Erklärung zur datenschutzgerechten Nutzung der hochschuleigenen Software SoSci Survey für Onlinebefragungen im Rahmen von Forschung und Lehre durch Dozenten

Aus datenschutzrechtlicher Sicht geht es bei Online-Befragungen in erster Linie darum, das Grundrecht der Betroffenen auf Schutz ihrer personenbezogenen Daten, Art. 8 der Charta der Grundrechte der Europäischen Union,[1] zu beachten. Die einschlägigen Datenschutzvorschriften der DSGVO[2] werden im folgenden 1. Abschnitt überblickshaft dargestellt. In Zweifelsfällen oder bei Unsicherheiten sollten Sie sich bei den Datenschutzbeauftragten der Hochschule Niederrhein erkundigen.

Die hinsichtlich der inhaltlichen Gestaltung ihrer Befragung und deren Durchführung (inkl. Auswertung und Veröffentlichung) zu beachtenden datenschutzrechtliche Vorgaben der DSGVO werden im Abschnitt 2 in Form einer Checkliste abgefragt. Wenn Sie diese vollständig und plausibel ausfüllen und die geforderten Anlagen beifügen, eine Kopie ihrer Schulungsbescheinigung gemäß Präsidiumsbeschluss vom 16.09.2014 vorlegen sowie die Haftungserklärung unter 3. unterschreiben, können Sie die hochschuleigene Software SoSci Survey für ihre Onlinebefragung im Rahmen von Forschung und Lehre durch Dozenten benutzen.

Für Zwecke der Verwaltung oder Studierende steht die software nicht zur Verfügung.

1. Überblick: datenschutzrechtliche Grundlagen

Bei jeder Befragung sind folgende datenschutzrechtliche Grundprinzipien der DSGVO zu beachten:[3]

a) Rechtsgrundlage Einwilligung

Befragungen stellen aus datenschutzrechtlicher Sicht eine **Datenerhebung** - das Beschaffen von Daten über die betroffene Person - dar (Art. 4 Nr. 1 und 2 DSGVO).

Soweit keine gesetzliche Grundlage besteht und auch keine Rechtsgrundlage durch die Hochschule selbst geschaffen wird, aus der sich eine Pflicht zur Teilnahme an Umfragen ergeben könnte, ist die Teilnahme an der Befragung grundsätzlich **freiwillig** (sog. Verbot der Datenerhebung mit Erlaubnisvorbehalt, Art. 6 Abs. 1 und 9 Abs. 1 DSGVO), erfordert also eine **Einwilligung** des Betroffenen (Art. 4 Nr. 11 DSGVO). Bei Mitarbeitenden der hsnr

[1] Text: https://dejure.org/gesetze/GRCh/8.html
[2] Text: https://dsgvo-gesetz.de/
[3] Es handelt sich um Hinweise zu den häufigsten Fragestellungen.

besteht bei Erfragung von subjektiven Einschätzungen und Bewertungen des Arbeitsumfeldes generell auch keine arbeitsvertragliche Verpflichtung zur Teilnahme.[4]

Eine **Einwilligung** liegt nach Art. 4 Nr. 11 DSGVO nur dann vor, wenn folgende Voraussetzungen gegeben sind:

- **Freiwilligkeit**
- **Informiertheit** (für den bestimmten Fall)
- **Ausdrücklichkeit** (durch unmissverständliche Willensbekundung)
- **Widerrufbarkeit (für die Zukunft)**Freiwilligkeit

Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Die Befragten sind ausdrücklich auf die **Freiwilligkeit** ihrer Mitwirkung **hinzuweisen**. Zudem sind die Befragten darüber aufzuklären, dass sich im Falle der Verweigerung einer Einwilligung **keine nachteiligen Folgen** für sie persönlich ergeben - dies ist gerade im Falle von Bedienstetenbefragungen durch den Arbeitgeber/Dienstherrn bedeutsam. Denn eine Einwilligung kann aus datenschutzrechtlicher Sicht nur dann wirksam abgelehnt oder akzeptiert werden, wenn sich der Betroffene nicht in einer Situation befindet, in welcher er faktisch dazu genötigt wird, sich mit der Erhebung der jeweils verlangten Daten einverstanden zu erklären. In dem speziellen Fall von Bedienstetenbefragungen sind darüber hinaus die **Personalräte** zu beteiligen. Von Freiwilligkeit kann zudem nur dann ausgegangen werden, wenn die einwilligende Person die nach **Art. 13/14 DSGVO erforderlichen Informationen** erhalten hat (informierte Einwilligung).

