Datenschutzkonzept der WWU

Gemäß § 2 Datenschutzgesetz NRW (DSG NRW) vom 17. Mai 2018 haben die der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts jeweils für ihren Bereich die Ausführung der EU-Datenschutzgrundverordnung (DSGVO) vom 27. April 2016, des DSG NRW sowie anderer Rechtsvorschriften über den Datenschutz sicherzustellen. Gem. §§ 1 Abs. 2 und 2 Abs. 1 Hochschulgesetz NRW (HG NRW) vom 16. September 2014, in der Fassung des Gesetzes zur Änderung des Hochschulgesetzes vom 12. Juli 2019, ist die WWU eine rechtsfähige Körperschaft des öffentlichen Rechts und untersteht gem. § 76 Abs. 1 HG der Rechtsaufsicht des zuständigen Ministeriums.

In Erfüllung der Verpflichtung aus § 2 DSG NRW verabschiedet das Rektorat für die WWU folgendes Datenschutzkonzept:

Allgemeines

1. Ziele des Datenschutzkonzepts

Das Datenschutzkonzept der WWU soll die Umsetzung der gesetzlichen Anforderungen des Datenschutzes durch die WWU gewährleisten. Es dient als Orientierung für alle Mitarbeiterinnen und Mitarbeiter der WWU, die im Rahmen ihrer Tätigkeit für die WWU personenbezogene Daten verarbeiten, und ist Ausdruck der Wahrnehmung der Verantwortung der Hochschulleitung für die Einhaltung und Umsetzung der gesetzlichen Vorgaben für den Datenschutz.

2. Geltungsbereich des Datenschutzkonzepts

Dieses Datenschutzkonzept gilt für alle Fachbereiche, die zentrale Verwaltung und das Rektorat, sowie für alle Betriebseinheiten und sonstigen Einrichtungen der WWU. Das Datenschutzkonzept der WWU gilt nicht für An-Institute der WWU, Gesellschaften oder Vereine, an denen die WWU beteiligt ist und sonstige Einrichtungen und Institutionen, an denen die WWU oder Mitglieder oder Angehörige der WWU im Namen oder im Interesse der WWU beteiligt ist bzw. sind. Die Hochschulleitung wird jedoch in den Fällen, in denen die WWU in maßgeblicher Weise an den zuvor genannten Organisationen beteiligt ist, im Rahmen ihrer Möglichkeiten darauf hinwirken, dass diese in ihrem Zuständigkeitsbereich für die entsprechende Anwendung des Datenschutzkonzepts sorgen oder ein eigenes vergleichbares Datenschutzkonzept etablieren.

3. Rechtsgrundlagen

Die von der WWU bei der Verarbeitung personenbezogener Daten zu beachtenden Vorschriften sind insbesondere die DSGVO, das DSG NRW, sowie datenschutzrechtliche Vorschriften im HG NRW. Daneben gibt es datenschutzrechtliche Spezialvorschriften in verschiedenen Gesetzen, die ggf. bei einer konkreten Verarbeitungstätigkeit zu beachten sind.

Darüber hinaus können sich datenschutzrechtliche Anforderungen aus Dienstvereinbarungen zwischen dem Rektorat und den Personalräten ergeben.

4. Verantwortlichkeiten

4.1. Die Verantwortung für die Einhaltung und Umsetzung der gesetzlichen Vorgaben für den Datenschutz an der WWU trägt die Rektorin/der Rektor. Für die konkrete Umsetzung der gesetzlichen Anforderungen in den einzelnen Einheiten (Fachbereiche, zentrale Verwaltung, Betriebseinheiten und sonstige Einrichtungen) der WWU sind jedoch deren jeweilige Leiterinnen bzw. Leiter verantwortlich.

4.2. Für jede in Anlage 1 genannte Einheit wird durch die Leiterin/den Leiter eine Datenschutzkoordinatorin/ein Datenschutzkoordinator benannt. Sie/Er ist Ansprechperson, wenn es um die konkrete Umsetzung datenschutzschutzrechtlicher Anforderungen in der jeweiligen Einheit geht, die Verantwortlichkeit der Leiterin/des Leiters bleibt jedoch unberührt. Die Einheiten melden den Namen und die Kontaktdaten der aktuellen Datenschutzkoordinatorin/des aktuellen Datenschutzkoordinators im April bzw. Oktober für das jeweilige Semester der/dem Datenschutzbeauftragten, die/der eine entsprechende Liste führt.

