

Das John-Rittmeister-Institut definiert eigene Datenschutz-Ziele als Selbstverpflichtung.

Dazu gehören:

- Unbedingte Einhaltung der Vorgaben der EU-Datenschutzgrundverordnung, des Bundesdatenschutzgesetzes und des Telemediengesetzes durch alle Mitarbeiter_innen, Funktionsträger_innen, Patienten, Praktikanten, Honorarkräfte, Ausbildungskandidaten, Dozenten, Supervisoren und Lehranalytiker_innen sowie Mitglieder_innen
- Unbedingte Einhaltung der institutseigenen Datenschutzvorschriften durch alle Mitarbeiter_innen, Funktionsträger_innen, Patienten, Praktikanten, Honorarkräfte, Ausbildungskandidaten, Dozenten, Supervisoren und Lehranalytiker_innen sowie Mitglieder_innen
- Strikte Verpflichtung zur Geheimhaltung und Vertraulichkeit
- Datenschutzkonforme Arbeitsplatzgestaltung
- Unbedingter Schutz vor Dateneinsicht durch Unbefugte
- Dabei orientiert sich das John-Rittmeister-Institut an Art. 5 EU-DSGVO sowie § 47 BDSG n.F.

Dem John-Rittmeister-Institut ist Datenschutz ein wichtiges Organisationsziel. Deshalb hat sich das John-Rittmeister-Institut sich Datenschutzziele gesetzt, die in jedem Organisationsprozess ihren Platz haben.

Die Schutzziele sind:

Vertraulichkeit und Datensicherheit: Für personenbezogene Daten gilt das Datengeheimnis. Sie müssen im persönlichen Umgang vertraulich behandelt werden und durch angemessene organisatorische und technische Maßnahmen gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe, sowie versehentlichen Verlust, Veränderung oder Zerstörung gesichert werden.

Rechtevergabe: Die Daten unterliegen der vertraulichen Verarbeitung. Wo es angezeigt ist, werden Verschlüsselungen, Passwortschutz, Zugriffsrechtevergabe, Zugriffskontrollverfahren und eine Protokollierung administrativer Tätigkeiten durchgeführt.

Verfügbarkeit: Gesicherter Zugriff auf Information innerhalb einer festgelegten Zeit. Daten werden immer nur den Mitarbeiter_innen, Funktionsträger_innen, Patienten, Praktikanten, Honorarkräfte, Ausbildungskandidaten, Dozenten, Supervisoren und Lehranalytiker_innen oder Mitglieder_innen zur Verfügung gestellt/haben Zugriff auf diese, wenn die Bearbeitung dieser zu den zugewiesenen Aufgaben gehört. Jede/r Mitarbeiter_inn, Funktionsträger_in, Patient_in, Praktikant_in, Honorarkraft, Ausbildungskandidat_in, Dozent_in, Supervisor_in und Lehranalytiker_in sowie jedes Mitglied hat unmittelbar auf alle Prozesse und Daten Zugriff, die er/sie für die Erledigung seiner/ihrer Aufgaben benötigt.

Datenvermeidung und Datensparsamkeit: Es werden nur die Daten verarbeitet, die für den Verwendungszweck unbedingt notwendig sind. Vor einer Verarbeitung personenbezogener Daten muss geprüft werden, ob und in welchem Umfang diese notwendig sind, um den mit der Verarbeitung angestrebten Zweck zu erreichen. Wenn es zur Erreichung des Zwecks möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Zweck steht, sind anonymisierte oder statistische Daten zu verwenden. Personenbezogene Daten dürfen nicht auf Vorrat für potentielle zukünftige Zwecke gespeichert werden, es sei denn, dies ist durch staatliches Recht vorgeschrieben oder erlaubt.

Integrität: Die Informationen sind (ggf. beschränkt auf eine festgelegte Zeit) gesichert echt. Die Informationen, die verarbeitet werden, sind von hoher Qualität. Ein Datenqualitätsmanagement sorgt für die Richtigkeit der verarbeiteten Daten. Werden Datenfehler festgestellt, werden diese unverzüglich behoben/korrigiert.