Sollen zudem **besondere Kategorien personenbezogener Daten** verarbeitet werden, muss sich die Einwilligung nach Art. 9 Abs. 2 lit a DSGVO auch hierauf beziehen, da gerade diese unter einem besonderen Schutz stehen.

Der Verantwortliche ist nach Art. 7 Abs. 1 DSGVO gezwungen **nachzuweisen**, dass die betroffene Person in die Verarbeitung ihrer Daten eingewilligt hat. Dies ist stellt soci survey durch einen elektronische Protokollierung sicher. Sind noch weitere Sachverhalte in der Einwilligung aufgeführt, so sind sie klar voneinander abzugrenzen (Koppelungsverbot, Art. 7 Abs.2 DSGVO).

Schließlich ist zu beachten, dass die betroffene Person das Recht hat, ihre Einwilligung jederzeit zu **widerrufen** (Art. 7 Abs. 3 DSGVO).

[4] LDI NRW, 18. Tätigkeitsbericht (2007), S. 131.

b) Verarbeitungsgrundsätze

Entscheidend ist aber nicht allein die rechtliche Erlaubnis zur Datenverarbeitung, sondern auch die Art und Weise ihrer Durchführung. Datenverarbeitungsvorgänge **müssen**:

- die **datenschutzrechtlichen Grundsätze**, Art. 5 DS-GVO, beachten: Rechtmäßig = Rechtsgrundlage, Transparenz, Zweckbindung, Datenminimierung, Speicherbegrenzung, Rechenschaftspflicht, …
- die **Betroffenenrechte**, die **Informationspflichten** (bei Erhebung und Zweckänderung, Art. 13/14 DSGVO) und das **Widerspruchsrecht** (Art. 21 Abs. 6) erfüllen
- „geeignete“ **technische und organisatorische Maßnahmen** (insbesondere Artt. 25, 30, 32 DSGVO) sicherstellen.

Nur dann, wenn diese Anforderungen erfüllt werden, können die Betroffenen auf die Wahrung ihrer Rechte vertrauen. Daher schreibt § 5 Abs. 2 DSGVO zwingend vor, dass

• der Verantwortliche für die Einhaltung der Grundsätze die **Verantwortung** trägt und

• er jederzeit imstande sein muss, dies **nachzuweisen („Rechenschaftspflicht**“).

2. Checkliste für die geplante Umfrage

Aus der Rechenschaftspflicht in Art. 5 Abs. 2 DS-GVO erwachsen i.E. nachfolgend abgefragte **Nachweispflichten (b-l).**

a) Zuvor bitten wir Sie zu unserem besseren Verständnis ihres Gesamtvorhabens **in Grundzügen den Datenfluss in Ihrem Projekt kurz zu beschreiben**

Was ist Ziel Ihres Projekts?

Sind externe Partner beteiligt?

Welche Rolle hat die Onlinebefragung im Rahmen Ihres Projekts?

Woher bekommen Sie die Kontaktdaten der zu Befragenden?

Wonach fragen Sie (Kategorien der zu erhebenden Daten)?

Wie und von wem werden die Daten ausgewertet?

Wer hat Zugriff auf die Daten (auch interne Mitarbeiter?

Ist eine Veröffentlichung geplant?

Wann sollen die Daten gelöscht werden?

b) Wer ist für das Forschungsprojekt Verantwortlich und Ansprechpartner

- Verantwortlicher für das Verfahren (Name, Anschrift, Kontaktdaten):

- Name und Kontaktdaten eines Ansprechpartners:

c) Aufklärung und Einwilligung

- Bitte fügen Sie dieser Unterlage einen Ausdruck des Anschreibens mit Aufklärung und Einwilligung bei. Ist als Anlage Nr.: ☐ beigefügt.

