Violence
Prevention Network

Privacy policy GRIDD PRO® - Social diagnostics APP

Professional support for individual strengthening, integration, distancing and development

Resource-orientated tool for preventing extremism

1 Introduction

The GRIDD PRO® APP from Violence Prevention Network gGmbH, Alt-Reinickendorf 25, 13407 Berlin, supports professionals in the prevention of extremism through efficient documentation and diagnostic processes. It enables structured recording of the counselling process in order to support professional work.

Data protection is an essential element in ensuring the integrity and confidentiality of the counselling process. The GRIDD PRO® APP does not require the collection of personal data and functions in anonymised form when used correctly, i.e. users record educational processes and no sensitive client data.

2 Scope of application

The GRIDD PRO® APP is designed exclusively for use in the field of social diagnostics and the prevention of extremism. Users recognise that the app may only be used in this specific context.

Only authorised persons are permitted to access and use the GRIDD PRO® APP. These persons must have completed appropriate training and be in possession of valid access data.

3 Data that is collected

Various types of data are collected in the GRIDD PRO® APP to effectively support counselling activities. These include

1. Anonymised client information: Gender, year of birth, personal interests, personal restrictions and additional measures and dates for negotiations, case conferences, etc.
2. Anonymised information and notes on the educational process: The users, usually specialists in the prevention of extremism. They document important educational development and counselling processes in anonymised form.

4 Purpose of data collection

4.1 Criteria as to whether a DPIA is to be carried out

4.1.1 **General:** A DPIA must be carried out for processing operations if they are likely to result in a high risk to the rights and freedoms of natural persons and if their risks have changed with regard to the type, scope, circumstances and purposes of the processing.

4.1.2 **Requirements from the GDPR:** According to Article 35 (3) GDPR, a DPIA must be carried out in the following cases in particular:

a) **Systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and which serves as a basis for decisions that produce legal effects concerning natural persons or similarly significantly affect them:** Recital 71 GDPR mentions in this context automated refusals in the context of online recruitment procedures or online credit applications without human review.

b) **Extensive processing of special categories of personal data pursuant to Article 9(1) GDPR or of personal data relating to criminal convictions and offences pursuant to Article 10 GDPR:** This includes personal data revealing "racial" or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership. It also includes biometric and genetic data, health data, data concerning sex life and sexual orientation and data relating to criminal convictions or offences and related data on security measures (based on recital 75 GDPR).

c) **Systematic, extensive surveillance of publicly accessible areas:** This could include video surveillance systems that record significant parts of the public road network, for example.

4.1.3 **Recommendations of the Article 29 Working Party:** The Article 29 Working Party assumes that a DPIA must be carried out in most cases if at least two of the following criteria are met. However, it may also be the case that the fulfilment of just one of the criteria listed below triggers the obligation to carry out a DPIA.

a) **Evaluating or categorising:** This includes profiling and predicting, in particular on the basis of aspects relating to the work performance, economic situation, health, personal preferences or interests, reliability or behaviour, place of residence or relocation of the person (see recital 71 GDPR). This criterion is met, for example, by a bank that searches credit reference agency databases and/or fraud databases and/or money laundering databases for its customers or by a company that creates behavioural or marketing profiles based on the use of its website or the navigation of the website by users.

b) **Automated decision-making with legal effect or similarly significant effect:** This includes processing activities on the basis of which decisions are to be made for data subjects "which produce legal effect(s) concerning natural persons" or "similarly significantly affect them" (see Art. 35 para. 3 lit. a) GDPR). This criterion is met if persons are excluded or disadvantaged. Processing activities with no or little impact on individuals do not fall under this criterion. Further information on these views/conceptions can be found in the guidelines on profiling.

c) **Systematic monitoring:** This includes processing activities that aim to observe, monitor or control data subjects and, for example, utilise data collected via networks. An example could be the systematic monitoring of employees' workstations by the employer. It also includes processing activities that aim to observe, monitor or control data subjects and, for example, rely on "systematic [...] monitoring of publicly accessible areas". It is often almost impossible for data subjects to prevent these processing activities. In such situations, data subjects often do not even know who is using their data and how (pursuant to Art. 35 (3) (c) GDPR).