Transparenz: Personenbezogene Verfahren sollen mit zumutbarem Aufwand nachvollzogen, überprüft und bewertet werden können. Die Quelle der Daten ist stets nachvollziehbar und jedem Dateninhaber kann innerhalb kurzer Zeit Auskunft über die sie betreffenden Daten gegeben werden. Der Betroffene muss über den Umgang mit seinen Daten informiert werden. Grundsätzlich sind personenbezogene Daten bei dem Betroffenen selbst zu erheben. Bei Erhebung der Daten muss der Betroffene mindestens Folgendes erkennen können oder entsprechend informiert werden über:

- die Identität der verantwortlichen Stelle
- den Zweck der Datenverarbeitung
- die hinterlegten Aufbewahrungsfristen
- Dritte oder Kategorien von Dritten, an die die Daten gegebenenfalls übermittelt werden

Löschung und Speicherbegrenzung: Personenbezogene Daten, die nach Ablauf von gesetzlichen oder geschäftsprozessbezogenen Aufbewahrungsfristen nicht mehr erforderlich sind, müssen gelöscht werden. Bestehen im Einzelfall Anhaltspunkte für schutzwürdige Interessen oder für eine historische Bedeutung dieser Daten, müssen die Daten weiter gespeichert bleiben, bis das schutzwürdige Interesse rechtlich geklärt.

Nichtverkettbarkeit: Personenbezogene Verfahren müssen so eingerichtet sein, dass deren Daten nicht oder nur mit unverhältnismäßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck erhoben, verarbeitet und genutzt werden können. Die Zweckbindung wird über alle Prozesse eingehalten.

Intervenierbarkeit: Personenbezogene Verfahren benötigen Maßnahmen, dass sie dem Betroffenen die Ausübung der ihm zustehenden Rechte wirksam ermöglichen. Neben der Auskunft über die sie betreffenden Daten ist gewährleistet, dass eine

Datenschutzziele des John-Rittmeister-Instituts e. V.

Korrektur einer angemahnten falschen Information unverzüglich an allen Stellen des Systems erfolgen kann.

Verfügbarkeit: Die Arbeit des John-Rittmeister-Instituts stützt sich auf eine reibungslos funktionierende Datenverfügbarkeit. Durch redundante Speichersysteme, Sicherheitskopien, Clustersysteme oder Ausweichzentren ist eine hohe Qualität der Verfügbarkeit gewährleistet.

Fairness und Rechtmäßigkeit: Bei der Verarbeitung personenbezogener Daten muss das informationelle Selbstbestimmungsrecht des Betroffenen gewahrt werden. Personenbezogene Daten müssen auf rechtmäßige Weise erhoben und verarbeitet werden.

Zweckbindung: Daten werden nur für den Zweck ihrer Erhebung verarbeitet und gespeichert. Die Verarbeitung personenbezogener Daten darf lediglich die Zwecke verfolgen, die vor der Erhebung der Daten festgelegt wurden. Nachträgliche Änderungen der Zwecke sind nur eingeschränkt möglich und bedürfen einer Rechtfertigung.

Sachliche Richtigkeit und Datenaktualität: Personenbezogene Daten sind richtig, vollständig und – soweit erforderlich – auf dem aktuellen Stand zu speichern. Es sind angemessene Maßnahmen zu treffen, um sicherzustellen, dass nicht zutreffende unvollständige oder veraltete Daten gelöscht, berichtigt, ergänzt oder aktualisiert werden.

Rechenschaftspflicht: Die oberste Leitung kann jederzeit die Einhaltung der hier beschriebenen Datenschutzziele nachweisen. Die oberste Leitung kann jederzeit über Datenverarbeitungszwecke, den Verbleib von Daten bei Weitergabe und Löschfristen einzelner Dateninhaber Auskunft geben. Die oberste Leitung sorgt für ein angemessenes Schutzniveau entsprechend dem Stand der Technik.

Zuständigkeit: Im John-Rittmeister-Institut sind die Aufgaben und Zuständigkeiten hinsichtlich der Erreichung dieser Ziele klar geregelt. Im John-Rittmeister-Institut gibt es eine Datenschutzleitlinie die allgemein bekannt ist und deren Umsetzung wird durch Organisationsregeln gewährleistet.