die Information, desto höher ist der Schutzbedarf. Akten, welche besondere Personendaten beinhalten, beispielsweise solche einer Administrativuntersuchung, sind unter Verschluss zu halten. Elektronische Akten sind durch Passwörter zu schützen.

Dozierendenevaluationen
Siehe unter Dozierendenevaluationen.

Leistungsnachweise
Für die Aufbewahrung von Leistungsnachweisen (schriftliche Prüfungen und Arbeiten, Protokolle von mündlichen Prüfungen, Speicherung respektive Ausdruck von elektronischen Prüfungen) sowie deren Beurteilungen und Auswertungsraster gelten dieselben Anforderungen.

§ 5 Abs. 2 und 3 IDG
§ 7 IDG
§§ 7 und 8 Archivgesetz

Siehe Merkblatt Informationsverwaltung

Siehe unter Informationssicherheit.
Siehe unter Personaldossier.

2.3 Amtsgeheimnis

Mitarbeitende der Hochschule unterstehen dem Amtsgeheimnis.
Das Amtsgeheimnis gilt auch, wenn Organisationen mit der Erfüllung öffentlicher Aufgaben betraut wurden oder wenn sie im Rahmen eines Auftragsverhältnisses für die Hochschule Informationen bearbeiten.

Es untersagt die Bekanntgabe von Informationen, die im Rahmen der amtlichen oder dienstlichen Stellung wahrgenommen werden, die weder allgemein zugänglich noch öffentlich bekannt sind und bezüglich derer die Hochschule ein Interesse an der Geheimhaltung hat.
Das Offenbaren von Geheimnissen ist nicht strafbar, wenn ein gesetzlicher Rechtfertigungsgrund vorliegt. Rechtfertigungsgründe können beispielsweise gesetzlich statuierte Meldepflichten, Amtshilfehandlungen, das Vorliegen einer Entbindung durch die vorgesetzte Behörde oder die Einwilligung Betroffener sein.
Diese Verpflichtung bleibt auch nach Beendigung des Arbeitsverhältnisses bestehen. Die Verletzung des Amtsgeheimnisses ist strafbar.

Art. 320 StGB
«1. Wer ein Geheimnis offenbart, das ihm in seiner Eigenschaft als Mitglied einer Behörde oder als Beamter anvertraut worden ist, oder das er in seiner amtlichen oder dienstlichen Stellung wahrgenommen hat, wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.
Die Verletzung des Amtsgeheimnisses ist auch nach Beendigung des amtlichen oder dienstlichen Verhältnisses strafbar.
2. Der Täter ist nicht strafbar, wenn er das Geheimnis mit schriftlicher Einwilligung seiner vorgesetzten Behörde geoffenbart hat.»

§ 3 Abs. 1 lit. c IDG
§§ 1 und 2 PVO-UZH
§ 14 Abs. 1 FaHG
§ 51 PG
Art. 320 StGB

2.4 Amtshilfe

Die Hochschule kann anderen öffentlichen Organen im Einzelfall Personendaten oder besondere Personendaten bekanntgeben, wenn das anfragende Organ diese zur Erfüllung seiner gesetzlichen Aufgaben benötigt.
Voraussetzungen der Amtshilfe sind, dass

- die Informationen nicht auf andere Weise beschafft werden können (Subsidiarität),
- ein Ersuchen vorliegt,
- es sich um einen Einzelfall handelt, also nicht um eine regelmässige Datenbekanntgabe.

Von der anfragenden Stelle können sowohl die Rechtsgrundlagen, auf die sie das Ersuchen stützt, als auch der Zweck, zu welchem sie die Informationen benötigt, verlangt werden.

Es dürfen nur für die Aufgabenerfüllung der anfragenden Behörde notwendige Personendaten bekannt gegeben werden (Verhältnismässigkeitsprinzip).
Wenn rechtliche Bestimmungen oder überwiegende öffentliche oder private Interessen entgegenstehen, kann die Amtshilfe verweigert oder aufgeschoben werden.

Fachspezifische Amts- und Rechtshilfebestimmungen gehen den datenschutzrechtlichen Bestimmungen vor.

Von der Amtshilfe betroffene Personen müssen nicht informiert werden.

§ 16 Abs. 2 IDG
§ 17 Abs. 2 IDG
§ 23 IDG

Siehe unter Bekanntgabe von Personendaten.
Siehe unter Zusammenarbeit mit hochschulexternen Diensten.
Siehe unter Zusammenarbeit mit der Staatsanwaltschaft.

2.5 Analyse Prüfungsbetrug

Hochschulen können Analysetools zum Aufdecken eines Prüfungsbetrugs einsetzen, wenn für das Bearbeiten daraus resultierender Daten eine Rechtsgrundlage existiert. Das Disziplinarreglement der Universität Zürich hält beispielsweise fest, dass, wer sich bei der Ausarbeitung einer Dissertation oder anderer schriftlicher Arbeiten, bei Abschluss- oder Zwischenprüfungen unerlaubter Mittel bedient, sich eines Disziplinarfehlers schuldig macht. Somit können unter bestimmten Voraussetzungen Analysetools auf dem schuleigenen Server installiert und die Aktivitäten der Studierenden geloggt und protokolliert werden, beispielsweise wenn Studierende für Prüfungen ihre eigenen Computer benützen dürfen.

Voraussetzungen sind, dass die Studierenden vorgängig klar und deutlich über den Einsatz eines solchen Analysetools sowie über den Umfang der Überwachung informiert werden. Weiter sollten als Alternative schulische Geräte zur Verfügung gestellt werden, die so konfiguriert sind, dass keine Überwachung notwendig ist.

Die Überwachung muss verhältnismässig sein. Es dürfen nur Aktivitäten, welche auf einen Prüfungsbetrug hindeuten können, geloggt werden. Das Loggen ist auf die Prüfungsdauer zu beschränken. So ist beispielsweise eine Überprüfung von Zugriffen auf Websites oder auf Kommunikationsplattformen verhältnismässig. Nicht protokolliert werden darf hingegen der Zugriff auf die auf dem eigenen Computer gespeicherten Daten, denn diese können auch private Informationen beinhalten.
Wird kein Betrugsfall festgestellt, sind die Logdateien sofort zu löschen. Bei konkreten Hinweisen auf einen Betrugsfall können die Daten bis zum Abschluss eines Verfahrens aufbewahrt werden.

Werden Analysetools in Anspruch genommen, die eine Cloud-Lösung beinhalten, gelten zusätzliche Anforderungen.

§ 7 Disziplinarordnung der Universität Zürich
§ 8 Verordnung zum Fachhochschulgesetz

Siehe unter Auslagerung.
Siehe unter Cloud Computing.

2.6 Anonymisierung

Anonymisieren bedeutet, dass Personendaten auf eine Art verändert werden, sodass diese Daten Personen nicht mehr zugeordnet werden können. Der Vorgang ist irreversibel. Anonymisierte Daten gelten nicht mehr als Personendaten.

Eine Anonymisierung lässt sich auch dadurch erzielen, dass eindeutige Merkmale durch allgemeinere Aussagen ersetzt werden. In einem Forschungsvorhaben können beispielsweise grössere Einordnungsgruppen gebildet werden. Anstelle der Altersangabe «55» kann «über 50» verwendet werden, anstelle des konkreten Ortes die Angabe des Bezirks oder des Kantons.

Daten gelten nicht als anonymisiert, wenn der Vorgang rückgängig gemacht werden kann. Erstellt die Hochschule für ein Forschungsvorhaben eine Liste mit Namen und Adressdaten von Probanden und eine separate Liste mit den Angaben oder Merkmalen der Probanden und wird durch eine weitere Bezugsliste respektive Konkordanztabelle festgehalten, welche Angaben oder Merkmale welchen Probanden zugeordnet werden können, so liegt eine Pseudonymisierung vor. Dies gilt auch für den Fall, dass die Bezugsliste verschlüsselt oder unter besonderem Verschluss gehalten wird.

§§ 9 Abs. 2, 18 Abs. 2 IDG
§ 11 Abs. 2 IDG
§ 21 Abs. 2 IDV

Siehe unter Informationssicherheit.
Siehe unter Pseudonymisierung.

