



Violence
Prevention Network

Datenschutzerklärung

GRIDD PRO[®] - Soziale Diagnostik APP

Professionelle Begleitung in der individuellen Stärkung,
Integration, Distanzierung und Entwicklung

Ressourcenorientiertes Tool der Extremismusprävention

1 Einleitung

Die GRIDD PRO® APP von Violence Prevention Network gGmbH, Alt-Reinickendorf 25, 13407 Berlin, unterstützt Fachkräfte in der Extremismusprävention durch effiziente Dokumentations- und Diagnostikprozesse. Sie ermöglicht eine strukturierte Erfassung des Beratungsprozesses, um professionelle Arbeit zu unterstützen.

Der Datenschutz ist ein wesentliches Element, um die Integrität und Vertraulichkeit des Beratungsprozesses zu gewährleisten. Die GRIDD PRO® APP kommt ohne personenbezogene Datenerfassung aus und funktioniert in der richtigen Anwendung in anonymisierter Form, d. h. Nutzer*innen halten darin pädagogische Prozesse und keine sensiblen Klient*innendaten fest.

2 Geltungsbereich

Die GRIDD PRO® APP ist ausschließlich für den Einsatz im Bereich der Sozialen Diagnostik und der Extremismusprävention konzipiert. Die Nutzer*innen erkennen an, dass die App nur in diesem spezifischen Kontext verwendet werden darf.

Der Zugriff auf und die Nutzung der GRIDD PRO® APP sind nur autorisierten Personen gestattet. Diese Personen müssen eine entsprechende Schulung absolviert haben und im Besitz gültiger Zugangsdaten sein.

3 Daten, die erhoben werden

In der GRIDD PRO® APP werden verschiedene Arten von Daten erhoben, um die Beratungstätigkeit effektiv zu unterstützen. Dazu gehören:

1. Anonymisierte Klient*inneninformationen: Geschlecht, Geburtsjahr, persönliche Interessen, persönliche Einschränkungen und zusätzlich Maßnahmen und Termine zu Verhandlungen, Fallkonferenzen u. ä.
2. Anonymisierte Informationen und Notizen über den pädagogischen Prozess: Die Nutzer*innen, i. d. R. Fachkräfte der Extremismusprävention. Sie dokumentieren wichtige pädagogische Entwicklungsverläufe und Beratungsprozesse in anonymisierter Form.

4 Zweck der Datenerhebung

4.1 Kriterien, ob eine DSFA durchzuführen ist

4.1.1 **Allgemeines:** Eine DSFA ist für Verarbeitungsvorgänge durchzuführen, wenn diese wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen und wenn sich deren Risiken in Hinblick auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung geändert haben.

4.1.2 **Vorgaben aus der DSGVO:** Gemäß Artikel 35 Absatz 3 DSGVO ist insbesondere in folgenden Fällen eine DSFA durchzuführen:

- a) **Systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung, einschließlich Profiling, gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen:** Erwägungsgrund 71 DSGVO erwähnt in diesem Zusammenhang automatische Ablehnungen im Rahmen von Online-Einstellungsverfahren oder Online-Kreditanträgen ohne menschliche Prüfung.
- b) **Umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 DSGVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 DSGVO:** Darunter fallen personenbezogenen Daten, aus denen die „rassische“ oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen. Zusätzlich sind biometrische und genetische Daten, Gesundheitsdaten, Daten zum Sexualleben sowie zur sexuellen Orientierung und Daten zu strafrechtlichen Verurteilungen bzw. Straftaten und damit zusammenhängende Daten über Sicherungsmaßnahmen umfasst (in Anlehnung an Erwägungsgrund 75 DSGVO).
- c) **Systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche:** Darunter könnten Videoüberwachungsanlagen subsumiert werden, welche beispielsweise wesentliche Teile des öffentlichen Straßennetzes aufzeichnen.

4.1.3 **Empfehlungen der Artikel 29-Gruppe:** Die Artikel 29-Gruppe geht davon aus, dass bei Vorliegen von mindestens zwei der nachfolgend genannten Kriterien in den meisten Fällen eine DSFA erfolgen muss. Es kann jedoch auch vorkommen, dass bereits die Erfüllung eines einzigen der unten genannten Kriterien die Pflicht zur Durchführung einer DSFA auslöst.