d) **Processing of confidential data or highly personal data: On the** one hand, this refers to the data listed in Articles 9 and 10 GDPR (processing of special categories of personal data - such as health data - and processing of personal data relating to criminal convictions and offences). This includes, for example, patient documentation kept by a hospital. On the other hand, this also includes location data, financial data, personal documents, emails, diaries, notes from e-readers with a note function and information from life-logging applications (pursuant to Art. 35 para. 3 lit. c) GDPR).

e) **Data processing on a large scale: The** following factors, for example, should be used to determine whether processing activities are carried out on a large scale: Number of data subjects, amount of data or data elements processed, duration of data processing and geographical scope of data processing.

f) **Matching or merging of data sets:** This refers to processing activities in which matching or merging of different sets of data for different purposes and/or by different controllers has been carried out. In addition, the matching or merging must take place in a way that goes beyond the reasonable expectations of the data subjects.

g) **Data on vulnerable data subjects:** The processing of this type of data is a criterion due to the greater imbalance of power between data subjects and controllers. This concerns data subjects who cannot easily consent to or object to the processing of their data or for whom it is not so easy to exercise their data subject rights. Vulnerable data subjects include, for example, the following population groups Children, **employees**, parts of the population with special protection needs (mentally ill people, asylum seekers, senior citizens, patients) and data subjects in situations where there is an unequal relationship between the position of the data subject and that of the controller.

h) **Innovative use or application of new technological or organisational solutions:** This refers to processing activities that use innovative methods of data processing, such as access control using a fingerprint in combination with facial recognition. The use of a new technology can entail a high risk to the rights and freedoms of a natural person and be the reason for the need for a DPIA. Applications of the
"The Internet of Things (IoT) can have a significant impact on people's everyday lives and private lives, making a DPIA mandatory.

i) **Cases in which the processing itself "prevents data subjects from exercising a right or using a service or performing a contract":** This includes processing activities that are intended to allow, modify or deny data subjects access to a service or the conclusion of a contract. An example of this is a bank that decides whether to grant a customer credit based on a comparison with a credit agency database.

4.1.4 **Blacklists and whitelists of the supervisory authorities:** The supervisory authorities must issue regulations in which data processing operations are listed for which a DPIA (blacklist) must be carried out in any case. They may also publish lists of data processing operations that do not require a DPIA (whitelist) (see Art. 35 (4) and (5) GDPR).

4.1.5 **Examination of these criteria:** The controller or the DPIA team will take the above criteria into account in its assessment in addition to examining the existence of a high risk to the rights and freedoms of data subjects and, if applicable, a legal exemption from the obligation to carry out a DPIA.

4.2 Description and evaluation of the processes:

4.2.1 When carrying out the DPIA, a **systematic description** of the processing operations must be provided. For this purpose, it is necessary to list and explain the processing operations.

4.2.2 The **purposes** pursued with the processing activity must also be stated. This is because personal data must be collected for specified, explicit and legitimate purposes and must not be further processed in a manner incompatible with those purposes ("purpose limitation"). In addition, personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed ("data minimisation").

4.2.3 If the controller relies on **legitimate interests**, these legitimate interests must be explained. A legitimate interest exists if the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

4.2.4 Furthermore, an assessment must be made as to why the processing activity in its concrete form with the specified processing operations is **necessary and proportionate** for the stated purpose. In doing so, the controller should ask themselves whether the purpose of the processing activity really cannot be achieved by less intrusive means that require less personal data. In addition, the assessment of necessity and proportionality should show that data security measures are already being used in the specific organisation of the processing activity.

4.2.5 The controller should seek the **views of the data subjects** where appropriate. In doing so, it seems sensible to ensure that opinions are obtained from members of different categories of persons (employees, suppliers, customers) if they are affected by the processing activity. The main statements and, in particular, concerns of these persons should be documented.

