Richtlinie zum Datenschutz an der FHNW

Die vorliegende Richtlinie basiert auf den kantonalen Erlassen der Trägerkantone zum Datenschutz[1], dem Staatsvertrag[2], dem Statut der FHNW[3] und dem Gesamtarbeitsvertrag[4]. Diese sind zu beachten.

1 Geltungsbereich

Diese Richtlinie gilt für das Bearbeiten und die Bekanntgabe von Personendaten durch die FHNW und deren Angehörige.

2 Begriffe

a) Personendaten
Daten, die sich auf bestimmte oder bestimmbare natürliche oder juristische Personen[5] beziehen.

b) Besonders schützenswerte Personendaten
- Daten mit besonderem Gefährdungspotential von Persönlichkeitsrechten oder Grundrechten
- Daten mit Bezug zur Religion, Weltanschauung, politischen oder gewerkschaftlichen Ansichten
- Gesundheits- und Herkunftsdaten
- Daten zu Unterstützungsleistungen (Sozialhilfe, Stipendien)
- Daten aus Straf- oder Verwaltungsverfahren
- Zusammenstellungen von Daten zu einem Persönlichkeitsprofil
- Durch Profiling[6] gewonnene Daten

c) Bearbeiten
Bearbeiten ist jeder Umgang mit Daten, namentlich Erheben, Beschaffen, Aufzeichnen, Sammeln, Aufbewahren, Verwenden, Umarbeiten, Verändern, zugänglich Machen, Bekanntgeben, Veröffentlichen, Archivieren und Vernichten.

[1] Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen des Kantons Aargau (IDAG, SAR 150.700)
Gesetz über die Information und den Datenschutz des Kantons Basel-Stadt (Informations- und Datenschutzgesetz, IDG, SG 153.260)
Gesetz über die Information und den Datenschutz des Kantons Basel-Stadt (Informations- und Datenschutzgesetz, IDG, SGS 162)
Informations- und Datenschutzgesetz des Kantons Solothurn (InfoDG, BGS 114.1)
[2] https://www.fhnw.ch/de/die-fhnw/organisation/media/staatsvertrag-fhnw.pdf
[3] https://www.fhnw.ch/de/die-fhnw/organisation/media/organisationsstatut-fhnw.pdf
[4] https://www.fhnw.ch/de/karriere/welcome-center/attraktive-anstellungsbedingungen/gesamtarbeitsvertrag-fhnw-1.pdf
[5] Juristische Personen sind privat- oder öffentlich-rechtliche Körperschaften sowie Anstalten mit eigener Rechtspersönlichkeit (bspw. Aktiengesellschaften, Vereine oder Stiftungen). Soweit deren Daten nicht öffentlich (insbesondere im Handelsregister) einsehbar sind, untersteht die Bearbeitung dieser Richtlinie. Namentlich Angaben über Finanzkennzahlen oder der Kundenstamm sind vertraulich.
[6] Profiling ist jede (automatisierte) Auswertung von Daten, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen, insbesondere bezüglich Arbeitsleistung, Gesundheit oder Intimsphäre.

3 Voraussetzungen für eine Datenbearbeitung

a) Grundsatz
Personendaten dürfen nur bearbeitet oder weitergegeben werden, wenn dafür eine gesetzliche Grundlage besteht oder dies zur Erfüllung einer rechtlichen Aufgabe erforderlich ist oder mit Einverständnis der betroffenen Personen.

b) Besonders schützenswerte Personendaten
Besonders schützenswerte Personendaten dürfen nur bearbeitet werden, wenn dies zur Erfüllung einer klar umschriebenen gesetzlichen Aufgabe erforderlich ist oder mit Einverständnis der betroffenen Personen.

c) Verhältnismässigkeit und Treu und Glauben
Die Gebote der Verhältnismässigkeit (so wenig wie möglich und so viel wie notwendig) und von Treu und Glauben sind bei jeder Datenbearbeitung zu beachten.

d) Zweckbindung
Personendaten dürfen nur auf Grund des der Beschaffung zu Grunde liegenden Anliegens bearbeitet werden. Über den Zweck sind die betroffenen Personen in Kenntnis zu setzen, soweit dies nicht erkennbar ist.

