Sicherheitskonzept Maßnahme Direkt

Das Sicherheitskonzept von Maßnahme Direkt erstreckt sich über drei Ebenen:

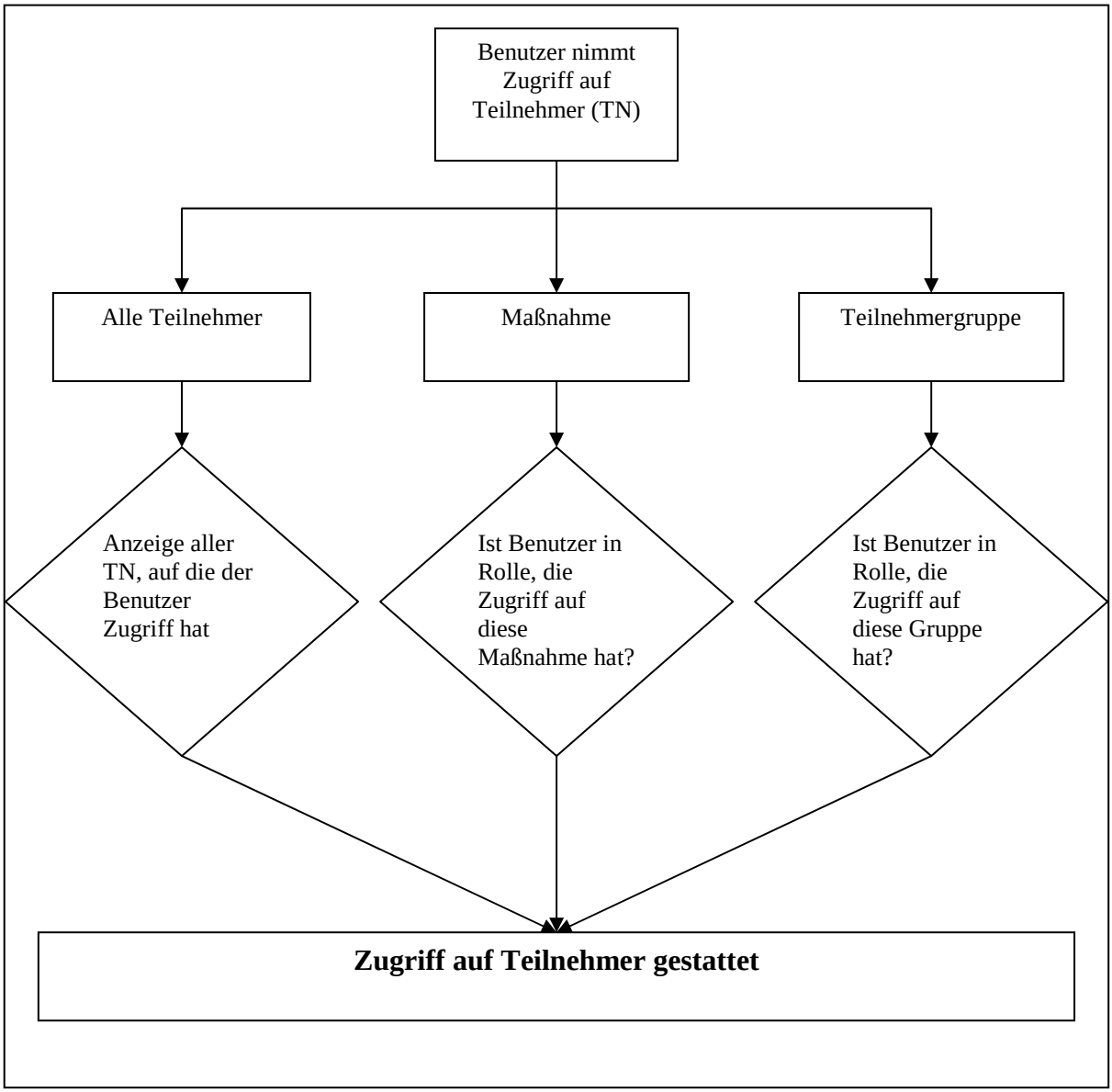
- Schutz vor unberechtigtem Zugriff auf Teilnehmer
- Schutz vor unberechtigtem Zugriff auf Programmfunktionen
- Protokollierung

Das Konzept wurde so umgesetzt, dass alle Datenschutzanforderungen gem. SGB X und Bundesdatenschutzgesetz umgesetzt werden können und dennoch eine hohe Flexibilität erreicht wird.

1. Zugriff auf Teilnehmer

Das Zugriffsrecht auf bestimmte Teilnehmer wird realisiert durch die Mitgliedschaft eines Benutzers in mehreren Rollen und der Zuweisung der Rollen, auf bestimmte Teilnehmergruppen bzw. Maßnahmen.