- a) **Bewerten oder Einstufen:** Darunter fallen das Erstellen von Profilen und Prognosen, insbesondere auf der Grundlage von Aspekten, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, Zuverlässigkeit oder Verhalten, Aufenthaltsort oder Ortswechsel der Person betreffen (siehe Erwägungsgrund 71 DSGVO). Dieses Kriterium erfüllt beispielsweise eine Bank, welche Datenbanken von Kreditauskunfteien und/oder Betrugsdatenbanken und/oder Geldwäschedatenbanken nach ihren Kund*innen durchsucht bzw. auch ein Unternehmen, das anhand der Nutzung seiner Website bzw. der Navigation der Website durch die Nutzer*innen Verhaltens- oder Marketingprofile erstellt.

- b) **Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung:** Darunter fallen Verarbeitungstätigkeiten, auf deren Grundlage für Betroffene Entscheidungen getroffen werden sollen, „die Rechtswirkung(en) gegenüber natürlichen Personen entfalten“ oder diese „in ähnlich erheblicher Weise beeinträchtigen“ (siehe Art. 35 Abs. 3 lit. a) DSGVO). Dieses Kriterium ist erfüllt, wenn es zum Ausschluss oder zur Benachteiligung von Personen kommt. Verarbeitungstätigkeiten mit keinen oder wenigen Auswirkungen auf Personen fallen nicht unter dieses Kriterium. Weitere Ausführungen zu diesen Auffassungen/Vorstellungen sind in den Guidelines betreffend Profiling zu finden.
- c) **Systematische Überwachung:** Darunter fallen Verarbeitungstätigkeiten, die die Beobachtung, Überwachung oder Kontrolle von Betroffenen zum Ziel haben und beispielsweise auf über Netzwerke erfasste Daten zurückgreifen. Ein Beispiel könnte die systematische Überwachung der Arbeitsplatzrechner von Angestellten durch den*die Arbeitgeber*in sein. Des Weiteren sind Verarbeitungstätigkeiten umfasst, die die Beobachtung, Überwachung oder Kontrolle von Betroffenen zum Ziel haben und beispielsweise auf „eine systematische [...] Überwachung öffentlich zugänglicher Bereiche“ zurückgreifen. Hier ist es für betroffene Personen oft kaum möglich, diese Verarbeitungstätigkeiten zu verhindern. Oftmals wissen die betroffenen Personen in solchen Situationen nicht einmal, wer ihre Daten wie verwendet (gemäß Art. 35 Abs. 3 lit. c) DSGVO).
- d) **Verarbeitung von vertraulichen Daten oder höchstpersönlichen Daten:** Damit sind einerseits jene Daten gemeint, welche in den Artikeln 9 und 10 DSGVO angeführt sind (Verarbeitung besonderer Kategorien personenbezogener Daten – wie beispielsweise Gesundheitsdaten – sowie Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten). Hierunter fällt beispielsweise eine von einem Krankenhaus geführte Patient*innendokumentation. Andererseits fallen darunter auch Standortdaten, Finanzdaten, persönliche Dokumente, E-Mails, Tagebücher, Notizen aus E-Readern mit Notizfunktion sowie Informationen von Life-Logging-Anwendungen (gemäß Art. 35 Abs. 3 lit. c) DSGVO).
- e) **Datenverarbeitung im großen Umfang:** Für die Ermittlung, ob Verarbeitungstätigkeiten im großen Umfang vorliegen, sollten beispielsweise folgende Faktoren herangezogen werden: Zahl der Betroffenen, verarbeitete Datenmenge bzw. Datenelemente, Dauer der Datenverarbeitung und geografisches Ausmaß der Datenverarbeitung.
- f) **Abgleichen oder Zusammenführen von Datensätzen:** Damit sind Verarbeitungstätigkeiten gemeint, bei denen ein Abgleich bzw. eine Zusammenführung unterschiedlicher Datensätze zu unterschiedlichen Zwecken und/oder von verschiedenen für die Verarbeitung Verantwortlichen durchgeführt wurden. Zusätzlich muss der Abgleich bzw. die Zusammenführung in einer Weise stattfinden, der über die vernünftigen Erwartungen der Betroffenen hinausgeht.