e) Richtigkeit
Personendaten müssen korrekt und für den Zweck der Bearbeitung vollständig sein.

f) Dauer
Personendaten dürfen nur so lange bearbeitet werden, als dies zur Erfüllung der gesetzlichen Aufgabe notwendig ist. Daten, die nicht gemäss Archivierungsrichtlinie aufbewahrt und archiviert werden müssen, sind zu vernichten.

g) Archivierung
Die Archivierung von Daten erfolgt gemäss Vereinbarung mit den Staatsarchiven der Trägerkantone ausschliesslich im Staatsarchiv des Kantons Aargau. Nähere Informationen enthält die Archivierungsrichtlinie der FHNW.

h) Datensicherheit
Es sind stets angemessene technische und organisatorische Massnahmen gegen eine unbefugte Bearbeitung zu ergreifen. Anhang II dieser Richtlinie regelt die Einzelheiten.

i) Datenschutz-Folgeabschätzung
Besteht bei der Bearbeitung ein erhöhtes Risiko für die Grundrechte der betroffenen Personen, so ist in Absprache mit dem Datenschutzbeauftragten oder der Datenschutzbeauftragten der FHNW eine Datenschutz-Folgeabschätzung vorzunehmen.

4 Bearbeiten von Personendaten durch Dritte

Werden Personendaten durch Dritte verarbeitet, so ist der Datenschutz durch Vereinbarungen, Weisungen oder in anderer Weise sicher zu stellen. Subdelegationen bedürfen der Zustimmung der FHNW oder deren Angehöriger, die auch im Falle der Delegation verantwortlich bleiben.

5 Datenverarbeitung für nicht personenbezogene Zwecke

Anonymisierte Personendaten dürfen für Forschung, Wissenschaft, Planung und Statistik bearbeitet werden, wenn diese nicht mehr für einen personenbezogenen Zweck verwendet werden.

Ergebnisse der Bearbeitung sind so zu verfassen, dass keine Rückschlüsse auf betroffene Personen möglich sind.

6 Bekanntgabe von Personendaten

Die Bekanntgabe von Personendaten bedarf einer Einwilligung der betroffenen Person, einer gesetzlichen Grundlage oder muss zur Erfüllung einer gesetzlichen Aufgabe erforderlich sein. Dabei sind die Grundsätze nach Art. 3 und 4 zu beachten.

Eine Bekanntgabe ins Ausland ist einzig dann zulässig, wenn eine entsprechende Gesetzgebung den Datenschutz im Sinne der vorliegenden Bestimmungen gewährleistet.

7 Bearbeitungsverzeichnisse, Auskunft sowie Einsicht

Jede Person kann schriftlich über die von ihr erhobenen Daten Auskunft und Einsicht verlangen. Das Gesuch ist an die Datenschutzbeauftragen oder den Datenschutzbeauftragten zu richten. Erweisen sich die Daten als unrichtig, sind die Daten zu berichtigen.

Die Datenschutzbeauftragte oder der Datenschutzbeauftragte erteilt schriftlich oder elektronisch Auskunft. Die Auskunft erfolgt innert 30 Tagen seit Eingang des Begehrens. Kann diese Frist nicht eingehalten werden, wird die betroffene Person informiert.

Nähere Informationen über die zu erteilenden Auskünfte und die Datenherausgabe enthält Anhang III.

Jede Organisationseinheit der FHNW führt ein Bearbeitungsverzeichnis der von ihr angelegten Sammlungen von Personendaten. Dieses Bearbeitungsverzeichnis ist auf Nachfrage öffentlich einsehbar.

8 Visuelle Überwachungen

Visuelle Überwachungen, welche eine Personenidentifikation zulassen, dürfen nur mit Zustimmung der Datenschutzbeauftragten oder des Datenschutzbeauftragten vorgenommen werden. Diese Stelle ist für die notwendigen Bewilligungen verantwortlich.

9 Meldung von Verletzungen

Verletzungen von Datenschutzbestimmungen sind der Datenschutzbeauftragten oder dem Datenschutzbeauftragen der FHNW zu melden.

Diese Stelle informiert die von der Verletzung betroffene Person, wenn dies zu ihrem Schutz erforderlich ist.