In dem **Anschreiben** (separat oder als Eingangsteil des Fragebogens) sind der verantwortliche Träger und Leiter des Forschungsvorhabens zu benennen und die Art und Weise der Datenverarbeitung zu erklären (Informiertheit). Es sind Anlass und Ziel der Befragung darzulegen und die Teilnehmenden über den Zweck der Befragung sowie über eine etwa beabsichtigte Übermittlung von personenbezogenen Daten an Kooperationspartner inkl. deren Aufgaben aufzuklären. Es muss ersichtlich sein, welche konkrete Nutzung der Daten geplant ist. Sollen besondere Arten personenbezogener Daten erhoben, verarbeitet oder genutzt werden, muss sich die Einwilligungserklärung ausdrücklich auf diese Daten beziehen (Art. 9 Abs. 2 lit a DSGVO). Weiter sind die Freiwilligkeit der

Teilnahme sowie die Folgenlosigkeit ihrer Verweigerung deutlich zu machen und der Zeitpunkt der Löschung bzw. Vernichtung der psb Daten festzulegen. Schließlich ist darauf hinzuweisen, dass jederzeit ein Widerruf der Einwilligung möglich ist, dieser aber die Rechtmäßigkeit einer bis zum Widerruf erfolgten Verarbeitung seiner psb nicht beeinträchtigt (Art. 7 Abs. 3 S. 2 DSG-GVO). Datenschutzrechtlich irrelevant sind Befragung, die einen Personenbezug von vornherein ausschließen.

Handreichung: Einwilligung auf der Website der Datenschutzbeauftragten der HSNR mit Checkliste

d) Informationen zur Datenerhebung sowie den Betroffenenrechten

- Bitte fügen Sie dieser Unterlage einen Ausdruck der **Informationen zur Datenerhebung sowie den Betroffenenrechten** bei. Ist als Anlage Nr.: ☐ beigefügt.

Handreichung: Einwilligung auf der Website der Datenschutzbeauftragten der HSNR

e) Verzeichnis der Verarbeitungstätigkeiten

- Bitte fügen Sie dieser Unterlage ein vom für das Forschungsprojekt Verantwortlichen unterschriebenes **Verzeichnis der Verarbeitungstätigkeiten** bei. Ist als Anlage Nr.: ☐ beigefügt.

Handreichung: Musterformular Verzeichnis der Verarbeitungstätigkeiten mit Erläuterungen auf der Website der Datenschutzbeauftragten der HSNR

f) Online-Fragebögen

- Bitte eine Ausdruck des Fragebogens dieser Unterlage beifügen. Ist als Anlage Nr.: ☐ beigefügt.

- Bitte erläutern und bestätigen Sie dabei ausdrücklich, dass die inhaltliche Ausgestaltung der Fragebögen den Vorgaben der Datenminimierung (Art. 5 Abs. 1 lit. c; Art. 25, 89 Abs. 1 DS-GVO) entsprechen.

Dieser Grundsatz verlangt zunächst, dass **Vertraulichkeit und Anonymität** gewahrt bleiben.

Als erstes ist zu prüfen, ob der angestrebte Forschungszweck nicht schon mit **anonymisierten Daten** erreicht werden kann oder, ob die Daten nicht im Laufe der Forschungsprojekts anonymisiert werden können. Soweit der Forschungszweck mit anonymen Daten erreicht werden kann, wäre die Verarbeitung nicht-anonymisierter Daten ein Verstoß gegen den Grundsatz der Datenminimierung (Art. 89 Abs. 1 S. 4 DSGVO), weil sie nicht „auf das notwendige Maß beschränkt“ worden ist.

Wird mit von vornherein anonymen Daten gearbeitet? Bitte dann hier ankreuzen ☐

Wird nicht mit von vornherein anonymen Daten gearbeitet, dann hier bitte begründen, warum dies angesichts des Forschungszwecks nicht möglich ist.

Werden die Daten im Lauf des Forschungszwecks anonymisiert? Bitte dann hier ankreuzen ☐

Werden die Daten nicht im Lauf des Forschungszwecks anonymisiert, dann hier bitte begründen, warum dies angesichts des Forschungszwecks nicht möglich ist.