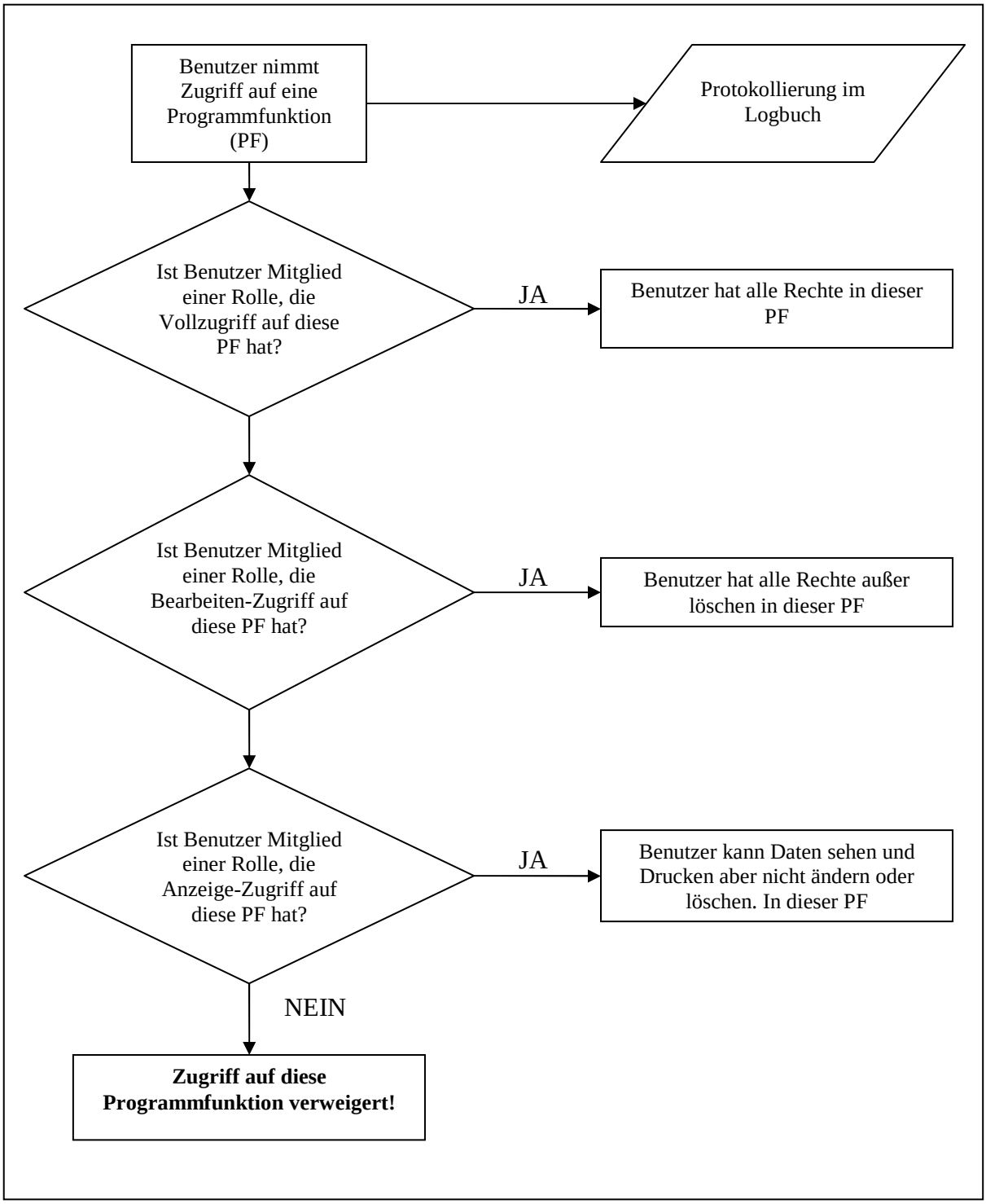
Die Sicherheitsprüfung läuft folgendermaßen ab:



2. Zugriff auf Programmfunktionen

Der Zugriff auf bestimmte Programmfunktionen ergibt sich aus der Mitgliedschaft des Benutzers in den Rollen.