2.7 Archivierung

Die staatlichen Hochschulen können als selbständige öffentlich-rechtliche Anstalten eigene Archive führen. Das zuständige Archiv entscheidet nach Anhörung der betreffenden Abteilung oder Fakultät der Hochschule über die Archivwürdigkeit von Akten. Archivwürdig sind Akten, die beispielsweise zu wissenschaftlichen oder historischen Zwecken dauernd aufbewahrt werden.

Das Staatsarchiv als zentrales Archiv des Kantons Zürich berät und beaufsichtigt diese Archive.

§ 3 FaHG
§ 1 UniG
§§ 5, 6, 8 Archivgesetz
§§ 3 und 6 Archivverordnung

Siehe unter Aktenaufbewahrung.

2.8 Auskunft über eigene Personendaten

Das Recht auf Auskunft über die eigenen Personendaten kann jedermann in Anspruch nehmen. Studierende oder Mitarbeitende können um Auskunft über ihre bei der Hochschule vorhandenen Personendaten ersuchen. Dazu gehört auch die Auskunft über Prüfungsnoten oder Dokumente bestandener Prüfungen. Es müssen keine Interessen geltend gemacht werden.
Die Hochschule muss prüfen, ob einer Einsicht überwiegende öffentliche oder private Interessen entgegenstehen, beispielsweise wenn der Prüfungsinhalt derart ist, dass er nicht neu erstellt werden kann, die Wirkung von Untersuchungs- oder Aufsichtsmassnahmen gefährdet wäre oder andere Personen betroffen sind. In diesen Fällen ist eine Interessenabwägung vorzunehmen.
Das Gesuch muss schriftlich gestellt werden, es sei denn, die Hochschule akzeptiert eine elektronische Zustellung. Zwecks Identifizierung ist eine Kopie eines amtlichen Dokuments (Pass, Identitätskarte) beizulegen.
Die Auskunft wird in der Regel schriftlich in Form eines Ausdrucks oder einer Fotokopie erteilt. Sie kann auch auf andere geeignete Weise oder, mit Zustimmung der gesuchstellenden Person, mündlich oder durch Einsichtnahme erteilt werden.
Wird der Zugang ganz oder teilweise verweigert oder aufgeschoben, erlässt die Hochschule eine begründete Verfügung mit Rechtsmittelbelehrung.
Es werden keine Gebühren erhoben.

Mit diesem Musterbrief Auskunft über eigene Personendaten kann um Auskunft ersucht werden.

Hängiges Verfahren
In einem hängigen Verfahren richtet sich das Akteneinsichtsrecht nach dem jeweiligen Verfahrens- und Prozessrecht. Das Recht auf Zugang zu den eigenen Personendaten kann jederzeit parallel zum verfahrensrechtlichen Akteneinsichtsrecht geltend gemacht werden.
Das Studium als Ganzes ist kein hängiges Verwaltungsverfahren. Der Zugang zu Informationen richtet sich somit nach den Bestimmungen des IDG.

§ 20 Abs. 2 und 3 IDG
§ 23 ff. IDG
§§ 16 ff. IDV
§ 8 VRG

2.9 Auskunft über bei der Hochschule vorhandene Informationen

Als Ausfluss des Öffentlichkeitsprinzips können interessierte Personen um Zugang zu allgemeinen Informationen bei der Hochschule ersuchen.
Das Ersuchen kann grundsätzlich formlos, das heisst per Telefon oder E-Mail, gestellt werden. Es besteht keine Identifikationspflicht und es müssen keine Interessen geltend gemacht werden. Schriftlichkeit ist dann notwendig, wenn eine Anhörung betroffener Dritter erforderlich, für die Interessenabwägung vertiefte Abklärungen zu treffen oder die Bearbeitung des Ersuchens mit besonderem Aufwand verbunden ist. Das Ersuchen soll möglichst genaue Angaben zu den gewünschten Informationen enthalten.
Einer Einsicht können rechtliche Bestimmungen wie Geheimhaltungspflichten oder überwiegende öffentliche oder private Interessen entgegenstehen. In diesen Fällen muss die Hochschule eine Interessenabwägung durchführen. Will die Hochschule die Informationen nach dieser Interessenabwägung zugänglich machen und sind Personendaten betroffen, muss sie den Betroffenen Gelegenheit zur Stellungnahme geben. Die Hochschule kann die Einsicht durch Abdecken bestimmter Passagen teilweise gewähren oder eine inhaltliche Zusammenfassung abgeben.
Wird der Zugang ganz oder teilweise verweigert oder gegen den Willen der Betroffenen gewährt, erlässt die Hochschule eine nach den Bestimmungen des VRG anfechtbare Verfügung.

Nicht eingesehen werden können Dokumente, die von Professorinnen oder Professoren oder weiteren Angehörigen der Hochschulen lediglich zum persönlichen Gebrauch erstellt wurden.

Die Hochschule kann eine Gebühr verlangen. Die Tarife sind im Anhang zu § 35 IDV aufgeführt.

Mit diesem Musterbrief Zugang zu Informationen kann um Auskunft ersucht werden.

Sitzungsprotokolle
Ersuchen um Einsicht in Sitzungsprotokolle sind nach denselben Bestimmungen wie andere Informationszugangsersuchen zu beurteilen.
Zu berücksichtigen ist, dass ein gesetzlich verankertes Sitzungsgeheimnis nicht automatisch bedeutet, dass auch die verfassten Sitzungsprotokolle geheim bleiben. Es ist im Einzelfall zu entscheiden, ob überwiegende öffentliche oder private Interessen einer Einsicht entgegenstehen.

Verträge mit Geheimhaltungspflichten
Aufgrund des Öffentlichkeitsprinzips sind grundsätzlich alle bei der Hochschule vorhandenen Informationen zugänglich. Eine absolute Geheimhaltung kann somit seitens der Hochschule nicht zugesichert werden, selbst wenn eine Vertraulichkeitsklausel vereinbart wurde. Ist Letzteres der Fall, ist eine Interessenabwägung vorzunehmen. Dabei ist zu beachten, dass zu den privaten Interessen einer juristischen Person das strafrechtlich geschützte Geschäfts- und Fabrikationsgeheimnis gehört.

§ 20 Abs. 1 IDG
§§ 23 ff. IDG
§§ 7 ff. IDV
§ 35 IDV inklusive Anhang

Siehe unter Öffentlichkeitsprinzip.

2.10 Auslagerung

Die Hochschule kann das Bearbeiten von Informationen Dritten übertragen, also auslagern. Dies ist beispielsweise bei der Nutzung von Dropbox, von Microsoft Office 365 oder wenn ein Gutachten in Auftrag gegeben wird, der Fall. Auch der Einsatz einer Plagiatserkennungs- oder einer anderen Software durch externe Dienstleister sowie der Betrieb und die Wartung der IT-Infrastruktur (Netzwerk, Server, Anwendungen) gehören dazu.

Werden im Rahmen von solchen Auslagerungen besondere Personendaten bearbeitet, sind zu deren Schutz besondere Massnahmen umzusetzen. Von einer Auslagerung ins Ausland sollte in diesen Fällen abgesehen werden.

Der Datenschutzbeauftragte überprüft gerne die datenschutzrechtlichen Aspekte Ihres ausgewählten Produkts.

Zu Voraussetzungen und Vorgehen siehe Leitfaden Bearbeiten im Auftrag
Siehe Merkblatt Online-Speicherdienste
Siehe Merkblatt privatim Cloud Computing im Schulbereich

§ 6 IDG
§ 25 IDV

Siehe unter Cloud Computing.
Siehe unter Microsoft Office 365.
Siehe unter Website.

2.11 Austausch von Informationen

Siehe unter Amtshilfe.
Siehe unter Bekanntgabe von Personendaten.
Siehe unter Zusammenarbeit innerhalb der Hochschule.
Siehe unter Zusammenarbeit mit hochschulexternen Diensten.
Siehe unter Zusammenarbeit mit der Staatsanwaltschaft.

2.12 Bearbeiten im Auftrag

Siehe unter Auslagerung.
Siehe unter Cloud Computing.
Siehe unter Microsoft Office 365.

