Datensicherheitskonzept eines Forschungsprojekts
an der <Hochschule X>

(Version 1.0)

|  |  |
| --- | --- |
| Forschungsprojekt |  |
| Fakultät |  |
| Lehrstuhl |  |
| Kontaktdaten  |  |

Die Mitarbeiterinnen und Mitarbeiter des Projektes sind verpflichtet den Datenschutz zu wahren und die Bestimmungen der EU-Datenschutzgrundverordnung (DSGVO), des Datenschutzgesetztes des Landes Nordrhein-Westfalen (DSG NRW) sowie weiterer Datenschutzvorschriften einzuhalten.

|  |  |  |
| --- | --- | --- |
| Nachname | Vorname | E-Mail-Adresse |
|  |  |  |
|  |  |  |
|  |  |  |

Das genannte Forschungsprojekt hat zur Gewährleistung der Sicherheit der Verarbeitung (gem. Art. 32 DSGVO) nachfolgende technische und organisatorische Sicherheitsmaßnahmen getroffen.

(bitte zutreffendes Ankreuzen und nichtvorgesehene Maßnahmen sowie weitere Beschreibungen ergänzen)

# Pseudonymisierung (Art. 32 Abs. 1 lit. a) DSGVO)

|  |
| --- |
| *Maßnahmen, um die Feststellung der Identität der Betroffenen auszuschließen oder wesentlich zu erschweren. Im Gegensatz zur Anonymisierung (die keinerlei Zuordnung der Daten zu einer Person mehr erlaubt) werden bei der Pseudonymisierung der Name und die anderen Identifikationsmerkmal durch ein Pseudonym (zumeist eine Buchstaben- /Zahlenkombination) ersetzt, sodass ohne Hinzuziehen weiterer Informationen die Zuordnung zu einer spezifischen betroffenen Person ausgeschlossen ist* : |
| [ ]  | Verwendung eines Pseudonymisierungsverfahrens  |
| [ ]  | Sichere Aufbewahrung der Zuordnungsfunktion |
|  | [ ]  | Hinterlegung der „Zuordnungstabelle“ bei einem Datentreuhänder |
|  |  | [ ]  | Notar |
|  |  | [ ]  | Datenschutzbeauftragter |
|  |  | [ ]  |  |
|  | [ ]  | Beschreibung der für den Zugriff auf die Zuordnung berechtigten Personen: |
| Weitere Beschreibung der Pseudonymisierung: |

# Verschlüsselung (Art. 32 Abs. 1 lit. a) DSGVO)

|  |
| --- |
| *Maßnahmen, damit der Zugriff auf personenbezogene Daten nur mit einem den befugten Personen zugänglichen elektronischen Schlüssel möglich ist*: |
| [ ]  | Daten werden auf persönlichen Rechnern (bspw. Notebooks) auf einer verschlüsselten Festplatte bzw. in verschlüsselten Containern (VeraCrypt, Bitlocker, …) gespeichert |
| [ ]  | Datentransporte (E-Mail, CD/DCD, USB-Stick, mobile Festplatte, …) finden ausschließlich mit verschlüsselten Daten(-trägern) statt |
| [ ]  | Zugriff auf elektronische Dienste erfolgt ausschließlich mit Transportverschlüsselung (HTTPS, TLS) |
| [ ]  | Einsatz von verschlüsselten Verbindungen bei Remote-Zugriffen (VPN der Hochschule)  |
| Weitere Beschreibung und Maßnahmen:  |

# Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO)

|  |
| --- |
| *Maßnahmen, damit nur Befugte personenbezogene Daten zur Kenntnis nehmen können*: |
| [ ]  | Daten werden auf dem zentralen Netzlaufwerk des Rechenzentrums der Hochschule gespeichert |
|  | [ ]  | Die Zugriffsberechtigungen werden über eine Gruppe vergeben, in der nur Projektmitarbeiter enthalten sind |
| [ ]  | Daten werden in einer zentralen Datenbank des Rechenzentrums der Hochschule gespeichert |
|  | [ ]  | Die Zugriffsberechtigungen werden über eine Gruppe vergeben, in der nur Projektmitarbeiter enthalten sind |
| [ ]  | Daten werden auf persönlichen Rechnern in Büroräumen der Hochschule gespeichert  |
| [ ]  | Daten werden mit persönlichen Rechnern in Büroräumen der Hochschule verarbeitet  |
|  | [ ]  | Büro/s wird/werden bei Abwesenheit immer verschlossen |
|  | [ ]  | Rechner verfügt über eine automatische Bildschirmsperrung |
|  | [ ]  | Rechner wird zentral administriert |
|  | [ ]  | Rechner verfügt über ausreichende Schutzmaßnahmen (sichere Passworte, BIOS-Schutz, Virenscanner, regelmäßige Updates, …) |
| [ ]  | Spezifische Anweisungen zum Umgang mit personenbezogenen Daten an die Projektmitarbeiter |
| [ ]  | Dokumentiertes Anonymisierungs- und Löschkonzept |
| [ ]  | Protokollierung der ordnungsgemäßen Löschung (Löschprotokoll) |
| Weitere Beschreibung und Maßnahmen: (bspw. eigene Server (wo, wie geschützt?), spezielle Systeme (wie gesichert?), Cloud-Dienste (Auftragsdatenverarbeitungsvertrag, …)) |