Bitte beachten Sie, dass Sie bei anonymen Daten auch die Möglichkeit einer (Re-) Identifizierung der an der Umfrage teilnehmenden Betroffenen vermeiden müssen. Hierfür genügt es meist nicht, wenn nur eine namentliche Nennung der Befragten unterbleibt (Formale Anonymisierung). Ein Personenbezug ergibt sich oft auch durch **Kombination mehrerer Antworten**. Dem kann z.B. durch Abfrage von aggregierten Größen begegnet werden. Auch bei der Auswertung muss gewährleistet sein, dass mit **vorhandenem Zusatzwissen** keine Rückschlüsse auf die Identität des Befragten gezogen werden können. Es empfiehlt sich daher, möglichst geschlossene Fragestellungen und keine offenen zu verwenden. Geschlossene Fragen sind solche, bei denen die Antwortmöglichkeiten vorgegeben sind (z.B. Alternativfragen). Die auf offene Fragen frei formulierten Antworten müssen unter Umständen erst von unerwünschtem Personenbezug befreit und zusammengefasst werden. Um bei der Auswertung zu gewährleisten, dass auch bei vorhandenem Zusatzwissen keine Rückschlüsse auf die Identität Betroffener gezogen werden können, empfiehlt sich, dass die kleinste statistische Auswertungsgröße 3 grundsätzlich nicht unterschreitet.

Als zweites ist zu prüfen, ob der angestrebte Forschungszweck nicht schon mit **pseudonymisierten Daten** erreicht werden kann oder, ob die Daten nicht im Laufe der Forschungsprojekts pseudonymisiert werden können. Soweit der Forschungszweck mit pseudonymen Daten erreicht werden kann, wäre die Verarbeitung nicht-pseudonymisierter Daten ein Verstoß gegen den Grundsatz der Datenminimierung, weil sie nicht „auf das notwendige Maß beschränkt“ worden ist.

Pseudonymisierung (Definition in Art. 4 Nr.5 DSGVO) setzt eine Verarbeitung personenbezogener Daten in der Art voraus, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. [5]

Wird mit von vornherein pseudonymen Daten gearbeitet? Bitte dann hier ankreuzen: ☐

Wird nicht mit von vornherein pseudonymen Daten gearbeitet, dann hier bitte begründen, warum dies angesichts des Forschungszwecks nicht möglich ist.

Werden die Daten im Lauf des Forschungszwecks pseudonymisiert? Bitte dann hier ankreuzen: ☐

Werden die Daten nicht im Lauf des Forschungszwecks pseudonymisiert, dann hier bitte begründen, warum dies angesichts des Forschungszwecks nicht möglich ist.

[5] Zu Verschlüsselungstechniken: Bundesamt für Sicherheit in der Informationstechnik (BSI), Faltblatt „Sicherheit durch Verschlüsselung", www.bsi-fuer-buerger.de

Wenn eine Pseudonymisierung von vornherein oder im Lauf des Forschungsprojekts erfolgt, **erläutern Sie bitte hier die Technik Ihrer Pseudonymisierung:**

Hinweis zur Erläuterung einer Pseudonymisierung. Hier stellen sich folgende **Fragen**:

- ob die identifizierenden Daten durch eine Nummer/Code ersetzt werden können,
- wer über die Zuordnungstabellen bzw. das Verschlüsselungs-verfahren verfügen soll, (nicht der Forscher, das wäre nur eine Maßnahme der Datensicherheit)
- wer das Pseudonym generieren soll,
- ob ein Reidentifizierungsrisiko ausgeschlossen werden kann,
- wer und unter welchen rechtlichen Voraussetzungen Pseudonym und Identifikations-daten zusammenführen darf,
- Pseudonym und Identifikationsdaten sind getrennt vom Fragebogen zu speichern und nur bei Erforderlichkeit zu nutzen. Anderenfalls sind sie unverzüglich zu vernichten.
- Schließlich ist - wie beim anonymisierten Verfahren - zu gewährleisten, dass – insbesondere auch im Rahmen der Auswertung (!) - ein Rückschluss auf bestimmte Einzelpersonen, sei es auf Grund der Fragestellung oder durch vorhandenes Zusatzwissen, möglichst vermieden wird. **Beispiel**: Werden Fragebögen mit einer Kennzahl versehen, um genaue Aussagen bezogen auf einen räumlichen Bereich zu erhalten (z.B. Stadtteil-Kennzahl), so muss gewährleistet sein, dass die räumliche Zuordnung so groß ist, dass sie nicht zu einer Re-Individualisierbarkeit führen kann. Gehen Sie bitte in Ihrer Erläuterung ausdrücklich darauf ein, dass bei der Auswertung eine Re-Identifizierung auch mit Zusatzwissen nicht möglich ist.