2.13 Bearbeiten von Personendaten durch die Hochschule

Eine Hochschule darf diejenigen Personendaten bearbeiten, die sie für ihre gesetzliche Aufgabenerfüllung benötigt. Das Bearbeiten von besonderen Personendaten erfordert eine formell-gesetzliche Grundlage. Grundsätzlich legt die Bildungsdatenverordnung in Anhang 1 die von den Rektoraten und den Schulsekretariaten zu erhebenden Personendaten fest. Bei den Studierenden sind dies unter anderem Name, Geburtsdatum, Geschlecht, Wohnadresse, Noten und Abschlüsse. Zugleich wird festgehalten, welche Empfänger welche Informationen regelmässig erhalten (Hochschulamt, Bildungsstatistik, Wohnkanton bei ausserkantonalen Studierenden).
Weitere Bestimmungen finden sich in den fachspezifischen Gesetzen.

§ 8 IDG
§§ 2 ff., 7a UniG
§§ 1 ff. PHG
§ 6a FaHG
§§ 1 ff. Allgemeine Studienordnung der Zürcher Hochschule der Künste
§§ 6 ff. Hochschulordnung der Zürcher Hochschule für Angewandte Wissenschaften
Anhang 1 Bildungsdatenverordnung

Adressen von Studierenden und Mitarbeitenden
Adressen von Studierenden und Mitarbeitenden dürfen nur zu dem Zweck bearbeitet werden, zu dem sie erhoben wurden. Eine anderweitige Bearbeitung ist nur gestützt auf eine rechtliche Bestimmung oder im Einzelfall mit Einwilligung der betroffenen Person möglich.
Die hochschulinterne Bearbeitung von Adressen, um beispielsweise auf Veranstaltungen oder Umfragen hinzuweisen, ist zulässig, soweit dies für den Bildungsauftrag geeignet und erforderlich ist. Die Studierenden und Mitarbeitenden sind bereits bei

der Angabe ihrer Adressen zu informieren, dass diese von der Hochschule auch für solche Zwecke verwendet werden.

§ 8 Abs. 1 IDG
§ 9 Abs. 1 IDG

Daten von Sponsoren
Das Sammeln und Auswerten von Informationen über bestehende und potenzielle Sponsoren ist zulässig, soweit dies zur Erfüllung der gesetzlichen Aufgabe der Hochschule notwendig ist. Ein weiteres Bearbeiten ist nur möglich, wenn eine rechtliche Bestimmung vorliegt oder die Sponsoren im Einzelfall einwilligen. Es muss für die Sponsoren erkennbar sein, zu welchen Zwecken diese Daten bearbeitet werden.
Bei der Universität Zürich beispielsweise gehört die Beschaffung finanzieller Mittel bei Dritten zum gesetzlich umschriebenen Aufgabenbereich.

§ 9 Abs. 1 IDG
§ 12 IDG
§ 40 UniG
§§ 12 ff. Finanzreglement der Universität Zürich

Daten von Spendenden siehe unter Bekanntgabe von Personendaten.

2.14 Bearbeiten von Personendaten für nicht personenbezogene Zwecke

Bei der Hochschule vorhandene Personendaten dürfen für nicht personenbezogene Zwecke wie Statistik oder Forschung bearbeitet werden. Voraussetzung ist, dass sie anonymisiert werden und aus den Auswertungen keine Rückschlüsse auf betroffene Personen möglich sind.

§ 9 Abs. 2 IDG

Siehe unter Forschungsvorhaben.

2.15 Bekanntgabe von Informationen von allgemeinem Interesse

Die Hochschule kann von Amtes wegen über Tätigkeiten von allgemeinem Interesse wie Anlässe, Neuigkeiten, Hochschulprogramme, aber auch bedeutende Entscheide und Massnahmen, Ziele usw. informieren. Aufbau, Zuständigkeit und Ansprechpersonen können ebenso veröffentlicht werden. Dazu gehören beispielsweise die Namen, Funktionen, die geschäftlichen Telefonnummern und E-Mail-Adressen der Hochschulmitarbeitenden, soweit diese Funktionen für die Hochschule ausüben, die von allgemeinem Interesse sind. Nicht dazu gehören beispielsweise die Staatsangehörigkeit der Professorinnen und Professoren.

Private Kontaktangaben oder Fotos dürfen nur mit Einwilligung der Betroffenen veröffentlicht werden.

Als Informationsträger kommen hauptsächlich die Hochschulwebsite, das Intranet oder Printmedien in Frage.

Art. 49 KV
§ 14 IDG

Siehe unter Website.
Siehe unter Intranet.

2.16 Bekanntgabe von Personendaten

Die Hochschule kann Personendaten wie Namen und Adressen bekannt geben, wenn

- eine rechtliche Bestimmung dies vorsieht oder
- die Einwilligung Betroffener vorliegt oder
- eine unmittelbare Gefahr für Leib und Leben besteht oder
- der notwendige Schutz anderer wesentlicher Rechtsgüter höher zu gewichten ist oder
- unter den Voraussetzungen der Amtshilfe.

Für die Bekanntgabe von sensitiven, also besonderen Personendaten gelten höhere Anforderungen. Es braucht eine formell-gesetzliche Grundlage. Es gilt immer das Verhältnismässigkeitsprinzip. Das heisst, dass nur die für die jeweilige Aufgabenerfüllung geeigneten und erforderlichen Informationen bekannt gegeben werden.

§§ 16 und 17 IDG
Bestimmungen in fachspezifischen Gesetzen

Siehe unter Amtshilfe.
Siehe unter Auskunft über eigene Personendaten.
Siehe unter Auskunft über bei der Hochschule vorhandene Informationen.
Siehe unter Forschungsvorhaben.
Siehe unter Informationsaustausch.
Siehe unter Zusammenarbeit innerhalb der Hochschule.
Siehe unter Zusammenarbeit mit hochschulexternen Diensten.
Siehe unter Zusammenarbeit mit der Staatsanwaltschaft.

Bekanntgabe von Titeln, akademischen Graden und Studienabschlüssen
Für regelmässige Bekanntgaben von Personendaten wie Titel, akademischen Graden und Studienabschlüssen bedarf es einer Rechtsgrundlage. So kann beispielsweise die Universität Zürich die erworbenen Titel und akademischen Grade mit den persönlichen Daten der Studierenden anlässlich des Erwerbs veröffentlichen.

Eine nachträgliche Veröffentlichung auf der Website ist möglich, wenn erworbene Titel und akademische Grade durch Eingabe eines Namens in ein Webformular einzeln und automatisch abrufbar sind. Ansonsten ist für die nach Erwerb des Titels und dessen Veröffentlichung erfolgende Bekanntgabe die Einwilligung der Betroffenen erforderlich.

§ 16 Abs. 1 lit. a IDG
§ 12 Abs. 3 VZS

Bekanntgabe von Informationen über Spendende im Jahresbericht
Für die Bekanntgabe von Namen, Adresse und Spendenbetrag von spendenden natürlichen oder juristischen Personen in Jahresberichten oder anderen Publikationen gelten ebenfalls die Voraussetzungen der §§ 16 und 17 IDG. Im Vordergrund steht die Einwilligung Betroffener, wobei eine konkludente Einwilligung möglich ist, nicht jedoch eine mutmassliche.

2.17 Bekanntgabe von Personendaten für nicht personenbezogene Zwecke

Siehe unter Forschungsvorhaben.

2.18 Bring Your Own Device

Siehe unter Informationssicherheit.

2.19 Cloud Computing

Die Nutzung von Cloud Services ist aus datenschutzrechtlicher Sicht ein Bearbeiten von Informationen durch Dritte. Produkte wie Microsoft Office 365, Dropbox, Turnitin, Evernote und andere, welche Informationen in der Cloud bearbeiten, dürfen durch die Hochschule unter Berücksichtigung der datenschutzrechtlichen Anforderungen eingesetzt werden. Mit dem Anbieter muss ein datenschutzkonformer Vertrag abgeschlossen respektive müssen datenschutzkonforme allgemeine Geschäftsbedingungen vereinbart werden.
Sind besondere Personendaten, beispielsweise Informationen über die Gesundheit, über religiöse oder politische Ansichten, betroffen, sind besondere Sicherheitsmassnahmen erforderlich. Im Vordergrund steht die Verschlüsselung dieser Daten. Der

Datenschutzbeauftragte rät, sensible Daten nur an Anbieter auszulagern, die diese in der Schweiz bearbeiten. Er überprüft gerne die datenschutzrechtlichen Aspekte Ihres ausgewählten Produkts.