10 Klassifizierung

Die FHNW klassifiziert ihre Personendaten gemäss Anhang. Die damit verbundenen Sicherheitsanforderungen sind von allen Angehörigen der FHNW einzuhalten.

11 Inkrafttreten

Die vorliegende Richtlinie ersetzt das Datenschutzreglement der FHNW vom 21. März 2023. Sie tritt am 23. April 2024 in Kraft.

Vom Direktionspräsidenten erlassen am 23. April 2024

Die Mitwirkung der MOM erfolgte am 14. Mai 2024

Gültig ab 21. Mai 2024

Anhang I

Klassifizierung von Personendaten

1. Zweck der Datenklassifizierung

Personendaten werden klassifiziert, um unterschiedliche Vertraulichkeitsgrade bzw. die entsprechende Zugangsberechtigung zu definieren.

2. Klassifizierungsstufen

Es existieren folgende Klassifizierungsstufen in der FHNW:

a) öffentlich
b) (FHNW-)intern
c) vertraulich
d) streng vertraulich/geheim

3. Öffentliche Informationen

Personendaten, die für die Öffentlichkeit bestimmt sind und allgemein zugänglich gemacht werden. Diese Daten sind insbesondere auf www.fhnw.ch zugänglich.

4. (FHNW-)Interne Personendaten

Personendaten, deren Kenntnisnahme durch Unberechtigte gegen die Interessen der FHNW oder ihrer Angehörigen verstösst. Diese Daten sind im Inside FHNW allen Angehörigen oder bestimmten Gruppen von Angehörigen zugänglich.

5. Vertrauliche Personendaten

Personendaten, deren Kenntnisnahme durch Unberechtigte der FHNW, ihren Angehörigen oder betroffenen Personen Schaden zufügen kann. Diese Daten sind einem geschlossenen und definierten Personenkreis zugänglich.

6. Streng vertrauliche/geheime Personendaten

a) Personendaten, deren Kenntnisnahme durch Unberechtigte der FHNW, ihren Angehörigen oder betroffenen Personen schweren Schaden zufügen kann. Diese Daten sind einem geschlossenen und definierten Personenkreis zugänglich.
b) Personen, die Zugang zu vertraulichen und streng vertraulichen/geheimen Daten haben sind Geheimnisträger bzw. Geheimnisträgerinnen.
c) Die Geheimnisträger und Geheimnisträgerinnen sind sorgfältig auszuwählen.
d) Die Geheimnisträger, Geheimnisträgerinnen sind zur Geheimhaltung zu verpflichten.

7. FHNW-Daten und Klassifizierung

Die Hochschulen, das Direktionspräsidium, die Vizepräsidien und das Generalsekretariat der FHNW klassifizieren Personendaten gemäss der nachstehenden Tabelle. Sie können Daten höher klassifizieren und weitere Daten klassifizieren.

Art der Personendaten	**Klassifizierung (öffentlich, intern, vertraulich, streng vertraulich/geheim**
Personendaten Mitarbeitende	
Mitarbeitende: - Name, Vorname - FHNW-Mail-Adresse - OE, Arbeitsort - Foto	Soweit eine Einwilligung vorliegt: Intern
Personenprofile von Leitungspersonen und Dozierenden gemäss Beschluss der Direktorinnen und Direktoren auf Hochschulebene, des Vizepräsidenten der Vizepräsidentin für die Services und des Direktionspräsidenten für das Direktionspräsidium und das Generalsekretariat	Öffentlich
Mitarbeitende: - Alle anderen Personendaten (mit Ausnahme der vorgenannten) - Bewerbungsunterlagen - Lohnausweis - Zeugnisse - Korrespondenz	Vertraulich
Besondere Personaldaten Mitarbeitende: - Daten zu Sanktionen, Strafen, Betreibungen, etc. - Arztzeugnisse - Daten zu Massnahmen der Sozialversicherung - Strafregisterauszüge - Daten zu religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Tätigkeiten	Streng vertraulich/geheim

