Leitlinie zur Informationssicherheit

Informationssicherheits-Policy - Ebene 1

Inhalt

1 Einleitung

Mit dieser Leitlinie bekennt sich die Deutsche Rentenversicherung zu ihrer Verantwortung für die Informationssicherheit[1]. Ziel ist ein angemessener Schutz für alle Informationen. Maßgeblich für die nachfolgenden Regelungen zur Informationssicherheit sind die Standards des IT-Grundschutzes des Bundesamts für Sicherheit in der Informationstechnik (BSI) und die Einhaltung der Datenschutzvorschriften.

Diese Leitlinie beschreibt

- den Stellenwert der Informationsverarbeitung,
- die Ziele der Informationssicherheit,
- die Sicherheitsstrategie einschließlich der Informationssicherheits-Policy als Rahmen und Regelwerk der Sicherheitskonzeption der Deutschen Rentenversicherung.

Diese Leitlinie enthält die Leitaussagen zur Sicherheitsstrategie der Deutschen Rentenversicherung und bildet die oberste Ebene der Informationssicherheits-Policy (vgl. Abschnitt 5.4).

2 Festlegung des Geltungsbereichs

Die in diesem Dokument beschriebenen Maßgaben und Zielsetzungen gelten unmittelbar und uneingeschränkt für alle Formen der Datenverarbeitung. Sie sind für die Träger der Deutschen Rentenversicherung verbindlich. Die Leitlinie zur Informationssicherheit ist allen Beschäftigten zur Kenntnis zu bringen.

3 Stellenwert der Informationsverarbeitung

Die Datenverarbeitung und der Einsatz vielfältiger Informations- und Kommunikationstechniken spielen eine Schlüsselrolle für die Aufgabenerfüllung in der Deutschen Rentenversicherung. Wichtig dabei ist insbesondere die rechtmäßige, zuverlässige und korrekte Verarbeitung der Informationen. Die zur Datenverarbeitung

[1] Informationssicherheit umfasst insbesondere den Datenschutz und die IT-Sicherheit.

genutzten und bereitgestellten Einrichtungen bedürfen daher eines Schutzes, der dieser Bedeutung gerecht wird.

4 Ziele der Informationssicherheit

Generelles Ziel ist der rechtmäßige Umgang mit Daten und die Aufrechterhaltung der Arbeitsfähigkeit und Erfüllung der Fachaufgaben der Deutschen Rentenversicherung. Hierzu sind die drei wichtigsten Sicherheitsziele der Informationssicherheit zu gewährleisten:

- Vertraulichkeit: Daten dürfen ausschließlich einem berechtigten Personenkreis zur Verfügung stehen.
- Integrität: Sicherstellung der Vollständigkeit und Unversehrtheit von Daten.
- Verfügbarkeit: Die Nutzung von Daten muss dem berechtigten Personenkreis stets wie vorgesehen möglich sein.

Für personenbezogene Daten ist insbesondere der Schutz der Persönlichkeitsrechte betroffener Personen zu gewährleisten. Hier sind folgende weitere Sicherheitsziele relevant:

- Rechtmäßigkeit: Verbot mit Erlaubnisvorbehalt.
- Zweckbindung und Nichtverkettbarkeit: Daten dürfen nur für den Zweck verarbeitet und ausgewertet werden, für den sie erhoben werden. Daten, die für verschiedene Zwecke erhoben wurden, dürfen nicht verknüpft werden.
- Transparenz: Jede Person muss die Verarbeitung ihrer personenbezogenen Daten nachvollziehen können (z.B. Auskunftsrechte etc.).
- Intervenierbarkeit: Jede betroffene Person muss ihre Betroffenenrechte geltend machen können.

Abhängig von Art und Zweck der Daten können weitere Sicherheitsziele wie Authentizität und Revisionsfähigkeit von Bedeutung sein. Die ausgewählten Sicherheitsziele sind bei allen mit der Datenverarbeitung verbundenen Aufgaben, insbesondere Beschaffung, Entwicklung,

Betrieb und sonstiger Nutzung von Informations- und Kommunikationstechnik zu berücksichtigen.