4.3. Jede Führungskraft ist verpflichtet, die ihr zugeordneten Mitarbeiterinnen und Mitarbeiter sowohl bei Aufnahme der Tätigkeit der betreffenden Mitarbeiterinnen/Mitarbeiter für die WWU, als auch bei Bedarf im Laufe ihrer weiteren Tätigkeit für die WWU für die datenschutzrechtlichen Aspekte der jeweiligen Aufgabe zu sensibilisieren.

4.4. Alle Mitarbeiterinnen und Mitarbeiter sind gehalten, sich bei Aufnahme ihrer Tätigkeit für die WWU über die dabei zu beachtenden Anforderungen des Datenschutzes zu informieren und die entsprechenden Kenntnisse während ihrer Tätigkeit in dem jeweils erforderlichen Umfang zu aktualisieren. Die WWU stellt die hierfür erforderlichen Informationen über die behördliche Datenschutzbeauftragte/den behördlichen Datenschutzbeauftragten zur Verfügung.

5. Behördliche Datenschutzbeauftragte/Behördlicher Datenschutzbeauftragter

5.1. Die WWU bestellt gem. Art. 37 Abs. 1 lit. a) DSGVO, § 31 DSG NRW eine behördliche Datenschutzbeauftragte bzw. einen behördlichen Datenschutzbeauftragten sowie ihre/seine Stellvertretung. Beide bilden zusammen die „Stabsstelle Datenschutz“, die der Kanzlerin/dem Kanzler zugeordnet ist. Die/Der Datenschutzbeauftragte berichtet der Kanzlerin/dem Kanzler bei Bedarf, mindestens aber einmal im Quartal, über die aktuellen datenschutzrechtlich relevanten Entwicklungen und Themen an der WWU.

5.2. Die/Der Datenschutzbeauftragte berät das Rektorat in allen datenschutzrechtlichen Fragen. Sie/Er steht daneben allen Mitgliedern der WWU bei Bedarf für datenschutzrechtliche Beratungen zur Verfügung. Auf Anfrage begleitet sie/er Datenschutzfolgeabschätzungen (Art. 35 DSGVO). Soweit sich Betroffene zur Wahrnehmung Ihrer Rechte (z.B. des Auskunftsrechts nach Art. 15 DSGVO oder des Rechts auf Löschung nach Art. 17 DSGVO) an die WWU wenden, koordiniert die/der Datenschutzbeauftragte die Bearbeitung der entsprechenden Anfragen. Außerdem ist die/der Datenschutzbeauftragte Anlaufstelle für die Aufsichtsbehörde, die

Landesbeauftragte bzw. den Landesbeauftragten für Datenschutz und Informationsfreiheit (LDI).

5.3. Die/Der Datenschutzbeauftragte überwacht die Einhaltung und Umsetzung der datenschutzrechtlichen Vorschriften an der WWU. Sie/Er hat in diesem Zusammenhang soweit dies zur Erfüllung ihrer/seiner Aufgabe erforderlich ist ein Recht auf Einsicht in sämtliche Akten, Datenbestände, IT-Systeme und sonstige Informationsquellen, ein Recht gegenüber allen Mitgliedern der WWU auf Information und Auskunft sowie nach Ankündigung oder bei Gefahr im Verzug ein Recht auf Zugang zu allen dienstlichen Einrichtungen. Der/Dem Datenschutzbeauftragten sind alle Informationen, die zur ihrer/seiner Aufgabenwahrnehmung erforderlich sind, unaufgefordert zur Verfügung zu stellen. Die/Der Datenschutzbeauftragte ist jedoch nicht befugt, gegenüber den Mitgliedern der WWU Weisungen zu erteilen. Die/Der Datenschutzbeauftragte ist zur Verschwiegenheit über die Identität von betroffenen Personen sowie über Umstände, die Rückschlüsse auf betroffene Personen zulassen, verpflichtet, soweit sie/er nicht durch die betroffenen Personen hiervon befreit ist. Die/Der Datenschutzbeauftragte erstellt in Abstimmung mit der Rektorin/dem Rektor und der Kanzlerin/dem Kanzler einen Prüfplan (vgl. Anlage 2), der eine regelmäßige, stichprobenartige Überprüfung der Einhaltung der datenschutzrechtlichen Anforderungen durch alle Einheiten im Sinne von Ziff. 4.1 gewährleistet.