§ 6 IDG
§ 25 IDV

Zu Voraussetzungen und Vorgehen siehe Leitfaden Bearbeiten im Auftrag

Siehe Merkblatt privatim Cloud Computing im Schulbereich
Siehe Merkblatt Online Speicherdienste

Siehe unter Auslagerung.
Siehe unter Microsoft Office 365.

2.20 Datenbearbeitung durch Dritte

Siehe unter Auslagerung.
Siehe unter Cloud Computing.

2.21 Datenbekanntgabe

Siehe unter Amtshilfe.
Siehe unter Auskunft über eigene Personendaten.
Siehe unter Auskunft über bei der Hochschule vorhandene Informationen.
Siehe unter Bekanntgabe von Informationen von allgemeinem Interesse.
Siehe unter Bekanntgabe von Personendaten.
Siehe unter Bekanntgabe von Personendaten für nicht personenbezogene Zwecke.
Siehe unter Forschungsvorhaben.
Siehe unter Zusammenarbeit innerhalb der Hochschule.
Siehe unter Zusammenarbeit mit hochschulexternen Diensten.
Siehe unter Zusammenarbeit mit der Staatsanwaltschaft.

2.22 Datenschutz

Was ist Datenschutz?
Datenschutz ist der Schutz der Privatsphäre und der Persönlichkeitsrechte, der Schutz vor missbräuchlicher Datenbearbeitung oder allgemein das Recht, selbst zu bestimmen, wer wann welche meiner persönlichen Daten zu welchen Zwecken bearbeiten darf und wem diese bekannt gegeben werden dürfen.

Warum braucht es Datenschutz?
Technische Errungenschaften ermöglichen ein nahezu unbeschränktes Sammeln, Auswerten und Bearbeiten von Informationen. Wer nicht weiss, was über ihn gespeichert und bearbeitet wird, verliert die Kontrolle über die persönlichen Informationen und wird manipulierbar. Im schlimmsten Fall können ohne Kenntnis der betroffenen Person unterschiedlichste Informationen aus verschiedensten Quellen aus dem Zusammenhang gerissen, neu gebündelt und ein völlig falsches Abbild der Person erzeugt werden. Dies kann mit gravierenden Konsequenzen familiärer, sozialer, beruflicher, finanzieller und sonstiger Art verbunden sein.
Unsere liberale Gesellschaft basiert auf der Selbstbestimmung im demokratisch rechtsstaatlichen Rahmen. Deshalb sind Rahmenbedingungen für den Staat und für Privatpersonen erforderlich, welche das Bearbeiten persönlicher Informationen an konkrete Voraussetzungen knüpfen und den Schutz der Persönlichkeitsrechte gewährleisten. Diese Rahmenbedingungen finden Sie in den Datenschutzgesetzen und in den für den Hochschulbereich geltenden Rechtsgrundlagen.

Siehe auf YouTube Why privacy matters.

Siehe unter Datenschutzrelevante Rechtsgrundlagen Fachhochschule.
Siehe unter Datenschutzrelevante Rechtsgrundlagen Universität.

2.23 Datenschutzrechtliche Begriffe

Informationen	Alle Aufzeichnungen, welche die Erfüllung einer öffentlichen Aufgabe betreffen, ausgenommen Notizen zum persönlichen Gebrauch
Sachdaten	Informationen, die sich nicht auf Personen beziehen
Personendaten	Informationen, welche sich auf bestimmte oder bestimmbare Personen beziehen Beispiel: Name, Vorname, Adresse
Besondere Personendaten	Informationen, bei denen wegen ihrer Bedeutung, der Art ihrer Bearbeitung oder der Möglichkeit ihrer Verknüpfung mit anderen Informationen die besondere Gefahr einer Persönlichkeitsverletzung besteht Beispiele: Informationen über die Gesundheit, politische Ansichten, strafrechtliche Verfolgungen
Bearbeiten	Jeder Umgang mit Informationen wie das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben oder Vernichten

Bekanntgabe	Art des Bearbeitens, jedoch explizit im IDG und in fachspezifischen Gesetzen geregelt
Informationssicherheit	Informationen müssen durch die Hochschule mit angemessenen organisatorischen und technischen Massnahmen geschützt werden. Die Massnahmen sind darauf auszurichten, dass sie die Vertraulichkeit, Integrität, Verfügbarkeit, Zurechenbarkeit und Nachvollziehbarkeit gewährleisten. Beispiele von Massnahmen sind die Installation eines Virenschutzes, Firewall, Back-up, Protokollierung usw.

2.24 Datenschutzrechtliche Prinzipien

Gesetzmässigkeit
Mitarbeitende der Hochschulen dürfen Personendaten bearbeiten, wenn dies zur Erfüllung der gesetzlich umschriebenen Aufgaben geeignet und erforderlich ist. Diese sind in Gesetzen, Verordnungen, Reglementen, Studien- oder Fachhochschulordnungen oder Weisungen umschrieben.
Für das Bearbeiten von besonderen Personendaten, also sensiblen Daten wie politische Ansichten oder Gesundheitsdaten gelten strengere Anforderungen als für Personendaten. Es ist eine Grundlage in einem formellen Gesetz erforderlich.

§ 8 Abs. 1 und 2 IDG

Siehe unter Datenschutzrelevante Rechtsgrundlagen Fachhochschule.
Siehe unter Datenschutzrelevante Rechtsgrundlagen Universität.
Siehe unter Gesetzesverzeichnis.

Verhältnismässigkeit
Die Hochschule darf nur diejenigen Personendaten bearbeiten, die für ihre Aufgabenerfüllung geeignet und erforderlich sind.

§ 8 Abs. 1 IDG

Zweckbindung
Personendaten dürfen durch Mitarbeitende der Hochschulen nur zu dem Zweck bearbeitet werden, zu dem sie erhoben wurden, es sei denn, es existiert eine rechtliche Grundlage oder die betroffenen Personen willigen in eine andere Bearbeitung ein.

Anonymisierte Daten können, beispielsweise im Rahmen von Statistiken, ohne Einwilligung bearbeitet und bekannt gegeben werden.

§ 9 Abs. 1 und 2 IDG

Transparenz
Die Beschaffung von Personendaten und der Zweck ihrer Bearbeitung durch die Hochschule müssen für die betroffenen Personen erkennbar sein. Dabei genügt es, wenn das Bearbeiten in einer rechtlichen Grundlage festgehalten ist.

§ 12 Abs. 1 IDG

Informationssicherheit
Verantwortliche der Hochschule müssen dafür sorgen, dass die Informationen, welche im Hochschulbereich bearbeitet werden, durch angemessene Massnahmen geschützt werden. Die Massnahmen sind darauf auszurichten, dass sie die Vertraulichkeit, Integrität, Verfügbarkeit, Zurechenbarkeit und Nachvollziehbarkeit gewährleisten.

§ 7 IDG

Siehe unter Informationssicherheit.