Die Sicherheitsprüfung läuft folgendermaßen ab:

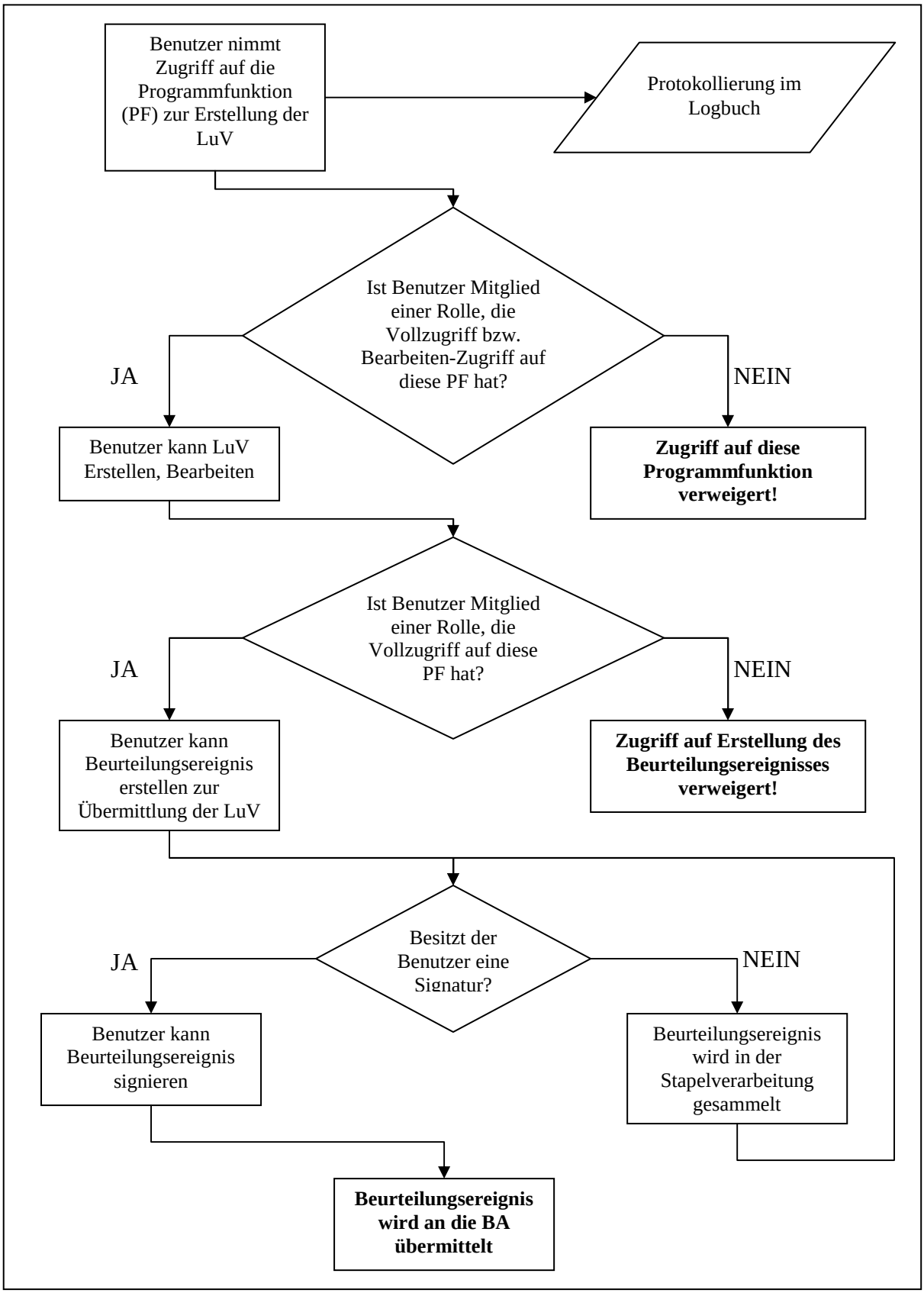


Für folgende Programmfunktionen lässt sich die Zugriffberechtigung festlegen:

- Stammdaten der Maßnahme
- Planung der Maßnahme
- Anwesenheit aller Teilnehmer einer Maßnahme
- maßnahmebezogene Nachrichten
- allg. Stammdaten des Teilnehmers
- zusätzliche Informationen des Teilnehmers
- Beruf- und Schuldaten des Teilnehmers
- Maßnahmedaten des Teilnehmers
- Anwesenheit des Teilnehmers
- Leistungs- und Verhaltensbeurteilung des Teilnehmers
- Kompetenzerfassung des Teilnehmers
- Maßnahmeplanung des Teilnehmers
- Zielvereinbarungen für Teilnehmers
- Soz.-Päd.-Betreuung des Teilnehmers
- Praktika und Kurse des Teilnehmers
- Qualifizierungsbausteine des Teilnehmers
- Verlaufs- und Erfolgskontrolle des Teilnehmers
- Kundenprofil
- Notizen zum Teilnehmers
- teilnehmerbezogene Nachrichten
- Teilnehmers verwalten
- Maßnahme/Bereiche
- Teilnehmergruppen
- Benutzerrollen
- Benutzer
- Schulfächer
- Schulabschlüsse
- Qualifizierungsbausteine
- Firmen
- eM@w-Protokoll