5.4. Nach Ablauf jedes Kalenderjahres erstellt die/der Datenschutzbeauftragte spätestens bis Ende Februar des Folgejahres einen Jahresbericht. Diesen legt sie/er zunächst dem IV-Lenkungsausschuss zur Stellungnahme und anschließend dem Rektorat vor. Mindestbestandteile des Jahresberichts sind:

- die Anzahl der Verdachtsfälle von Datenschutzverletzungen, die ihr/ihm gemeldet worden sind, die Anzahl dieser Fälle, die zu einer Meldung an die/den LDI geführt haben und zu welchem Ergebnis die Meldung geführt hat
- die Anzahl der der/dem Datenschutzbeauftragten bekannten Fälle, in denen Betroffene ihre Rechte (z.B. auf Auskunft oder auf Löschung) der WWU gegenüber geltend gemacht haben
- ein Überblick darüber, welche Organisationseinheiten im Rahmen des Prüfplans im Sinne von Ziff. 5.3 Satz 5 von ihr/ihm geprüft worden sind und welches Ergebnis die Prüfung ergeben hat.

Umsetzung des Datenschutzes an der WWU

6. Technische und organisatorische Maßnahmen

6.1. Die WWU trifft abhängig von der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos von Datenschutzverletzungen (Art. 32 Abs. 1 DSGVO) geeignete technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

6.2. Zu diesen technischen und organisatorischen Maßnahmen gehören in Anlehnung an das Standard-Datenschutzmodell der „Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder“ insbesondere:

6.2.1. Maßnahmen zur Gewährleistung der Verfügbarkeit von personenbezogenen Daten

- Anfertigung von Sicherheitskopien von Daten, Prozesszuständen, Konfigurationen, Datenstrukturen, Transaktionshistorien
- Schutz vor äußeren Einflüssen (Schadsoftware, Sabotage, höhere Gewalt)
- Redundanz von Hard- und Software sowie Infrastruktur
- Erstellung von Notfallkonzepten, Reparaturstrategien und Ausweichprozessen
- Vertretungsregelung für abwesende Beschäftigte

6.2.2. Maßnahmen zur Gewährleistung der Integrität von personenbezogenen Daten

- Löschen oder Berichtigen falscher Daten
- Härten von IT-Systemen, so dass diese keine oder möglichst wenig Nebenfunktionalitäten aufweisen
- Prozesse zur Aufrechterhaltung der Aktualität von Daten
- Prozesse zur Identifizierung und Authentifizierung von Personen und Gerätschaften
- Durchführung von Test zur Feststellung und Dokumentation der Funktionalität, von Risiken sowie Sicherheitslücken und Nebenwirkungen von Prozessen
- Schutz vor äußeren Einflüssen (Spionage, Hacking)

6.2.3. Maßnahmen zur Gewährleistung der Vertraulichkeit von personenbezogenen Daten

- Festlegung eines Rechte- und Rollen-Konzepts
- Festlegung und Kontrolle der Nutzung zugelassener Ressourcen, insbesondere Kommunikationskanäle
- Spezifizierte, für die jeweilige Verarbeitungstätigkeit ausgestattete Umgebungen (Gebäude, Räume)
- Festlegung und Kontrolle organisatorischer Abläufe, interner Regelungen und vertraglicher Verpflichtungen
- Verschlüsselung von gespeicherten oder transferierten Daten sowie Prozesse zur Verwaltung und zum Schutz der kryptografischen Informationen
- Implementierung von Datenmasken, die Datenfelder unterdrücken, sowie automatischer Sperr- und Löschroutinen, Pseudonymisierungs- und Anonymisierungsverfahren

7. Schulung von Mitarbeiterinnen und Mitarbeitern

Die/Der Datenschutzbeauftragte bietet sowohl im allgemeinen Fortbildungsprogramm der WWU als auch auf Nachfrage Schulungen für Mitarbeiterinnen und Mitarbeiter an. Die Schulungen behandeln allgemeine datenschutzrechtliche Fragestellungen, werden bei Bedarf aber auch auf besondere datenschutzrechtliche Anforderungen ausgerichtet, die durch die Tätigkeit der Teilnehmerinnen und Teilnehmer bedingt sind.