2.25 Datenschutzrelevante Rechtsgrundlagen Fachhochschule

Die für den Bereich der Fachhochschule wichtigsten Rechtsgrundlagen sind:

Gesetze
- Archivgesetz, LS 170.6
- Bildungsgesetz, BiG, LS 410.1
- Fachhochschulgesetz, FaHG, LS 414.10
- Gesetz über die Information und den Datenschutz, IDG, LS 170.4
- Gesetz über die Pädagogische Hochschule, PHG, LS 414.41
- Gesetz über den Beitritt des Kantons Zürich zur Interkantonalen Vereinbarung über die Anerkennung von Ausbildungsabschlüssen, LS 410.4
- Gesetz über den Beitritt zum Regionalen Schulabkommen über die gegenseitige Aufnahme von Auszubildenden und Ausrichtung von Beiträgen (RSA 2009), LS 414.16

Verordnungen
- Archivverordnung, LS 170.61
- Verordnung über Datenbearbeitung im Bildungsbereich (Bildungsdatenverordnung), LS 410.7

- Verordnung zum Fachhochschulgesetz, LS 414.101
- Verordnung über die Information und den Datenschutz, IDV, LS 170.41
- Personalverordnung der Zürcher Fachhochschule, PVF, LS 414.112
- Verordnung über das besondere Aufnahmeverfahren an der pädagogischen Hochschule, LS 414.413
- Verordnung über die Organisation und Verfahren der Rekurskommission der Zürcher Hochschulen, LS 415.111.7

Reglemente

- Reglement über die Anerkennung der Lehrdiplome in Schulischer Heilpädagogik, LS 410.412
- Organisationsreglement des Fachhochschulrates der Zürcher Fachhochschule, LS 414.113
- Reglement über die Zulassung zum Studium an der Pädagogischen Hochschule Zürich, LS 414.412
- Reglement über die Prüfungen an der Pädagogischen Hochschule Zürich, LS 414.414
- Reglement Erwerb eines zusätzlichen Stufendiploms, LS 414.417
- Reglement zum Zusatzdiplom Grundstufe an der Pädagogischen Hochschule Zürich, LS 414.417.1
- Reglement zum ausserschulischen Praktikum, LS 414.412.2
- Reglement über den Titel der Professorin oder des Professors an der Zürcher Fachhochschule, LS 414.112.2
- Reglement betreffend Ergänzungsstudien an der Pädagogischen Hochschule Zürich, LS 414.414.2
- Weitere Diplomreglemente
  Beispiel: Diplomreglement zum Master of Advanced Studies Pädagogische Hochschule Zürich in Bildungsmanagement sowie zum Master of Advanced Studies Pädagogische Hochschule Zürich in Bildungsinnovation, LS 414.421.1

Fachhochschulordnungen

- Allgemeine Studienordnung der Zürcher Hochschule der Künste, LS 414.262
- Hochschulordnung der Zürcher Hochschule für Angewandte Wissenschaften, LS 414.251
- Hochschulordnung der Pädagogischen Hochschule Zürich, LS 414.410
- Hochschulordnung der Zürcher Hochschule der Künste, LS 414.261
- Rahmenprüfungsordnung für Bachelor- und Masterstudiengänge an der Zürcher Hochschule für Angewandte Wissenschaften, LS 414.252.3
- Weitere Studienordnungen
  Beispiel: Studienordnung für den Masterstudiengang Architektur an der Zürcher Hochschule für Angewandte Wissenschaften, LS 414.253.115

Weisungen

- Weisung zum Aufnahme- und Immatrikulationsverfahren an der Pädagogischen Hochschule Zürich, LS 414.412.1
- Weisung zu Weiterbildungsveranstaltungen der Pädagogischen Hochschule Zürich, LS 414.419
- Weisung zur Benutzung der Bibliothek der Pädagogischen Hochschule Zürich, LS 414.410.3
- Weisung zu den Professuren an der Pädagogischen Hochschule Zürich, LS 414.410.1

2.26 Datenschutzrelevante Rechtsgrundlagen Universität

Die für den universitären Bereich wichtigsten Rechtsgrundlagen sind:

Gesetze

- Archivgesetz, LS 170.6
- Bildungsgesetz, BiG, LS 410.1
- Gesetz über die Information und den Datenschutz, IDG, LS 170.4
- Universitätsgesetz, UniG, LS 415.11

Verordnungen

- Archivverordnung, LS 170.61
- Verordnung über Datenbearbeitung im Bildungsbereich (Bildungsdatenverordnung), LS 410.7
- Verordnung über die Information und den Datenschutz, IDV, LS 170.41
- Personalverordnung der Universität Zürich, PVO-UZH, LS 415.21
- Verordnung über die Organisation und Verfahren der Rekurskommission der Zürcher Hochschulen, LS 415.111.7
- Verordnung über die Zulassung zum Studium an der Universität Zürich, VZS, LS 415.31
- Weitere Rahmenverordnungen über Studiengänge
  Beispiel: Rahmenverordnung über den Bachelor- und Masterstudiengang sowie die Nebenfachstudienprogramme an der Rechtswissenschaftlichen Fakultät der Universität Zürich, LS 415.415.1
- Weitere Verordnungen über die Promotion
  Beispiel: Verordnung über die Promotion zur Doktorin / zum Doktor der Rechtswissenschaft (Dr. iur.) an der Rechtswissenschaftlichen Fakultät der Universität Zürich (Promotionsverordnung), LS 415.413

Reglemente

- Organisationsreglement des Universitätsrats, LS 415.111.1
- Reglement zum Schutz vor sexueller Belästigung an der Universität Zürich, LS 415.116

- Reglement über die Beurteilung von Lehrveranstaltungen durch die Studierenden an der Universität Zürich, LS 415.121
- Reglement über die Aufnahmeprüfung an die Universität Zürich, LS 415.311
- Finanzreglement der Universität Zürich, LS 415.112
- Reglement über die Verwendung des Forschungskredits der Universität Zürich, LS 415.165
- Siehe Reglement über die Videoüberwachung und die Videounterstützung an der Universität Zürich
- Schlüsselreglement der Universität Zürich

Universitätsordnungen

- Universitätsordnung der Universität Zürich, LS 415.111
- Disziplinarordnung der Universität Zürich, LS 415.33
- Allgemeine Hausordnung der Universität Zürich, LS 415.111.411

Weitere universitäre Richtlinien / Reglemente, Weisungen und Merkblätter finden Sie unter http://www.rd.uzh.ch/de/rechtssammlung/richtlinien.html.

2.27 Datensicherheit

Siehe unter Informationssicherheit.

2.28 Datenvernichtung

Siehe unter Vernichten elektronischer Akten.

2.29 Dozierendenevaluationen

Dozierendenevaluationen, die von der Studiengangleitung durchgeführt werden, können personalrechtlichen Zwecken oder solchen der Qualitätsverbesserung dienen.

Werden sie als personalrechtliches Instrument eingesetzt, sind sie im Personaldossier aufzubewahren und es gelten die personalrechtlichen Aufbewahrungsfristen.

Siehe unter Personaldossier.

Werden sie als Instrument zur Verbesserung der Lehrqualität eingesetzt, gelten die allgemeinen Bestimmungen und Fristen der Aktenaufbewahrung und Archivierung.

Siehe unter Aktenaufbewahrung.

§§ 1 ff. Reglement über die Beurteilung von Lehrveranstaltungen durch die Studierenden an der Universität Zürich

2.30 Dropbox

Siehe unter Auslagerung.
Siehe unter Cloud Computing.

2.31 E-Mails

Siehe unter Informationssicherheit.

2.32 Facebook

Siehe unter Soziale Medien.

2.33 Forschungsvorhaben

Forschungsvorhaben mit Daten anderer öffentlicher Organe oder Daten Dritter
Möchte die Hochschule von einem anderen öffentlichen Organ oder einem Dritten Personendaten für ein Forschungsvorhaben beschaffen, so muss sie sicherstellen, dass

- das Bearbeiten dieser Personendaten für nicht personenbezogene Zwecke erfolgt und
- keine rechtliche Bestimmung entgegensteht und
- ein schriftliches Ersuchen verfasst wird, in dem unter anderem festgehalten wird, dass die Personendaten so früh wie möglich anonymisiert und spätestens nach ihrer Auswertung gelöscht werden.

Sind vom Projekt medizinische Daten, welche unter das Berufsgeheimnis fallen, betroffen, so sind Art. 321bis StGB und Art. 45 ff. Humanforschungsgesetz zu berücksichtigen.

Das angefragte öffentliche Organ oder der Dritte ist nicht verpflichtet, die Personendaten bekannt zu geben.
Die Hochschule kann zudem Personen selbst kontaktieren, um sie auf ein Forschungsvorhaben und die freiwillige Teilnahme an einem Projekt hinzuweisen.

Wird die Hochschule um Bekanntgabe von Personendaten für Forschungsvorhaben gebeten, gelten dieselben Anforderungen.

§ 18 IDG
§ 21 IDV
§ 3 ff. UniG

Siehe Merkblatt Personendaten für Forschungsvorhaben

Forschungsvorhaben mit bei der Hochschule vorhandenen Daten
Die Hochschule darf ihre eigenen Daten wie die von Studierenden und Mitarbeitenden zu nicht personenbezogenen Zwecken bearbeiten, wenn sie anonymisiert werden und aus den Auswertungen keine Rückschlüsse auf betroffene Personen möglich sind. Dies ist beispielsweise bei internen Forschungsprojekten oder Statistiken der Fall.