5 Sicherheitsstrategie

Auf der Grundlage der bisher gewonnenen Erfahrungen und aus der Erkenntnis heraus, dass es eine absolute Sicherheit nicht gibt, leitet die Deutschen Rentenversicherung die Verpflichtung ab, durch aufeinander abgestimmte technische, organisatorische, infrastrukturelle und personelle Maßnahmen die stets bestehenden Risiken so zu beschränken, dass das verbleibende Restrisiko - abhängig vom Schutzbedarf der Daten - tragbar ist.

5.1 Ziele der Sicherheitsstrategie

Voraussetzung zur Erreichung einer angemessenen Informationssicherheit sind verantwortungsbewusste und kompetente Beschäftigte, die koordiniert zusammenarbeiten. Als Grundlage für diese Zusammenarbeit dient das Regelwerk zur Sicherheit bei der Informationsverarbeitung in der Deutschen Rentenversicherung (Informationssicherheits-Policy), in dem hierarchisch gegliedert die Regelungen zur Informationssicherheit zusammengefasst sind (vgl. Abschnitt 5.4). Konkret verfolgt die Sicherheitsstrategie der Deutschen Rentenversicherung folgende Ziele:

- Gewährleistung der aus gesetzlichen Vorgaben resultierenden Anforderungen:
    - Schutz von Sozialdaten sowie von Betriebs- und Geschäftsgeheimnissen gemäß den Anforderungen, insbesondere aus dem Sozialgesetzbuch.
    - Schutz anderer personenbezogener Daten nach den jeweils anzuwendenden Datenschutzvorschriften.
    - Sicherheit gemäß den Rechnungsbestimmungen für IT-Verfahren.

- Begrenzung der Sicherheitsrisiken auf ein vertretbares Maß.

- Sensibilisierung der Beschäftigten für die Aufgabe Informationssicherheit.

- Sicherstellung der Verfügbarkeit von technischen Systemen und Daten (Verfügbarkeitsquoten, Minimierung der Ausfallzeiten und Begrenzung finanzieller Verluste durch Notfallvorsorge).

- Sicherstellung und Weiterentwicklung des hohen Niveaus bei der Qualitätssicherung von technischen Systemen.

- Ständige personenunabhängige Verfügbarkeit des notwendigen Fachwissens (Festlegung von Aufgaben und Verantwortlichkeiten, Dokumentationsrichtlinien).

- Gewährleistung des guten Rufs der Deutschen Rentenversicherung in der Öffentlichkeit (Schutz vor Imageverlust).

Die Umsetzung dieser Ziele wird, basierend auf einem angepassten Sicherheitsprozess, durch geeignete und aufeinander abgestimmte technische, organisatorische, infrastrukturelle und personelle Sicherheitsmaßnahmen erreicht. Die Sicherheitsmaßnahmen müssen dabei in einem wirtschaftlich angemessenen Verhältnis zum Schutzbedarf der IT-Verfahren und der zugrunde liegenden Daten stehen.

5.2 Informationssicherheitsmanagement

Die Verantwortung für die Informationssicherheit liegt bei der Geschäftsführung bzw. beim Direktorium.[2] Wesentlicher Erfolgsfaktor zur Gewährleistung der Informationssicherheit ist ein effektives Informationssicherheitsmanagement. Zur operativen Aufgabenwahrnehmung und regelmäßigen Berichterstattung benennt jeder Träger der Deutschen Rentenversicherung neben der bzw. dem gesetzlich zu bestellenden behördlichen Datenschutzbeauftragten deshalb eine Person, die als IT-Sicherheitsbeauftragte oder IT- Sicherheitsbeauftragter diese Rolle wahrnimmt und das IT-Sicherheitsmanagement repräsentiert und verantwortlich steuert.

