GUIDANCE ON

PROMISE Hub and Data Protection

For a video introduction and technical walk through of PROMISE Hub, see this webinar.
Registered users have access to their Barnahus' Hub at: http://hub.barnahus.eu

What is this guidance about?

This guidance clarifies and provides guidance on how to manage the roles and responsibility of PROMISE Hub users to ensure compliance with data protection laws when deploying and managing the PROMISE Hub.

What is the PROMISE Hub?

The PROMISE Hub is a case management software, developed by Bonigi, and provided by the PROMISE Barnahus Network that has been developed to support multidisciplinary case management in Barnahus. It provides Barnahus with a simple tool to:

- record the daily events in each case, thereby providing a useful case management tool;
- measure performance at each Barnahus, nationally, and internationally on progress towards meeting the PROMISE Barnahus Quality Standards;
- collect comparable European data on violence against children and their interventions, which may be used to influence policy, law and practice.

Why does PROMISE provide a case management tool for Barnahus?

The UN Committee on the Rights of the Child (CRC) promotes effective procedures for the implementation of children's right to be protected from violence, including interagency coordination. Interagency case planning, supported by procedures, protocols and documentation, is important to ensuring multidisciplinary, coordinated, efficient and relevant interventions by the interagency team and the respective agencies.

Case documentation and tracking enables the team, in accordance with legal requirements and the best interest of the child, to collect and share information so that specific cases can be consulted and revisited through all stages of the investigative and judicial process. Case documentation and tracking can furthermore allow the interagency team to monitor progress and outcomes of cases referred to the service. The Hub also supports Barnahus to monitor their progress against Barnahus Quality standards, drawing on the case data that is entered into the tool.

The PROMISE Barnahus Quality Standard 5 provides guidance for interagency case management including case documentation and tracking.

5.3 Continuous case tracking: The Barnahus ensures continuous documentation and access to relevant case information for interagency team members on the progress of the case until the case is closed, observing national laws on data protection, privacy and confidentiality.

To implement standard 5.3, it is recommended that the Barnahus systematically documents case specific information, including but not limited to: the victim's and family's demographics, number of multidisciplinary case review meetings held, agency representation at these meetings, and case specific interventions such as forensic interviews (including observation), crisis support, therapeutic and medical interventions, follow up meetings etc.

The Hub also provides an opportunity to implement aspects of the standards concerning child participation, including an integrated questionnaire for children, and the possibility to extract a "child log", which gives children and caregivers an overview of the child's journey and case events in Barnahus.

Does the PROMISE Hub software comply with data protection laws?

Laws and procedures concerning data protection and confidentiality often shape multidisciplinary information exchange, joint case documentation and storage of data in Barnahus. In the EU, the General Data Protection Regulation (GDPR) provides a legal framework that sets guidelines for the collection and processing of personal information from individuals in the European Union (EU).

The PROMISE Hub software was designed to allow Barnahus to register case specific data in full compliance with data protection laws, if it is used in accordance with its purpose to collect anonymised data and, in full respect of the Hub guidelines that address user related risks caused by incorrect or inappropriate user practice.

A GDPR assessment of the PROMISE Hub, carried out by LINALTEC AB, concluded that there are no inherent risks in the software per se, but that there are potential user related risks in terms of (a) insecure login and password management (b) inappropriate and/or incorrect recording of personal data, which compromises the anonymity of the data that is entered in the system.

The GDPR assessment further concluded that (a) the Hub has a legitimate purpose for collecting information (b) it does not require requesting for permission to collect the information due to its legitimate purpose (c) the system only prompts collection of information that is anonymised.

What is a Data Protection Impact Assessment?

A DPIA is a process for identifying, quantifying, and mitigating the risks to data privacy associated with the processing of personal data. It is undertaken to ensure appropriate controls are in place when a new process is implemented, or an existing process undergoes a change, which potentially can result in a risk to personal data.