§ 9 Abs. 2 IDG

2.34 Fotos auf der Website

Siehe unter Website.

2.35 Gesetzliche Grundlagen

Siehe unter Datenschutzrelevante Rechtsgrundlagen Fachhochschule.
Siehe unter Datenschutzrelevante Rechtsgrundlagen Universität.
Siehe unter Gesetzesverzeichnis.

2.36 Informationsaustausch

Siehe unter Amtshilfe.
Siehe unter Bekanntgabe von Personendaten.
Siehe unter Bekanntgabe von Personendaten für nicht personenbezogene Zwecke.
Siehe unter Forschungsvorhaben.
Siehe unter Zusammenarbeit innerhalb der Hochschule.
Siehe unter Zusammenarbeit mit hochschulexternen Diensten.
Siehe unter Zusammenarbeit mit der Staatsanwaltschaft.

2.37 Informationssicherheit

Die Hochschule muss ihre Informationen mit angemessenen organisatorischen und technischen Sicherheitsmassnahmen schützen.

Die von der Hochschule zum Schutz der Informationen umzusetzenden Massnahmen richten sich nach der Art der Informationen, nach Art und Zweck der Bearbeitung und nach dem jeweiligen Stand der Technik. Je sensibler die Informationen, desto umfassender sind die zum Schutz der Daten zu treffenden Massnahmen. Letztere richten sich nach den folgenden Schutzzielen:

- Vertraulichkeit
  Es muss verhindert werden, dass Unberechtigte Kenntnis von den Informationen erlangen.
  Mögliche Massnahmen: Zugriffskonzept und Beschränkung der Zugriffe auf die für die Ausübung der Funktion notwendigen Daten, Verschlüsselung der Daten

- Integrität
  Informationen müssen richtig und vollständig sein.
  Mögliche Massnahme: Protokollierung der Änderungen

- Verfügbarkeit
  Informationen müssen bei Bedarf vorhanden sein.
  Mögliche Massnahmen: Sicherung der Daten (Back-up), redundante Architektur der Systeme

- Zurechenbarkeit
  Das Bearbeiten von Informationen muss einer Person zugerechnet werden können.
  Mögliche Massnahme: Protokollierung der Zugriffe, persönliche Benutzerkonten

- Nachvollziehbarkeit
  Veränderungen von Informationen müssen erkennbar und nachvollziehbar sein.
  Mögliche Massnahme: Protokollierung der Änderungen und der Zugriffe

Im Massnahmenkatalog finden die verantwortlichen IT-Leiterinnen und -Leiter die für die Hochschule angemessenen Massnahmen.

Siehe unter Anonymisierung.
Siehe unter Pseudonymisierung.

E-Mails
Werden E-Mails mit sensitiven Informationen über ungesicherte Netze wie das Internet versandt, müssen Massnahmen zum Schutze der Vertraulichkeit umgesetzt wer-

den. Beispielsweise können die Informationen verschlüsselt oder anonymisiert werden. Werden Abkürzungen verwendet, ist sicherzustellen, dass keine Rückschlüsse auf die betroffenen Schülerinnen oder Schüler möglich sind.

Siehe Merkblatt Sichere E-Mails

Mobile private Geräte «Bring Your Own Device»
Werden private Geräte (Smartphones, Notebooks, Tablets) zur Erfüllung der Aufgaben der Hochschule eingesetzt, müssen die Informationen mit den geeigneten organisatorischen und technischen Massnahmen geschützt werden. Unbeaufsichtigte, vergessene oder unsichere Geräte bergen Risiken.
Minimummassnahmen sind beispielsweise das Einrichten von Passwörtern oder PIN-Schutz, die Installation eines Virenschutzes und das Durchführen regelmässiger Updates. Sensible Daten sind bei der Speicherung und Übermittlung durch Verschlüsselung zu schützen.

Siehe Leitfaden Einsatz mobiler Geräte in der Verwaltung

Papierdossiers
Auch physische Dossiers müssen geschützt werden, wobei insbesondere die Vertraulichkeit eine grosse Rolle spielt. Die Massnahmen sind hauptsächlich darauf auszurichten, dass nur berechtigte Personen Kenntnis von deren Inhalt erlangen. Beispielsweise sind Personaldossiers oder Prüfungsergebnisse in abschliessbaren Schränken aufzubewahren.

Private E-Mail-Accounts von Hochschulangehörigen
Mitarbeitende von Hochschulen dürfen dienstliche Informationen grundsätzlich nicht an ihre private E-Mail-Adresse weiterleiten, es sei denn, die zum Schutz dieser Informationen notwendigen Massnahmen werden umgesetzt.
Werden solche Informationen ausserhalb der Hochschule bearbeitet, kann dies die Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit, Zurechenbarkeit und Nachvollziehbarkeit verletzen respektive gefährden.

Siehe im vorangehenden Abschnitt «Mobile private Geräte».

Website
Der Datenschutzbeauftragte überprüft auf Anfrage Ihre Website mit einem Webscanner automatisiert auf Schwachstellen und Sicherheitslücken.

§ 7 IDG

2.38 Informationszugang

Siehe unter Auskunft über eigene Personendaten.
Siehe unter Auskunft über bei der Hochschule vorhandene Informationen.
Siehe unter Öffentlichkeitsprinzip.

2.39 Internet

Siehe unter Intranet.
Siehe unter Website.

2.40 Intranet

Wird das Intranet als internes Informationsmedium genutzt, so ist zu beachten, dass das Intranet je nach Grösse der Hochschule trotzdem nahezu öffentlich sein kann. Bei einer Publikation von Personendaten im Intranet sind deshalb grundsätzlich die Vorschriften über die Bekanntgabe von Personendaten einzuhalten.
Die Informationstätigkeit von Amtes wegen erfolgt über die amtlichen Publikationsorgane, das Internet oder die Medien (Zeitung, Radio, Fernsehen). Das Intranet genügt in diesem Fall nicht als alleiniges Publikationsmittel.

§ 14 IDG
§ 4 IDV

2.41 Jahresberichte

Siehe unter Bekanntgabe von Personendaten.

2.42 Learning Analytics

Siehe unter Analyse Prüfungsbetrug.

2.43 Microsoft Office 365

Microsoft Office 365 kann durch die Hochschulen datenschutzkonform genutzt werden, wenn erstens die Zusatzvereinbarung, welche auf schweizerische Rechtsverhältnisse zugeschnitten ist, vereinbart wird. Darin wird die Datenspeicherung in Europa festgehalten, das schweizerische Recht für anwendbar erklärt und ein schweizerischer Gerichtsstand vereinbart. Zweitens sind bei der konkreten Anwendung die der Art der Daten entsprechenden Massnahmen wie das Verschlüsseln von besonderen Personendaten zu berücksichtigen.

Siehe unter Cloud Computing.

2.44 Mobile private Geräte

Siehe unter Informationssicherheit.

2.45 Öffentlichkeitsprinzip

Das in der Kantonsverfassung verankerte Öffentlichkeitsprinzip bedeutet, dass jede Person das Recht auf Zugang zu amtlichen Dokumenten hat, soweit nicht überwiegende öffentliche oder private Interessen entgegenstehen.

Weitere Informationen zum Öffentlichkeitsprinzip finden Sie unter www.zh.ch / Rechtliche Grundlagen / Öffentlichkeitsprinzip.

§ 17 KV
§ 20 Abs. 1 IDG

Siehe unter Auskunft über bei der Hochschule vorhandene Informationen.

2.46 Outsourcing

Siehe unter Auslagerung.
Siehe unter Cloud Computing.
Siehe unter Microsoft Office 365.

2.47 Personaldossier

Inhalt eines Personaldossiers
In ein Personaldossier gehören nur Informationen, die im Zusammenhang mit der Anstellung relevant sind, zum Beispiel die Beurteilung der Mitarbeitenden oder Akten über besondere Ereignisse und Verfahren. Falls Dozierendenevaluationen auch als personalrechtliches Instrument verwendet werden, so sind sie im Personaldossier aufzubewahren. Angaben über privates Verhalten, Gesinnung oder Informationen über das Beziehungsnetz gehören nicht dazu. Steht ein Vorfall aus dem Privatleben in direktem Zusammenhang mit dem Arbeitsverhältnis und ist beispielsweise ein Gerichtsurteil ergangen, darf ein Vermerk erfolgen. Neben dem Personaldossier dürfen keine Personalakten geführt werden.