Sonderproblem: Rückantwort (Adressbogen)

Falls vorgesehen, erläutern Sie bitte die wissenschaftliche Notwendigkeit der Rückantwort und die Technik der Re-Identifizierung der pseudonymisierten Daten:

Der Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c; Art. 25, 89 Abs. 1 DS-GVO) verlangt über die Vertraulichkeit hinaus, dass **nur die für die für den Forschungszweck erforderlichen Daten erhoben werden**. Die Verarbeitung von Daten, muss dem Zweck angemessen und auf das für die Erreichung der Zwecke der Verarbeitung notwendige Maß beschränkt sein.

Die Erhebung und Verarbeitung **unnötiger Daten** gilt es also zu vermeiden. So ist die Namenserfassung der Befragten für Befragungen zu rein statistischen Zwecken überflüssig. Nur wenn der spätere Kontakt zu den Befragten unumgänglich ist - so z.B. bei Langzeitstudien, die wiederholte Befragungen oder Erhebungen über eine bestimmte Person erfordern -, dürfen Angaben, die eine Identifizierung der hinter pseudonymisierten Daten stehenden Person ermöglichen, erhoben und zeitweise gespeichert werden.

Die Datenverarbeitung ist von vorneherein an die festgelegten Forschungszwecke auszurichten **(Zweckbindung).** . Es dürfen nur solche Fragen gestellt werden, die **für das Befragungsziel notwendig** sind. Werden bei Gelegenheit einer Erhebung zusätzlich Daten erfasst, die nicht ausdrücklich Untersuchungs- bzw. Erhebungsgegenstand sind, ist ihre Erhebung rechtswidrig. Deshalb ist auf abrundende und lediglich wünschenswerte Fragen zu verzichten; Fragen sollten sich auf die Punkte beschränken, die zur Zweckerreichung erforderlich sind. Werden bei längeren Befragungen **Kontrollfragen** gestellt, die vorangegangene Antworten auf ihrer Wahrhaftigkeit überprüfen sollen, können diese als datenschutzrechtlich unbedenklich eingestuft werden, wenn sie methodisch zutreffend eingesetzt und von dem Zweck der Untersuchung abgedeckt sind.

Bitte benennen Sie ihre Verarbeitungsziele und **begründen sie die Erforderlichkeit** der erhobenen Daten zur Erreichung dieser Zwecke. Es ist zulässig, dass sie nicht jedes Datum einzeln aufführen, sondern die Daten zu sinnvollen Kategorien zusammenfassen.

g) Berechtigungskonzept

Wenn auf die erhobenen Daten von verschiedenen Personen zugegriffen werden soll, muss festgelegt werden, wer wann auf was zugreifen darf (sog. Berechtigungskonzept) und es ist zu protokollieren (wer wann zu welchen Zwecken auf welche Daten zugegriffen hat). Hierzu gehört auch festzulegen, wer für Änderungen der Berechtigungen zuständig ist. Bitte erläutern Sie ihr Berechtigungskonzept und die Vorkehrungen Ihrer Protokollierung von Verarbeitungszugriffen.

h) Löschkonzept

Speicherbegrenzung (Art. 5 Abs. 1 lit. e DS-GVO): Es ist zu erläutern, dass die Löschung der erhobenen und verarbeiteten Daten zum frühestmöglichen Zeitpunkt und Berücksichtigung von notwendigen Forschungszwecken wie eventuellen Rückantworten, Kontrollfragen, Folgeberatung etc. erfolgt. Fragebögen sind nach Erreichung des Ziels der Befragung und Auswertung des Ergebnisses zu **vernichten**; sofern nicht - entsprechend einem dem Betroffenen im Rahmen der Einwilligung transparent gemachten Befragungsplan - in einer Folgebefragung die zuvor ermittelten Daten personengenau zugeordnet werden müssen oder noch Kontakt zum Befragten aufgenommen werden muss. Im Zuge der Auswertung gespeicherte Daten, die nicht unmittelbar zum Auswertungsergebnis gehören, sind zu **löschen.**

Bitte erläutern:

i) Datenschutz-Folgenabschätzung

Ein Datenschutz-Folgenabschätzung zwingt dazu zu überlegen, wo die Risiken für Datenmissbrauch etc. liegen und die diesbezüglichen Feststellungen zu dokumentieren. Sie bildet die Basis der einzurichtenden technisch-organisatorischen Maßnahmen (unten l.).