Näheres zur Organisationsstruktur und zur Umsetzung des Sicherheitsprozesses wird im Dokument *Grundzüge zur Informationssicherheit* geregelt.

[2] nach der gültigen Fassung von § 36 SGB IV

5.3 Mitwirkung aller Beschäftigten bei der Informationssicherheit

Informationssicherheit ist eine Daueraufgabe für alle Beschäftigten. Die Verantwortung für den sicherheitsbewussten Umgang mit Systemen zur Datenverarbeitung liegt daher bei allen Organisationseinheiten und Beschäftigten. Diese sind gehalten den Informationssicherheitsprozess zu unterstützen. Hierzu gehören im Wesentlichen die schnelle Information über Sicherheitsvorfälle, Sicherheitslücken, Sicherheitsschwachstellen und anstehende Änderungen im technischen und organisatorischen Bereich, die Auswirkungen auf die Informationssicherheit haben könnten.

Pflicht aller Beschäftigten ist es, mit allen zu dienstlichen Zwecken bereitgestellten Daten vertraulich umzugehen, Amtsgeheimnisse oder sonstige Geheimnisse zu wahren und sorgfältig mit den zur Verfügung gestellten technischen Systemen umzugehen. Diese Verpflichtung gilt wegen der unauflöslichen Verbindung von Datenschutz und IT-Sicherheit auch entsprechend für die Umsetzung von Maßnahmen zur Informationssicherheit.

5.4 Informationssicherheits-Policy

Die Planung, Umsetzung und Kontrolle von Informationssicherheitsmaßnahmen ist ein laufender Prozess, der regelmäßig überprüft und ggf. verbessert werden muss.

In der Deutschen Rentenversicherung wird der Informationssicherheitsprozess durch die hierarchisch aufgebaute Informationssicherheits-Policy (ISP) unterstützt.

Diese gliedert sich in:

1. Allgemeine Zielfestlegungen (Ebene 1 - diese Leitlinie).
2. Verbindliche Grundzüge der Informationssicherheit (Ebene 2).
3. Richtlinien zu Teilbereichen der Informationssicherheit (Ebene 3).
4. Konzepte zu Teilbereichen der Informationssicherheit (Ebene 4) und
5. Handlungsanweisungen (Ebene 5).

Dabei schränken Festlegungen auf höherer Ebene den Regelungsspielraum der darunter liegenden Ebenen ein. Während Richtlinien und Konzepte teilweise rentenversicherungsweit verbindlich festgelegt werden, unterliegt die Ausgestaltung der Handlungsanweisungen den einzelnen Trägern der Deutschen Rentenversicherung. Das Ebenenmodell der Informationssicherheits-Policy ist in der **Anlage** grafisch dargestellt.

6 Verstöße und Sanktionen

Vorsätzliche oder grob fahrlässige Handlungen, welche die Schutzziele der Informationssicherheit gefährden, werden als Verstöße verfolgt und können durch Maßnahmen des Arbeitsrechts, des Disziplinarrechts, des Strafrechts oder des Ordnungswidrigkeitsrechts geahndet werden.

7 Aktualisierung der Sicherheitsleitlinie

Die Leitlinie zur Informationssicherheit sowie deren Umsetzung sind in regelmäßigen Abständen durch das für die Koordinierung der Informationssicherheit in der DRV-IT zuständige Gremium[3] auf ihre Aktualität und Angemessenheit hin zu prüfen. Die Leitlinie muss zudem bei Änderungen von Rahmenbedingungen, Geschäftszielen, Aufgaben oder der Informationssicherheitsstrategie überprüft und gegebenenfalls aktualisiert werden.

[3] Zum derzeitigen Stand liegt die Zuständigkeit beim IT-Lenkungsausschuss (ITLA)

Ebenenmodell der Informationssicherheit-Policy der Deutschen Rentenversicherung