- g) **Daten zu schutzbedürftigen Betroffenen:** Die Verarbeitung dieser Art von Daten stellt auf Grund des größeren Machtungleichgewichts zwischen Betroffenen und Verantwortlichen ein Kriterium dar. Hier geht es um Betroffene, die der Verarbeitung ihrer Daten nicht einfach zustimmen oder widersprechen können bzw. für die es nicht so leicht möglich ist, ihre Betroffenenrechte auszuüben. Zu den schutzbedürftigen Betroffenen gehören bspw. folgende Bevölkerungsgruppen: Kinder, **Arbeitnehmer*innen**, Teile der Bevölkerung mit besonderem Schutzbedarf (psychisch Kranke, Asylwerber*innen, Senior*innen, Patient*innen) und Betroffene in Situationen, in denen ein ungleiches Verhältnis zwischen der Stellung der*des Betroffenen und der der*des Verantwortlichen vorliegt.
- h) **Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen:** Damit sind Verarbeitungstätigkeiten gemeint, die innovative Methoden der Datenverarbeitung einsetzen, wie beispielsweise die Zugangskontrolle mit Hilfe eines Fingerabdrucks in Kombination mit einer Gesichtserkennung. Der Einsatz einer neuen Technologie kann ein hohes Risiko für die Rechte und Freiheiten einer natürlichen Person mit sich bringen und Grund für die Notwendigkeit einer DSFA sein. Auch Anwendungen des „Internet der Dinge“ (IoT) können sich erheblich auf den Alltag und das Privatleben von Personen auswirken und somit eine DSFA obligatorisch machen.
- i) **Fälle, in denen die Verarbeitung an sich „die betroffenen Personen an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags hindert“:** Dies beinhaltet Verarbeitungstätigkeiten, mit deren Hilfe Betroffenen der Zugriff auf eine Dienstleistung oder der Abschluss eines Vertrags gestattet, geändert oder verwehrt werden soll. Ein Beispiel dafür ist eine Bank, die anhand eines Abgleichs mit einer Datenbank einer Kreditauskunftei entscheidet, ob sie einem*einer Kund*in einen Kredit gewährt.

4.1.4 **Black- und Whitelists der Aufsichtsbehörden:** Die Aufsichtsbehörden haben Verordnungen zu erlassen, in denen Datenverarbeitungsvorgänge angeführt sind, für die jedenfalls eine DSFA (Blacklist) durchzuführen ist. Sie können zudem Listen veröffentlichen, in denen Datenverarbeitungsvorgänge angeführt sind, für die keine DSFA (Whitelist) durchzuführen ist (siehe Art. 35 Abs. 4 und 5 DSGVO).

4.1.5 **Prüfung dieser Kriterien:** Der Verantwortliche bzw. das DSFA-Team wird neben der Prüfung des Vorhandenseins eines hohen Risikos für die Rechte und Freiheiten der Betroffenen und ggf. einer gesetzlichen Befreiung von der Pflicht zur Durchführung einer DSFA die obigen Kriterien bei seiner Prüfung berücksichtigen.

4.2 Beschreibung und Bewertung der Vorgänge:

4.2.1 Bei der Durchführung der DSFA muss eine **systematische Beschreibung** der Verarbeitungsvorgänge erfolgen. Dazu ist es notwendig, die Verarbeitungsvorgänge aufzulisten und zu erläutern.