3. Erstellung und Signierung der LuV

Die Sicherheitsprüfung läuft folgendermaßen ab:



4. Beispiel Zugriff auf Teilnehmer

Folgende Daten sind gegeben:

Teilnehmer:	- Teilnehmer A - Teilnehmer B - Teilnehmer C - Teilnehmer D
Teilnehmergruppen:	- TN-Gruppe 1 - TN-Gruppe 2 - TN-Gruppe 3
Benutzer:	- Benutzer 1 - Benutzer 2 - Benutzer 3
Rollen:	- Benutzer Standort A - Benutzer Standort B - Ausbilder A/B

Mitgliedschaften der Teilnehmer in den Teilnehmergruppen:

TN-Gruppe 1:	- Teilnehmer A - Teilnehmer B
TN-Gruppe 2:	- Teilnehmer C - Teilnehmer D
TN-Gruppe 3:	- Teilnehmer A - Teilnehmer C

Mitgliedschaften der Benutzer in den Rollen*:*

Benutzer Standort A:	- Benutzer 1
Benutzer Standort B:	- Benutzer 2
Ausbilder A/B:	- Benutzer 1 - Benutzer 3

Zugriffsrechte der Rollen auf die Teilnehmergruppen*:*

Benutzer Standort A:	- TN-Gruppe 1
Benutzer Standort B:	- TN-Gruppe 2
Ausbilder A/B:	- TN-Gruppe 3

Folgende Zugriffsrechte ergeben sich aus dieser Konstellation:

Benutzer 1:	Teilnehmer A (da Mitglied „Benutzer Standort A“) Teilnehmer B (da Mitglied „Benutzer Standort A“) Teilnehmer C (da Mitglied „Ausbilder A/B“)
Benutzer 2:	Teilnehmer C (da Mitglied „Benutzer Standort B“)

	Teilnehmer D (da Mitglied „Benutzer Standort B“)
Benutzer 3:	Teilnehmer A (da Mitglied „Ausbilder A/B“) Teilnehmer C (da Mitglied „Ausbilder A/B“)

Beachten Sie bitte, dass sich die Zugriffsrechte durch die Rollenmitgliedschaften addieren, wie im Beispiel des „Benutzer 1“ ersichtlich ist.

5. Beispiel Zugriff auf Programmfunktionen

Folgende Daten sind gegeben:

Benutzer:	Bildungsbegleiter Standort A Bildungsbegleiter Standort B Lehrkraft Standort A Lehrkraft Standort B
Rollen:	Bildungsbegleiter Lehrkräfte Benutzer Standort A Benutzer Standort B

Folgende Sicherheitseinstellungen sind gefordert:

Die Bildungsbegleiter beider Standorte sollen auf alle Programmfunktionen Zugriff haben.
Die Lehrkräfte beider Standorte sollen nur auf die Notizen Zugriff haben.

Richten Sie die Programmzugriffsrechte folgendermaßen ein:

Bildungsbegleiter:	Vollzugriff auf alle Programmfunktionen
Lehrkräfte:	Vollzugriff auf Notizen, kein Zugriff auf alle anderen Programmfunktionen
Benutzer Standort A:	Kein Zugriff auf alle Programmfunktionen
Benutzer Standort B:	Kein Zugriff auf alle Programmfunktionen

Weisen Sie den Benutzern folgende Rollen zu:

Bildungsbegleiter:	Bildungsbegleiter Standort A Bildungsbegleiter Standort B
Lehrkräfte:	Lehrkraft Standort A Lehrkraft Standort B
Benutzer Standort A:	Bildungsbegleiter Standort A Lehrkraft Standort A
Benutzer Standort B:	Bildungsbegleiter Standort B Lehrkraft Standort B

6. Sicherheitskonzept

Die Einrichtung der Zugriffs- und Programmrechte kann in größeren Instituten und in Kooperationen aufwendig sein.

Klären Sie also bitte im Vorfeld folgende Fragen ab:

- Welche Benutzer sollen auf welche Teilnehmer zugreifen können?
- Welche Aufgaben haben diese Benutzer?
- Welche Programmfunktionen benötigen sie aufgrund der Aufgabe?
- Welcher Benutzer benötigt eine Signatur?

Legen Sie dann Rollen für den Zugriff auf die Programmfunktionen an. Diese Rollen sollten auf keine Teilnehmergruppe oder Maßnahme Zugriff haben. Weiterhin legen Sie Rollen für den Teilnehmerzugriff an. Diese sollten wiederum keine Rechte auf alle Programmfunktionen haben. Weisen Sie dann jedem Benutzer die entsprechenden Rollen zu (also mindestens 2 Rollen). Durch die Addition dieser Rechte erhält der Benutzer alle Privilegien, die er benötigt und die Übersicht bleibt gewahrt.