8. Verpflichtung von Mitarbeiterinnen und Mitarbeitern

Da alle Mitarbeiterinnen und Mitarbeiter der WWU aufgrund beamten- bzw. tarifrechtlicher Vorschriften grundsätzlich verpflichtet sind, dienstlich erlangte Informationen sowohl innerhalb der WWU als auch gegenüber Externen vertraulich zu behandeln, erfolgt in der Regel keine

separate Verpflichtung der Mitarbeiterinnen und Mitarbeiter auf das Datengeheimnis. Ausnahmen im Einzelfall sind mit der/dem Datenschutzbeauftragten abzustimmen.

9. Datenschutzrechtlich relevante Dokumente/Muster

Die/Der Datenschutzbeauftragte stellt Muster für Datenschutzerklärungen, Einwilligungserklärungen durch die Betroffenen sowie Vereinbarungen für Auftragsverarbeitungen (Art. 28 DSGVO) und Vereinbarungen für gemeinsam Verantwortliche (Art. 26 DSGVO) zur Verfügung.

10. Verzeichnis von Verarbeitungstätigkeiten

10.1. Alle Mitglieder der WWU erfassen in ihrem Zuständigkeitsbereich solche Verarbeitungstätigkeiten, die personenbezogene Daten beinhalten, in dem gesetzlich vorgeschriebenen „Verzeichnis von Verarbeitungstätigkeiten“ (Art. 30 DSGVO). Sie sind gehalten, das Verzeichnis für die in ihrem Zuständigkeitsbereich erfassten Verarbeitungstätigkeiten bei Bedarf zu aktualisieren. Die/Der Datenschutzbeauftragte hat Zugriff auf alle in dem Verzeichnis erfassten Verarbeitungstätigkeiten.

10.2. Für die Erfassung des Verzeichnisses von Verarbeitungstätigkeiten stellt die WWU ein Online-Tool zur Verfügung. Alle Mitglieder der WWU sind gehalten, die in ihrem Zuständigkeitsbereich erfolgenden Verarbeitungstätigkeiten ausschließlich in diesem Tool zu erfassen. Ausnahmen sind mit der/dem Datenschutzbeauftragten abzustimmen.

11. Datenschutz-Folgenabschätzung

11.1. Wenn eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, ist vor Aufnahme der Verarbeitungstätigkeit eine Abschätzung ihrer Folgen vorzunehmen (Art. 35 Abs. 1 DSGVO). Jedes Mitglied der WWU, unter dessen Leitung eine Verarbeitung personenbezogener Daten durchgeführt wird, ist gehalten, vor Aufnahme der Verarbeitungstätigkeit in geeigneter Weise zu prüfen, ob zunächst eine Datenschutzfolgenabschätzung vorzunehmen ist. Die/Der Datenschutzbeauftragte stellt hierfür ein geeignetes Prüfschema zur Verfügung.

11.2. Wenn das Ergebnis der Vorprüfung ergibt, dass für die betreffende Verarbeitungstätigkeit eine Datenschutzfolgenabschätzung durchzuführen ist, darf die betreffende Verarbeitungstätigkeit nicht aufgenommen werden, bevor nicht die entsprechende Datenschutzfolgenabschätzung durchgeführt und die dabei ggf. identifizierten notwendigen Änderungen der Verarbeitungstätigkeit umgesetzt worden sind.

11.3. Die/Der Datenschutzbeauftragte unterstützt und berät bei der Durchführung der Vorprüfung und der eigentlichen Datenschutzfolgenabschätzung.

12. Löschung von Daten

12.1. Personenbezogene Daten sind grundsätzlich dann zu löschen, wenn sie für die Zwecke, für die sie erhoben worden oder auf sonstige Weise verarbeitet worden sind, nicht mehr notwendig sind (Art. 17 Abs. 1 DSGVO).