- 4.2.2 Zusätzlich sind die mit der Verarbeitungstätigkeit verfolgten **Zwecke** anzuführen. Denn personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“). Zusätzlich müssen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).
- 4.2.3 Stützt sich der Verantwortliche auf **berechtigte Interessen**, sind diese berechtigten Interessen zu erläutern. Ein berechtigtes Interesse liegt vor, wenn die Verarbeitung zur Wahrung der berechtigten Interessen der*des Verantwortlichen oder einer*eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.
- 4.2.4 Des Weiteren hat eine Bewertung zu erfolgen, warum die Verarbeitungstätigkeit in ihrer konkreten Ausprägung mit den angeführten Verarbeitungsvorgängen für den genannten Zweck **notwendig und verhältnismäßig** ist. Dabei sollte sich der*die Verantwortliche die Frage stellen, ob der Zweck der Verarbeitungstätigkeit wirklich nicht durch gelindere Mittel erreichbar ist, welche mit weniger personenbezogenen Daten auskommen. Außerdem sollte aus der Bewertung der Notwendigkeit und Verhältnismäßigkeit hervorgehen, dass bei der konkreten Ausgestaltung der Verarbeitungstätigkeit schon Datensicherheitsmaßnahmen zum Einsatz kommen.
- 4.2.5 Der*die Verantwortliche sollte gegebenenfalls den **Standpunkt der betroffenen Personen** einholen. Dabei erscheint es sinnvoll darauf zu achten, dass man von Mitgliedern unterschiedlicher Personenkategorien (Mitarbeiter*innen, Lieferant*innen, Kund*innen) Stellungnahmen erhält, sofern diese von der Verarbeitungstätigkeit betroffen sind. Die wesentlichen Aussagen und insbesondere Bedenken dieser Personen sollten dokumentiert werden.
- 4.2.6 Der*die **Datenschutzbeauftragte** ist frühzeitig in die DSFA einzubinden. So kann diese*r bei der Durchführung der DSFA schon in der Anfangsphase der DSFA beraten. Diese*r soll eine Stellungnahme abgeben.
- 4.3 Risikobewertung
- 4.3.1 Bei der anschließenden Risikobewertung werden mögliche Risiken für die Rechte und Freiheiten der betroffenen Personen identifiziert (**Risikoidentifikation**) und analysiert (**Risikoanalyse**).
- 4.3.2 Bei dieser Risikobewertung werden zwingend folgende **Risiken** bewertet:
- Verlust der Vertraulichkeit
 - Verlust der Integrität
 - Verlust der Verfügbarkeit, Belastbarkeit
- 4.3.3 Im Zuge der Risikoanalyse wird die Höhe des Risikos für die Rechte und Freiheiten natürlicher Personen (Risikowert) ermittelt. In einem ersten Schritt werden die **Eintrittswahrscheinlichkeit** einer Bedrohung sowie die zu erwartenden **Auswirkungen** wie folgt beurteilt:

Beurteilung der Eintrittswahrscheinlichkeit

Vernachlässigbar	Für die ausgewählte Risikoquelle scheint es nicht sehr wahrscheinlich zu sein, eine Schwachstelle eines unterstützenden Wertes auszunutzen, um eine Bedrohung eintreten zu lassen (zum Beispiel: Diebstahl von Papierdokumenten aus einem Raum, der durch ein Ausweislesegerät und einen Zugangscode gesichert ist).
Eingeschränkt	Für die ausgewählte Risikoquelle scheint es schwierig zu sein, eine Schwachstelle eines unterstützenden Werts auszunutzen, um eine Bedrohung eintreten zu lassen (zum Beispiel: Diebstahl von Papierdokumenten aus einem Raum, der durch ein Ausweislesegerät gesichert ist).
Signifikant	Für die ausgewählte Risikoquelle scheint es möglich zu sein, eine Schwachstelle eines unterstützenden Werts auszunutzen, um eine Bedrohung eintreten zu lassen (zum Beispiel: Diebstahl von Papierdokumenten aus einem Büro, welches nur zugänglich ist, nachdem man einen Empfang passiert hat).
Maximal	Für die ausgewählte Risikoquelle scheint es einfach zu sein, eine Schwachstelle eines unterstützenden Werts auszunutzen, um eine Bedrohung eintreten zu lassen (zum Beispiel: Diebstahl von Papierdokumenten aus einer öffentlich zugänglichen Lobby).