4.2.6 The **data protection officer** must be involved in the DPIA at an early stage. This allows them to advise on the implementation of the DPIA in the initial phase of the DPIA. This person should provide an opinion.

4.3 Risk assessment

4.3.1 In the subsequent risk assessment, potential risks to the rights and freedoms of data subjects are identified (**risk identification**) and analysed (**risk analysis**).

4.3.2 The following **risks** must be **assessed** in this risk assessment:

- Loss of confidentiality
- Loss of integrity
- Loss of availability, resilience

4.3.3 As part of the risk analysis, the level of risk to the rights and freedoms of natural persons (risk value) is determined. In a first step, the **probability of** a threat **occurring** and the expected **impact** are assessed as follows:

Assessment of the probability of occurrence	
Negligible	For the selected risk source, it does not seem very likely to exploit a vulnerability of a supporting asset to allow a threat to materialise (for example: theft of paper documents from a room secured by an ID card reader and an access code).
Restricted	For the selected risk source, it seems difficult to exploit a vulnerability of a supporting asset to allow a threat to materialise (for example: theft of paper documents from a room secured by an ID card reader).
Significant	For the selected risk source, it seems possible to exploit a vulnerability of a supporting asset to allow a threat to materialise (for example: theft of paper documents from an office that is only accessible after passing through a reception).
Maximum	For the selected risk source, it seems easy to exploit a vulnerability in a supporting asset to allow a threat to materialise (for example: theft of paper documents from a publicly accessible lobby).
Assessment of the impact	
Negligible	Those affected may experience discomfort, but they can overcome this with a few problems.
Restricted	Those affected may suffer significant inconvenience, which they can overcome with some difficulty.
Significant	Those affected may suffer significant consequences that they can only overcome with serious difficulties.
Maximum	Those affected may suffer significant or even irreversible consequences that they cannot overcome.

4.3.4 When assessing the probability of occurrence and impact, all technical and organisational measures taken to date must be taken into account.

4.3.5 The risk value is then calculated using the following formula:

Risk value = probability of occurrence of a threat x severity of the impact

4.3.6 Risk classes (low, medium, high risk) are then formed from the product of the impact and the probability of occurrence using the following matrix:

Maximum	medium	medium	high	high
Significant	medium	medium	medium	high
Restricted	low	medium	medium	medium
Negligible	low	low	medium	medium
Impact	Negligible	Restricted	Significant	Maximum

Probability of occurrence

4.3.7 The respective risk assessment is carried out and documented using the attached "DPIA template" document.

4.4 Remedial actions and risk treatment

4.4.1 Pursuant to Art. 35 (7) (d) GDPR, the controller must ensure that "the measures envisaged to address the risks, including safeguards, security measures and procedures, are in place to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned".

4.4.2 Identified risks are dealt with promptly and prioritised by defining, documenting and implementing suitable measures to minimise risk (taking measures), in particular in accordance with the requirements of Art. 32 (1) GDPR, risk avoidance (refraining from the risky activity), risk transfer (outsourcing of risk consequences to third parties) or risk acceptance (conscious decision not to take any further measures).

4.4.3 If risks are to be reduced by introducing measures, a corresponding list of measures can be kept that documents the planned measures, responsibilities and implementation deadlines.

4.5 Risk assessment after measures taken

4.5.1 Finally, the risk must be reassessed and documented, taking into account the measures taken.

4.5.2 If the DPIA carried out shows that the processing would result in a high risk for the data subjects and no further measures can be taken to mitigate the risk, the supervisory authority must be consulted before processing begins.

4.5.3 Once the DPIA has been finalised, the results should be submitted to top management or the executive board for sign-off and approval.

5 Improving the process

This procedure is regularly reviewed with regard to its implementation, appropriateness and effectiveness to identify any need for adjustments or additions and updated if necessary.

Changes to this procedure are effective informally. The employees will be informed immediately and in an appropriate manner about the changed requirements.