(**Handreichung:** Nachweispflicht Anlage Datenschutzfolgenabschätzung)

Eine **Datenschutz-Folgenabschätzung** muss gemäß Art. 35 Abs. 7 DS-GVO zumindest die nachfolgend genannten Punkte beinhalten:

I. eine systematische Beschreibung
   - o der geplanten Verarbeitungsvorgänge,
   - o der Zwecke der Verarbeitung,
   - o ggfs. die vom Verantwortlichen verfolgten berechtigten Interessen,

II. eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck,

Die Aufgaben I. und II. haben Sie oben schon erledigt, so dass nur noch folgende Schritte zu erledigen sind:

III. eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen,

IV. die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren,

- durch die der Schutz personenbezogener Daten sichergestellt und
- der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird,
- wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

Die Aufgabe IV. müssen Sie unten unter j) nur für den von Ihnen selbst durchgeführten Teil der Datenverarbeitung nicht aber für die Nutzung von soci survey erledigen. Hier ist in Abstimmung mit der KIS die Datensicherheit sichergestellt. Hier führen Sie also nur eine Bewertung der Risiken ihres Forschungsprojekts für die Rechte und Freiheiten der betroffenen Personen durch.

j) Beschreibung der technisch-organisatorischen Maßnahmen (Art. 30 Abs. 1 lit. g DS-GVO)

Auf der Grundlage der analysierten Risiken in der Datenschutzfolgeabschätzung wird festgelegt, welche technisch-organisatorischen Schutzmaßnahmen erforderlich sind. Der Verarbeitung im System soci survey selbst können Sie außen vor lassen. Hier werden seitens der Hochschule die erforderlichen Maßnahmen sichergestellt.

(**Hilfestellung:** VVT und Erläuterung)

Maßnahmenbereiche, die sich aus Art. 32 Abs. 1 DS-GVO ergeben:

1) Maßnahmen zur Anonymisierung/Pseudonymisierung personenbezogener Daten

- ○ Die Daten werden anonymisiert, siehe Erläuterungen oben
- ○ Die Daten werden pseudonymisiert, siehe Erläuterungen oben
- ○ Die Daten werden nicht anonymisiert / pseudonymisiert, siehe Erläuterungen oben

2) Maßnahmen zur Gewährleistung der Vertraulichkeit der Systeme und Dienste

A. Zugangskontrolle

Die Zugangskontrolle soll verhindern, dass Unbefugte Zugang zu Verarbeitungsanlagen erhalten, mit denen die Verarbeitung durchgeführt wird. Zum Beispiel:

- Alarmanlage
- Chipkarten-/Transponder-Schließsystem
- Abschließbare Serverschränke
- Sorgfältige Auswahl Reinigungspersonal
- Sicherheitsschlösser

B. Datenträgerkontrolle

Die Datenträgerkontrolle soll verhindern, dass Unbefugte Datenträger lesen, kopieren, verändern oder löschen können. Zum Beispiel:

- Sichere Aufbewahrung von Datenträgern
- Einrichtungen von Standleitungen beziehungsweise VPNTunneln
- Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- Verschlüsselung von (mobilen) Datenträgern
- Ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)

• Einsatz von Aktenvernichtern beziehungsweise Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
• Protokollierung der Vernichtung

C. Speicherkontrolle

Die Speicherkontrolle soll verhindern, dass unbefugte von gespeicherten personenbezogenen Daten Kenntnis nehmen sowie diese eingeben, verändern und löschen können. Zum Beispiel:

• Festlegung von Berechtigungen in den IT-Systemen
• Differenzierte Berechtigungen für lesen, löschen und ändern
• Differenzierte Berechtigungen für Daten, Anwendungen und Betriebssystem
• Verwaltung der Rechte durch Systemadministratoren
• Anzahl der Administratoren auf das „Notwendigste“ reduziert
• Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
• Protokollierung von Zugriffen auf Anwendungen

D. Benutzerkontrolle

Die Benutzerkontrolle soll verhindern, dass Unbefugte automatisierte Verarbeitungssysteme mit Hilfe von Datenübertragung nutzten können. Zum Beispiel:

• Festlegung zugangsberechtigter Mitarbeiter
• Erstellen von Benutzerprofilen
• Passwortvergabe
• Authentifikation mit Benutzername/Passwort
• Regelmäßige Kontrolle von Berechtigungen
• Sperrung von Berechtigungen ausscheidender Mitarbeiter
• Zuordnung von Benutzerprofilen zu IT-Systemen
• Einsatz von Verschlüsselungs-Technologie
• Einsatz von Anti-Viren-Software

E. Zugriffskontrolle

Die Zugriffskontrolle soll gewährleisten, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben. Zum Beispiel:

- Festlegung von Berechtigungen in den IT-Systemen
- Differenzierte Berechtigungen für lesen, löschen und ändern
- Differenzierte Berechtigungen für Daten, Anwendungen und Betriebssystem
- Verwaltung der Rechte durch Systemadministratoren
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Protokollierung von Zugriffen auf Anwendungen

F. Übertragungskontrolle

Die Übertragungskontrolle soll gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können. Zum Beispiel:

- Einrichtungen von Standleitungen beziehungsweise Verschlüsselungs-Technologien
- Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
- Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung beziehungsweise vereinbarter Löschfristen

G. Transportkontrolle

Die Transportkontrolle soll gewährleisten, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden. Zum Beispiel:

- Einrichtungen von Standleitungen beziehungsweise Verschlüsselungs-Technologien

H. Wiederherstellbarkeit

Die Wiederherstellbarkeit soll gewährleisten, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können. Zum Beispiel:

- Erstellen eines Backup- & Recoverykonzepts
- Festplattenspiegelung nach Vereinbarung mit dem Auftraggeber
- Testen von Datenwiederherstellung
- Erstellen eines Notfallplans

I. Zuverlässigkeit

Die Zuverlässigkeit soll gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden. Zum Beispiel:

- Unabhängig voneinander funktionierende Systeme
- Automatisierte Meldung von Fehlfunktionen
- Anti-Viren-Schutz

J. Datenintegrität

Die Datenintegrität soll gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können. Zum Beispiel:

- Erstellen eines Backup- & Recoverykonzepts

K. Verfügbarkeitskontrolle

Die Verfügbarkeitskontrolle soll gewährleisten, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind. Zum Beispiel: :

- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte in Serverräumen
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Erstellen eines Notfallplans

k) Meldung von Datenschutzverstößen

Datenpannen müssen zukünftig binnen 72 Stunden der Aufsichtsbehörde gemeldet werden und die Betroffenen informiert werden, Art. 33, 34 DSGVO

Ich habe diese Pflicht zur Kenntnis genommen und stelle sicher, dass dieser Meldung erfolgen kann. Bitte zur Bestätigung Haken setzen: ☐

l) Erforderlichkeit der Übermittlung

Für die Übermittlung personenbezogener Daten von Mitgliedern der hsnr an externe Forschungseinrichtungen - ob öffentlich oder nicht-öffentlich -, die der Empfänger zu wissenschaftlichen Zwecken verarbeiten will, sind weitere Voraussetzungen zu beachten.

Ist eine solche Übermittlung beabsichtigt? Ja ☐ Nein ☐

Im Bejahensfall bitte den zuständigen DSB kontaktieren.

3. Ergänzender Hinweis

Bitte denken Sie daran, bei Mitarbeiterbefragungen die Personalräte und bei Studierendenbefragungen die Koordinierungsstelle Evaluation der Hochschule Niederrhein einzubinden.

4. Kopie der Datenschutzschulung Forschung

Meine Schulungsbescheinigung gemäß Präsidiumsbeschluss vom 16.09.2014. habe ich in Kopie als Anlage Nr. ☐ beigefügt.

5. Haftungserklärung

Ich erkläre hiermit verbindlich, dass ich mir über die datenschutzrechtlichen Pflichten als für das Forschungsprojekt Verantwortlicher im Klaren bin und die Beachtung der Datenschutzbestimmungen bei meinem Forschungsvorhaben sicherstelle sowie die vorstehenden Angaben nach bestem Wissen gemacht habe. Ich bin darüber informiert, dass ich mich in Zweifelsfällen bei den Datenschutzbeauftragten der hsnr erkundigen kann. Ich weiß, dass ich für Verstöße gegen den Datenschutz persönlich hafte.

……

Name in Blockschrift Datum Unterschrift