12.2. Grundsätzlich ist jedes Mitglied der WWU, unter dessen Leitung personenbezogene Daten verarbeitet werden, gehalten, so frühzeitig wie möglich eine Frist für Löschung der personenbezogenen Daten des betreffenden Verarbeitungsvorgangs festzulegen (Löschkonzept). Bei Bedarf erstellt die Leiterin/der Leiter einer Einheit im Sinne von Ziff. 4.1 Satz 2 für ihren/seinen Zuständigkeitsbereich allgemeine Löschkonzepte. Für Dokumente der zentralen Verwaltung gilt insoweit die „Richtlinie über Aufbewahrung, Aussonderung und Vernichtung von Schriftgut“ in der jeweils aktuellen Fassung. Die/der behördliche Datenschutzbeauftragte stellt eine Handreichung für die Erstellung von Löschkonzepten zur Verfügung.

13. Vorgehen bei Datenschutzvorfällen

13.1. Verletzungen des Schutzes personenbezogener Daten sind unverzüglich und möglichst innerhalb von 72 Stunden nach Kenntnis der/dem Landesbeauftragten für Datenschutz und Informationsfreiheit (LDI) zu melden (Art. 33 Abs. 1 DSGVO). Eine Verletzung des Schutzes personenbezogener Daten ist gem. Art. 4 Ziff. 12 DSGVO jede „Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden“.

13.2. An der WWU ist im Falle des Verdachts einer Verletzung des Schutzes personenbezogener Daten dieser Verdacht unverzüglich zunächst der/dem Datenschutzbeauftragten zu melden, die/der eine Einschätzung vornimmt, ob tatsächlich eine Datenschutzverletzung vorliegt und wie hoch das Risiko für die Betroffenen voraussichtlich ist. Die/Der Datenschutzbeauftragte legt anschließend das Ergebnis ihrer/seiner Prüfung der Kanzlerin/dem Kanzler vor, die/der darüber entscheidet, ob eine Meldung an die LDI erfolgt und ob die Betroffenen von der Verletzung benachrichtigt werden.

13.3. Besteht im Fall des Verdachts einer Verletzung des Schutzes personenbezogener Daten voraussichtlich die Gefahr eines erheblichen Schadens für die Betroffenen und/oder sind personenbezogene Daten in erheblichem Umfang von der vermuteten Verletzung betroffen, so legt die/der Datenschutzbeauftragte das Ergebnis ihrer/seiner Prüfung sowohl der Rektorin/dem Rektor als auch der Kanzlerin/dem Kanzler vor. Die Entscheidung im Sinne von Ziff. 13.2 Satz 2 wird in diesem Fall von Rektorin/Rektor und Kanzlerin/Kanzler in gegenseitigem Einvernehmen getroffen.

13.4. Die/Der Datenschutzbeauftragte legt ggf. im Nachgang zu einem Datenschutzvorfall der Rektorin/dem Rektor bzw. der Kanzlerin/dem Kanzler Vorschläge für technische und/oder organisatorische Maßnahmen vor, um vergleichbare Datenschutzvorfälle für die Zukunft nach Möglichkeit zu verhindern.

14. IT-Sicherheit

14.1. Datenschutz hängt in großem Umfang von der Sicherheit der betreffenden IT-Systeme ab. Die WWU hat unter Federführung des IV-Sicherheitsteams die „Informationssicherheitsleitlinie der Westfälischen Wilhelms-Universität“ erlassen. Diese formuliert u.a. allgemeine Sicherheitsziele bei der Informationsverarbeitung und ist von allen Mitgliedern der WWU bei der technischen Verarbeitung personenbezogener Daten zu beachten.

14.2. Die/Der Datenschutzbeauftragte steht in regelmäßigem Austausch mit der Leiterin/dem Leiter des IT-Sicherheitsteams der WWU.

15. Datenschutzrechtliche Angelegenheiten der Medizinischen Fakultät

Die Bearbeitung der datenschutzrechtlichen Angelegenheiten der Medizinischen Fakultät richtet sich nach den Regelungen des Kooperationsvertrages zwischen WWU und UKM sowie ergänzender datenschutzrechtlicher Vereinbarungen zwischen der WWU und dem UKM.

Ausgefertigt aufgrund des Beschlusses des Rektorats der Westfälischen Wilhelms-Universität vom 25.06.2020. Das vorstehende Datenschutzkonzept wird hiermit verkündet.

Münster, den 09.07.2020 Der Rektor

Prof. Dr. Johannes W e s s e l s