# Integrität (Art. 32 Abs. 1 lit. b) DSGVO)

|  |
| --- |
| *Maßnahmen, damit personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben:* |
| [ ]  | Vermeidung unbefugter oder zufälliger Datenverarbeitung durch Entfernen von Schreibberechtigungen (Dokumente schreibgeschützt gespeichert, Nur-Lese-Berechtigung vergeben) |
| [ ]  | Verwendung von Signaturverfahren |
| [ ]  | Daten liegen in einem nicht einfach/versehentlich bearbeitbaren Format vor (PDF) |
| [ ]  | Regelmäßige Kontrolle der Aktualität der Daten |
| Weitere Beschreibung und Maßnahmen: |

# Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b) DSGVO)

|  |
| --- |
| *Maßnahmen, damit personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können:* |
| [ ]  | Papierdokumente sind beschriftet und weisen eine klare und übersichtliche Ordnung auf |
| [ ]  | Eigene Server werden in geeigneten Räumen betrieben (Brandschutz, USV, …)  |
| [ ]  | Eigene Server sind durch eine Firewall vor unzulässigen Netzzugriffen geschützt |
| [ ]  | Betrieb erfolgt über geschultes IT-Fachpersonal |
| Weitere Beschreibung und Maßnahmen (besondere Schutzmaßnahmen gegen den Ausfall von Systemen, …): |

# Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall (Art. 32 Abs. 1 lit. c) DSGVO)

|  |
| --- |
| *Maßnahmen, um nach einem physischen oder technischen Zwischenfall die Verarbeitung möglichst schnell wieder in den Regelbetrieb zu versetzten :* |
| [ ]  | Systeme können jederzeit neu installiert werden (Software, Lizenzdaten, …) |
| [ ]  | Wichtige Passworte sind sicher (verschlossen und feuergeschützt) in einem Tresor hinterlegt |
| [ ]  | Wiederherstellung der Daten ist jederzeit aus der Datensicherung möglich |
|  | [ ]  | zentrale Datensicherung |
|  | [ ]  | Datensicherung auf externem Medium (Festplatte, CD/DVD, …), das sicher (verschlossen und feuergeschützt) aufbewahrt wird |
| [ ]  | Dokumentiertes Notfallkonzept / Notfallhandbuch |
| [ ]  | Durchführung von Notfallübungen |
| Weitere Beschreibung und Maßnahmen (insb. gegen Datenverlust): |

# Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen (Art. 32 Abs. 1 lit. d) DSGVO)

|  |
| --- |
| *Maßnahmen, um die Wirksamkeit der technischen und organisatorischen Maßnahmen nachzuweisen:* |
| [ ]  | Regelmäßige Überarbeitung des Sicherheitskonzepts |
| [ ]  | Beteiligung einer Datenschutzkoordinatorin / eines Datenschutzkoordinatoren bei der Erstellung |
| [ ]  | Beteiligung der / des IT-Sicherheitsbeauftragten bei der Erstellung |
| [ ]  | Beteiligung der / des Datenschutzbeauftragten bei der Erstellung |
| [ ]  | Externe Prüfungen, Audits, Zertifizierungen |
| Weitere Maßnahmen: |

# Weitere Maßnahmen

|  |  |
| --- | --- |
| [ ]  | vollständige, übersichtliche und jederzeit nachprüfbare Dokumentation aller wesentlichen Datenverarbeitungsvorgänge |
| [ ]  | Sensibilisierung und/oder Schulung der an den Verarbeitungsvorgängen beteiligten Personen |
| [ ]  | Verpflichtung der an den Verarbeitungsvorgängen beteiligten Personen auf das Datengeheimnis |
| Weitere Maßnahmen: |