Personendaten Studierende und Weiterbildungsteilnehmende	
- Name, Vorname - FHNW-Mail-Adresse - Studiengang/WB-Angebot - Studienort	Soweit eine Einwilligung vorliegt: Intern
- Alle anderen Personendaten (mit Ausnahme der vorgenannten) - Zulassungsunterlagen - Leistungsausweise, Prüfungsergebnisse etc. - Korrespondenz	Vertraulich
Besondere Personaldaten Studierende und Teilnehmende Weiterbildungsprogramme - Daten zu Sanktionen, Vorstrafen, Betreibungen - Arztzeugnisse - Daten zu religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Tätigkeiten	Streng vertraulich/geheim
Übrige Personendaten	
Besonders schützenswerte Personendaten, insbesondere in Forschungs- und Dienstleistungsprojekten	Streng vertraulich/geheim
Übrige Personendaten in Forschungs- und Dienstleistungsprojekten	Vertraulich
Forschungsdaten abgeschlossene Projekte	Öffentlich (anonymisiert) sofern keine Geheimhaltung
Ausländische Exchange-Studierende	Analog Studierende FHNW
Weitere Personendaten - Adresslisten, Personenverzeichnisse etc.	Vertraulich

Anhang II

Anforderungen an technische und organisatorische Massnahmen zum Schutz von Personendaten

1.
Jede Hochschule, das Direktionspräsidium, die Vizepräsidien und das Generalsekretariat bestimmen eine*n Informationsschutzbeauftragte*n. Diese*r führt das Bearbeitungsverzeichnis gemäss Ziff. 7 der Richtlinie. Das Bearbeitungsverzeichnis enthält die Sammlung der bearbeiteten Personendaten und die für die Datenbearbeitung verantwortlichen Personen.

Die verantwortliche Person - in Absprache mit dem/der Informationsschutzbeauftragten der Hochschule und der verantwortlichen Person in der CIT - sowie der Auftragsbearbeiter, die Auftragsbearbeiterin müssen technische und organisatorische Massnahmen treffen, damit die bearbeiteten Daten ihrem Schutzbedarf entsprechend:

a) nur Berechtigten zugänglich sind (Vertraulichkeit);
b) verfügbar sind, wenn sie benötigt werden (Verfügbarkeit);
c) nicht unberechtigt oder unbeabsichtigt verändert werden (Integrität);
d) nachvollziehbar bearbeitet werden (Nachvollziehbarkeit).

2.
Um die Vertraulichkeit zu gewährleisten, müssen der oder die Verantwortliche und der Auftragsbearbeiter oder die Auftragsbearbeiterin geeignete Massnahmen treffen, damit:
a) berechtigte Personen nur auf diejenigen Personendaten Zugriff haben, die sie zur Erfüllung ihrer Aufgaben benötigen (Zugriffskontrolle);
b) nur berechtigte Personen Zugang zu den Räumlichkeiten und Anlagen haben, in denen Personendaten bearbeitet werden (Zugangskontrolle);
c) unbefugte Personen automatisierte Datenbearbeitungssysteme nicht mittels Einrichtungen zur Datenübertragung nutzen können (Benutzerkontrolle).

3.
Um die Verfügbarkeit und Integrität zu gewährleisten, müssen der oder die Verantwortliche und der Auftragsbearbeiter oder die Auftragsbearbeiterin geeignete Massnahmen treffen, damit:
a) unbefugte Personen Datenträger nicht lesen, kopieren, verändern, verschieben, löschen oder vernichten können (Datenträgerkontrolle);
b) unbefugte Personen Personendaten im Speicher nicht speichern, lesen, ändern, löschen oder vernichten können (Speicherkontrolle);
c) unbefugte Personen bei der Bekanntgabe von Personendaten oder beim Transport von Datenträgern Personendaten nicht lesen, kopieren, verändern, löschen oder vernichten können (Transportkontrolle);
d) die Verfügbarkeit von Personendaten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können (Wiederherstellung);
e) alle Funktionen des automatisierten Datenbearbeitungssystems zur Verfügung stehen (Verfügbarkeit), Fehlfunktionen gemeldet werden (Zuverlässigkeit) und gespeicherte Personendaten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität);

f) Betriebssysteme und Anwendungssoftware stets auf dem neusten Sicherheitsstand gehalten und bekannte kritische Lücken geschlossen werden (Systemsicherheit).