Der Inhalt des Personaldossiers muss periodisch überprüft werden. Personalakten, die für die Durchführung des Arbeitsverhältnisses oder die Erstellung eines Arbeitszeugnisses nicht mehr geeignet und notwendig sind, sind zu vernichten.

§§ 34 ff. PG
§§ 21 ff. Vollzugsverordnung zum Personalgesetz

Anspruch auf Dossiereinsicht
Mitarbeitende der Hochschule haben das Recht auf Einsicht in die sie betreffenden Daten. Die Einsicht in das Personaldossier kann zur Wahrung überwiegender öffentlicher oder privater Interessen verweigert oder eingeschränkt werden, beispielsweise wenn eine Beschwerde Teil des Dossiers ist. Eine Verweigerung oder Einschränkung ist zu begründen. Der wesentliche Inhalt ist bekannt zu geben.

§ 20 Abs. 2 IDG
§ 23 IDG

Siehe unter Auskunft über eigene Personendaten.

Anspruch auf Löschung
Sind im Personaldossier Akten vorhanden, die nicht mit der Anstellung zusammenhängen oder mit denen die betroffenen Hochschulmitarbeitenden nie konfrontiert wurden, besteht unter Umständen ein Anspruch auf Löschung oder Gegendarstellung.

Wurde eine Akte abgelegt, die persönliche oder berufliche Vorfälle thematisiert, ohne dass weitere Handlungen erfolgten, so besteht nach Ablauf einer gewissen Zeit ein Anspruch auf Vernichtung. Die Beobachtung während einer gewissen Zeitspanne kann erforderlich sein, da häufig erst mehrere Vorfälle zu weiteren Abklärungen oder personalrechtlichen Konsequenzen führen. Wurde die betroffene Person mit dem Inhalt der Akte konfrontiert und wird diese von der Hochschule als für das Personaldossier notwendig empfunden, hat die betroffene Person die Möglichkeit, sich im Rahmen einer Gegendarstellung, die ins Personaldossier Eingang findet, zu äussern.

§ 21 IDG
§ 37 lit. b PG

2.48 Plagiatserkennungssoftware

Siehe unter Auslagerung.
Siehe unter Cloud Computing.

2.49 Private E-Mail-Accounts

Siehe unter Informationssicherheit.

2.50 Private mobile Geräte

Siehe unter Informationssicherheit.

2.51 Prüfungsunterlagen

Siehe unter Auskunft über eigene Personendaten.
Siehe unter Aktenaufbewahrung.

2.52 Pseudonymisierung

Pseudonymisieren bedeutet, Personendaten durch neutrale Angaben, sogenannte «Pseudonyme» zu ersetzen. Namen können durch Buchstaben- oder Zahlenkombinationen ersetzt oder die Daten verschlüsselt werden. Dieser Vorgang erschwert oder verunmöglicht die Identifizierung konkreter Personen.

Eine Pseudonymisierung liegt vor, wenn die Hochschule beispielsweise für ein Forschungsvorhaben eine Liste mit Namen und Adressdaten von Probanden und eine separate Liste mit den Angaben oder Merkmalen der Probanden erstellt. Durch eine weitere Bezugsliste (Konkordanztabelle) wird festgehalten, welche Angaben oder Merkmale welchen Probanden zugeordnet werden können.
Im Hochschulbereich kann eine Zuordnung von Daten zu Personen beispielsweise notwendig sein, wenn einer Patientin oder einem Patienten Forschungsergebnisse mitgeteilt werden sollen. In diesem Fall schützen Pseudonyme die Identität des Betroffenen gegenüber Dritten, nicht jedoch gegenüber der Hochschule.

§ 11 IDG

Siehe unter Anonymisierung.

2.53 Rechtsgrundlagen

Siehe unter Datenschutzrelevante Rechtsgrundlagen Fachhochschule.
Siehe unter Datenschutzrelevante Rechtsgrundlagen Universität.
Siehe unter Gesetzesverzeichnis.

2.54 Sitzungsprotokolle

Siehe unter Auskunft über bei der Hochschule vorhandene Informationen.

2.55 Soziale Medien

Hochschulen, welche Informationen über Whatsapp, Facebook und beispielsweise Blogs auf der Website der Hochschule veröffentlichen, müssen die datenschutzrechtlichen Rahmenbedingungen einhalten. Grundsätzlich bedarf es für die Veröffentlichung der Einwilligung der Studierenden.
Da die Studierenden für die Nutzung sozialer Medien auch eigene Daten bekannt zu geben haben, muss das Einrichten eines «Accounts» freiwillig und müssen die Informationen auch auf andere Weise zugänglich sein.
Der interaktive Austausch ist infolge der heiklen umfassenden Datenerfassung, -speicherung und -weiterbearbeitung durch die Betreiber auf ein Minimum zu beschränken.

Siehe Merkblatt privatim Datenschutzkonforme Nutzung sozialer Medien durch öffentliche Organe

Siehe unter Website.

2.56 Spenderdaten

Siehe unter Bekanntgabe von Personendaten.

2.57 Sponsorendaten

Siehe unter Bearbeiten von Personendaten durch die Hochschule.

2.58 Statistiken

Siehe unter Bearbeiten von Personendaten für nicht personenbezogene Zwecke.
Siehe unter Forschungsvorhaben.

2.59 Studierendendossier

In das Studierendendossier gehören Unterlagen über die Studierenden, die im Zusammenhang mit dem gesetzlichen Auftrag der Hochschule relevant sind.
Studierende haben Anspruch auf Einsicht in ihr Studierendendossier. Sie können die Berichtigung oder Vernichtung unrichtiger Personendaten verlangen.

§ 8 Abs. 1 IDG
§ 20 Abs. 2 IDG
§ 21 IDG

Siehe unter Bearbeiten von Personendaten durch die Hochschule.
Siehe unter Auskunft über eigene Personendaten.

2.60 Titelauskünfte

Siehe unter Bekanntgabe von Personendaten.

2.61 Twitter

Siehe unter Soziale Medien.

2.62 Vernichten elektronischer Akten

Siehe Merkblatt Vernichten elektronischer Daten

Siehe unter Aktenaufbewahrung.

2.63 Verträge mit Geheimhaltungspflichten

Siehe unter Auskunft über bei der Hochschule vorhandene Informationen.

2.64 Videokameras

Überwachung des Hochschulareals
Die Hochschule kann das Hochschulareal mit einer Videoüberwachung ausstatten, wenn beispielsweise Vandalismus oder Diebstahl eine solche erforderlich machen. Datenschutzkonform ist eine Videoüberwachung, wenn sie dazu dient, den Schulbetrieb ohne Störung aufrecht zu erhalten und die Sicherheit nicht mit anderen, weniger in die Persönlichkeitsrechte eingreifenden Mitteln gewährleistet werden kann.
Die Überwachung ist räumlich und zeitlich auf das absolut Notwendige zu beschränken. Die Aufbewahrungsfrist der Aufnahmen muss möglichst kurz sein. Es muss zudem auf die Videoüberwachung hingewiesen werden. Die Modalitäten, insbesondere auch diejenigen der Auswertung, müssen in einem Reglement festgehalten werden.

Überwachung von Hörsälen und Seminarräumen
Mittels Einsatz von Videosupportkameras ist eine Echtzeitüberwachung von Hörsälen und Seminarräumen möglich. Wesentlich ist, dass ein Einsatz solcher Kameras in allen Bereichen verhältnismässig ist. Es muss zwischen den einzelnen Zwecken differenziert und die Rahmenbedingungen müssen diesen angepasst werden.
Videosupportkameras dürfen zum Einsatz kommen, falls diese nur zu Unterstützungszwecken genutzt werden, keine Überwachung von Personen erfolgt, keine Daten gespeichert werden und der Einsatz derselben genügend gekennzeichnet ist.