Einschätzung der Auswirkungen

Vernachlässigbar	Betroffene erleiden eventuell Unannehmlichkeiten, die sie aber mit einigen Problemen überwinden können.
Eingeschränkt	Betroffene erleiden eventuell signifikante Unannehmlichkeiten, die sie aber mit einigen Schwierigkeiten überwinden können.
Signifikant	Betroffene erleiden eventuell signifikante Konsequenzen, die sie nur mit ernsthaften Schwierigkeiten überwinden können.
Maximal	Betroffene erleiden eventuell signifikante oder sogar unumkehrbare Konsequenzen, die sie nicht überwinden können.

4.3.4 Bei der Bewertung der Eintrittswahrscheinlichkeiten und Auswirkungen sind alle bisher getroffenen technischen und organisatorischen Maßnahmen zu berücksichtigen.

4.3.5 Der Risikowert wird sodann mit folgender Formel berechnet:

$$\text{Risikowert} = \text{Eintrittswahrscheinlichkeit einer Bedrohung} \times \text{Schwere der Auswirkungen}$$

4.3.6 Aus dem Produkt der Auswirkung und der Eintrittswahrscheinlichkeit werden dann anhand der folgenden Matrix Risikoklassen (geringes, mittleres, hohes Risiko) gebildet:

	Maximal	mittel	mittel	hoch	hoch
	Signifikant	mittel	mittel	mittel	hoch
	Eingeschränkt	gering	mittel	mittel	mittel
Auswirkung	Vernachlässigbar	gering	gering	mittel	mittel
		Vernachlässigbar	Eingeschränkt	Signifikant	Maximal
		Eintrittswahrscheinlichkeit			

4.3.7 Die jeweilige Risikobewertung wird anhand des anliegenden Dokuments „Vorlage DSFA“ durchgeführt und dokumentiert.

4.4 Abhilfemaßnahmen und Risikobehandlung

4.4.1 Gemäß Art. 35 Abs. 7 lit. d) DSGVO hat der*die Verantwortliche sicherzustellen, dass „die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.“

4.4.2 Identifizierte Risiken werden zeitnah und priorisiert behandelt, indem geeignete Maßnahmen zur Risikominimierung (Setzen von Maßnahmen), insbesondere gemäß den Anforderungen des Art. 32 Abs.1 DSGVO, Risikovermeidung (Unterlassen der risikobehafteten Aktivität), Risikotransfer (Auslagerung von Risikofolgen auf Dritte) oder Risikoakzeptanz (bewusste Entscheidung, keine weiteren Maßnahmen zu treffen) definiert, dokumentiert und umgesetzt werden.

4.4.3 Sofern Risiken durch die Einleitung von Maßnahmen verringert werden sollen, kann eine entsprechende Maßnahmenliste geführt werden, die die geplanten Maßnahmen, die Verantwortlichkeiten und die Umsetzungsfristen dokumentiert.

4.5 Risikobewertung nach getroffenen Maßnahmen

4.5.1 Schließlich ist das Risiko unter Berücksichtigung der getroffenen Maßnahmen erneut zu bewerten und zu dokumentieren.

- 4.5.2 Wenn aus der durchgeführten DSFA hervorgeht, dass die Verarbeitung ein hohes Risiko für die Betroffenen zur Folge hätte und keine Maßnahmen zur Eindämmung des Risikos mehr getroffen werden können, muss vor der Aufnahme der Verarbeitung die Aufsichtsbehörde konsultiert werden.
- 4.5.3 Nach Fertigstellung der DSFA sollten die Ergebnisse dem Topmanagement bzw. der Geschäftsführung zur Abzeichnung und Genehmigung vorgelegt werden.

5 Verbesserung des Verfahrens

Dieses Verfahren wird regelmäßig hinsichtlich der Umsetzung, Angemessenheit und Effektivität auf einen Anpassungs- oder Ergänzungsbedarf hin überprüft und gegebenenfalls aktualisiert.

Änderungen dieses Verfahrens sind formlos wirksam. Die Mitarbeiter*innen werden umgehend und in geeigneter Art und Weise über die geänderten Vorgaben in Kenntnis gesetzt.