4.
Um die Nachvollziehbarkeit zu gewährleisten, müssen der oder die Verantwortliche und der Auftragsbearbeiter oder die Auftragsbearbeiterin geeignete Massnahmen treffen, damit:

a) überprüft werden kann, welche Personendaten zu welcher Zeit und von welcher Person im automatisierten Datenbearbeitungssystem eingegeben oder verändert werden (Eingabekontrolle);
b) überprüft werden kann, wem Personendaten mit Hilfe von Einrichtungen zur Datenübertragung bekanntgegeben werden (Bekanntgabekontrolle);
c) Verletzungen der Datensicherheit rasch erkannt (Erkennung) und Massnahmen zur Minderung oder Beseitigung der Folgen ergriffen werden können (Beseitigung).

5. Protokollierung

a) Der oder die Verantwortliche und sein oder ihr Auftragsbearbeiter oder Auftragsbearbeiterin protokollieren bei der automatisierten Bearbeitung von Personendaten zumindest das Speichern, Verändern, Lesen, Bekanntgeben, Löschen und Vernichten der Daten.
b) Die Protokollierung muss Aufschluss geben über die Identität der Person, die die Bearbeitung vorgenommen hat, die Art, das Datum und die Uhrzeit der Bearbeitung sowie gegebenenfalls die Identität der Empfängerin oder des Empfängers der Daten.
c) Die Protokolle müssen während mindestens einem Jahr getrennt vom System, in welchem die Personendaten bearbeitet werden, aufbewahrt werden. Sie dürfen ausschliesslich den Organen und Personen zugänglich sein, denen die Überprüfung der Anwendung der Datenschutzvorschriften oder die Wahrung oder Wiederherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Daten obliegt, und dürfen nur für diesen Zweck verwendet werden.

Anhang III

Modalitäten des Auskunftsrechts

1. Zu erteilende Informationen

Die betroffene Person erhält diejenigen Informationen, die erforderlich sind, damit sie ihre Rechte nach dieser Richtlinie geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist. In jedem Fall werden ihr, folgende Informationen mitgeteilt:

a) die Kontaktdaten des bzw. der Verantwortlichen
b) die bearbeiteten Daten
c) der Bearbeitungszweck
d) die Aufbewahrungsdauer der Daten
e) die verfügbaren Angaben über die Herkunft der Daten
f) gegebenenfalls die Bekanntgabe an Dritte

2. Auftragsbearbeitung

Der Verantwortliche oder die Verantwortliche bleibt auskunftspflichtig, wenn er oder sie Personendaten von einem Auftragsbearbeiter oder einer Auftragsbearbeiterin bearbeiten lässt.

3. Recht auf Datenherausgabe oder -übertragung

Die betroffene Person hat das Recht, die Herausgabe von selber eingegebenen Personendaten in einem gängigen Format zu verlangen, wenn:

a) die Daten automatisiert bearbeitet werden und
b) die Daten mit der Einwilligung der betroffenen Person oder in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrages zwischen ihr und der FHNW bearbeitet werden.

Als selber eingegebene Personendaten gelten neben willentlich zur Verfügung gestellten Daten auch solche, die über das Verhalten im Rahmen der Nutzung eines Dienstes oder Geräts erhoben werden.

Die betroffene Person kann verlangen, dass die Personendaten einer anderen Verantwortlichen übertragen werden, wenn die vorstehenden Voraussetzungen erfüllt sind und dies keinen unverhältnismässigen Aufwand verursacht.

Die Herausgabe der Daten erfolgt kostenlos. Verursacht die Herausgabe einen grossen Aufwand, kann eine angemessene Entschädigung verlangt werden.

4. Identifikation

Der oder die Datenschutzbeauftragte sorgt für die Identifikation der betroffenen Person. Diese hat dabei mitzuwirken.

5. Einschränkungen des Auskunftsrechts der Datenherausgabe

Das Auskunftsrecht und die Datenherausgabe können eingeschränkt werden, wenn dies gesetzlich vorgesehen oder zur Wahrung von überwiegenden öffentlichen oder überwiegenden privaten Interessen erforderlich ist. Der Datenschutzbeauftragte begründet die Einschränkungen gegenüber der betroffenen Personen.