Verwendung der Videoaufnahmen für die Ahndung von Bagatelldelikten
Die Videoüberwachung durch die Hochschule darf nur zu präventiven Zwecken, also quasi zum Abschrecken vor Straftaten erfolgen. Die Ahndung der Taten selbst ist der Polizei vorbehalten. Besteht ein Verdacht auf das Vorliegen einer Straftat, dürfen die Aufnahmen durch im Reglement bestimmte Mitarbeitende der Schule durchgesehen werden. Sie müssen bei Verdacht auf Straftaten den Strafverfolgungsbehörden übergeben werden. Eine Auswertung von Vorfällen mit Bagatellcharakter und die Ahndung derselben mit den Videoaufnahmen durch die Hochschule selbst sind weder vom Zweck einer Videoüberwachung umfasst noch verhältnismässig.

§ 8 Abs. 1 IDG
§ 12 IDG

Siehe Reglement über die Videoüberwachung und die Videounterstützung an der Universität Zürich

Siehe Leitfaden Videoüberwachung durch öffentliche Organe

2.65 Videos auf der Website

Siehe unter Website.

2.66 Website

Betreiben der Website durch externe Dienstleister
Das Betreiben der Website durch externe Dienstleister ist eine Auslagerung. Mit diesen muss ein gesetzeskonformer Vertrag abgeschlossen werden.

Siehe unter Auslagerung.

Einbinden von Videos
Werden beispielsweise YouTube-Filme auf der Website eingebunden, so ist aus datenschutzrechtlicher Sicht sicherzustellen, dass beim Seitenaufruf keine Daten des

Nutzers ohne sein Einwirken übertragen werden. Dies ist mit der «Zwei-Klick-Lösung» möglich.

Siehe Merkblatt Dienste Dritter auf Websites

Informationen von allgemeinem Interesse
Siehe unter Bekanntgabe von Informationen von allgemeinem Interesse.

Informationen von Mitarbeitenden
Die Hochschule stellt Informationen über Aufbau, Zuständigkeiten und Ansprechpersonen zur Verfügung. Informationen zu den Ansprechpersonen sind im Normalfall Name, Funktion, geschäftliche Telefonnummer und E-Mail-Adresse.
Private Kontaktangaben oder Fotos dürfen nur mit Einwilligung der Betroffenen veröffentlicht werden.

§ 14 IDG

Siehe unter Bekanntgabe von Personendaten.

Informationen von Studierenden
Persönliche Informationen von Studierenden sollten aus Gründen des Persönlichkeitsschutzes nicht auf der Website der Hochschule publiziert werden. Dies selbst dann nicht, wenn die Studierenden eingewilligt haben. Dazu gehören insbesondere Vor- und Familiennamen sowie Hobbies. Fotos von Studierenden dürfen grundsätzlich nur mit deren Einwilligung ins Netz gestellt werden. Ausnahmen gelten, wenn sich die Bekanntgabe dieser Daten auf eine gesetzliche Grundlage stützt wie beispielsweise die Bekanntgabe der Titel.

Siehe unter Bekanntgabe von Personendaten.

Kontaktformular
Bietet die Website der Hochschule ein Kontaktformular oder eine Kontakt-E-Mail-Adresse an, so ist ein Hinweis anzubringen, dass keine vertraulichen Inhalte auf diesem Weg übermittelt werden sollten, es sei denn, der Kommunikationskanal ist verschlüsselt.

Sicherheitsprüfung der Website
Siehe unter Informationssicherheit.

2.67 Weitergabe von Informationen

Siehe unter Amtshilfe.
Siehe unter Auskunft über eigene Personendaten.

Siehe unter Auskunft über bei der Hochschule vorhandene Informationen.
Siehe unter Bekanntgabe von Informationen von allgemeinem Interesse.
Siehe unter Bekanntgabe von Personendaten.
Siehe unter Bekanntgabe von Personendaten für nicht personenbezogene Zwecke.
Siehe unter Forschungsvorhaben.
Siehe unter Zusammenarbeit innerhalb der Hochschule.
Siehe unter Zusammenarbeit mit hochschulexternen Diensten.
Siehe unter Zusammenarbeit mit der Staatsanwaltschaft.

2.68 Zusammenarbeit innerhalb der Hochschule

Werden Informationen über Studierende benötigt, um den gesetzlichen Auftrag zu erfüllen, können diese zwischen allen Beteiligten ausgetauscht werden.

§ 8 Abs. 1 IDG

2.69 Zusammenarbeit mit hochschulexternen Diensten

Hochschulexterne Dienste des privaten Rechts (beispielsweise Aktiengesellschaften, Vereine oder Stiftungen) gelten als öffentliche Organe, soweit sie mit der Erfüllung öffentlicher Aufgaben betraut wurden. Solche Einheiten sind nicht Teil der Hochschule, sondern eigenständige öffentliche Organe, die ebenfalls dem IDG unterstehen. Das IDG ist dann nicht anwendbar, wenn diese am wirtschaftlichen Wettbewerb teilnehmen und dabei nicht hoheitlich handeln. Die Tatsache, dass solche Einheiten mit der Hochschule vertraglich verbunden sind oder von dieser gegründet wurden, hat auf deren Status grundsätzlich keinen Einfluss.
Der Informationsaustausch zwischen der Hochschule und solchen Einheiten stützt sich entweder auf die Bestimmungen der Bekanntgabe oder im Einzelfall auf jene der Amtshilfe.

§ 3 Abs. 1 lit. c IDG
§§ 16 und 17 IDG

Siehe unter Amtshilfe.
Siehe unter Bekanntgabe von Personendaten.

2.70 Zusammenarbeit mit der Staatsanwaltschaft

Verlangt die Staatsanwaltschaft im Rahmen einer Strafuntersuchung gestützt auf eine Verfügung Informationen von der Hochschule, ist bis zum Zeitpunkt der Anklageerhebung und damit der Rechtshängigkeit des Verfahrens vor Gericht das IDG anwend-

bar. Vor der Herausgabe der Informationen muss die Hochschule eine Interessenabwägung vornehmen, das heisst prüfen, ob rechtliche Bestimmungen oder überwiegende öffentliche oder private Interessen der Bekanntgabe entgegenstehen. Weiter muss sie darauf achten, dass das Verhältnismässigkeitsprinzip eingehalten wird. Es dürfen nur diejenigen Informationen bekannt gegeben werden, die die Staatsanwaltschaft für die Aufgabenerfüllung benötigt.

Art. 194 StPO

Siehe unter Amtshilfe.
Siehe unter Bekanntgabe von Personendaten.

3 Gesetzesverzeichnis

	Archivgesetz, LS 170.6
	Archivverordnung, LS 170.61
BiG	Bildungsgesetz, LS 410.1
	Verordnung über Datenbearbeitung im Bildungsbereich (Bildungsdatenverordnung), LS 410.7
GR-KR	Geschäftsreglement des Kantonsrates, LS 171.11
FaHG	Fachhochschulgesetz, LS 414.10
	Finanzreglement der Universität Zürich, LS 415.112
IDG	Gesetz über die Information und den Datenschutz, LS 170.4
IDV	Verordnung über die Information und den Datenschutz, LS 170.41
KV	Kantonsverfassung, LS 101
PG	Gesetz über das Arbeitsverhältnis des Staatspersonals (Personalgesetz), LS 177.10
	Vollzugsverordnung zum Personalgesetz, LS 177.111
PHG	Gesetz über die Pädagogische Hochschule, LS 414.41
PVO-UZH	Personalverordnung der Universität Zürich, LS 415.21
StGB	Schweizerisches Strafgesetzbuch, SR 311.0
StPO	Schweizerische Strafprozessordnung, SR 312.0
UniG	Universitätsgesetz, LS 415.11
VRG	Verwaltungsrechtspflegegesetz, LS 175.2
	Verordnung zum Fachhochschulgesetz, LS 414.101
VZS	Verordnung über die Zulassung zum Studium an der Universität Zürich, LS 415.31

LS	Loseblattsammlung des geltenden kantonalen zürcherischen Rechts
SR	Systematische Sammlung des geltenden Bundesrechts

dsb

datenschutzbeauftragter
kanton zürich

Datenschutzbeauftragter
des Kantons Zürich
Postfach, 8090 Zürich

Telefon 043 259 39 99
datenschutz@dsb.zh.ch

www.datenschutz.ch
twitter.com/dsb_zh