Article 35 of the General Data Protection Regulation (GDPR) states that a Data Protection Impact Assessment (DPIA) must be conducted by a Controller wherever data processing, in particular using new technologies, is likely to result in a high risk to the rights and freedoms of individuals. The GDPR also sets out several other instances in which Controllers must conduct a DPIA. If required, a DPIA must be completed prior to commencing the relevant data processing activity.

Under GDPR, the organisation that implements the PROMISE Hub would be considered a "Controller" of personal data, as the organisation determines the purpose and means of processing for the personal data it collects from service users.

Who is responsible for ensuring compliance with data protection laws when using the Hub?

Compliance with data protection laws through appropriate and correct deployment, management and use of the PROMISE Hub is the sole responsibility of the Barnahus, similar service or other user that implements the PROMISE Hub and controls the data that is entered into it (the Controller). The PROMISE Network and Bonigi do not assume responsibility for risks and breaches of law that is caused by incorrect and inappropriate deployment, management, and use of the PROMISE Hub.

To support the use of PROMISE Hub, this guidance, and a webinar introduce an overview of user related risks and examples of good practice to reduce such risks. It is highly recommended that all Barnahus that introduce the PROMISE Hub develop strict user terms, which clearly set out the terms and conditions for safe use of the PROMISE Hub, based on the information shared in this guidance and the webinar.

To ensure appropriate and correct deployment, management, and use of the PROMISE Hub in your national legal context, it is always best to consult with data protection experts in your country. As noted above, the GDPR analysis concludes that the system only collects anonymised data, however, in some contexts, it may be recommended to perform a Data Protection Impact Assessment (DPIA) due to the sensitive nature of the data, often related to vulnerable individuals, that is collected. It is therefore recommended that each organisation makes their own assessment and decision whether to perform a DPIA or not.

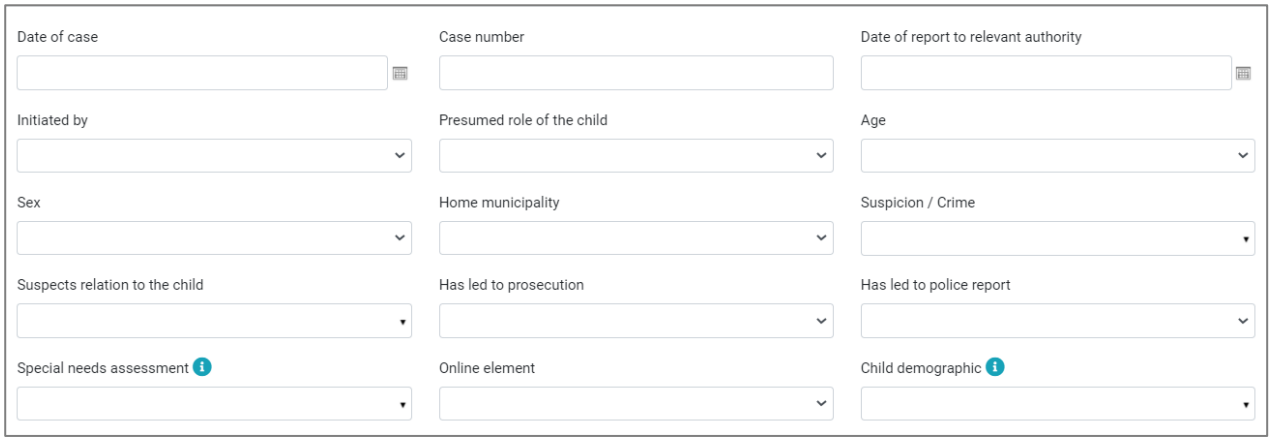
PROMISE further recommends that all services that use the Hub develop a data protection policy which, among other things, provide a description of roles and responsibilities for case specific information sharing and documentation including confidentiality, privacy, and data protection, including where and how data is stored. A detailed description of the procedures and considerations for documentation of case specific information can also be included. In addition to the data protection policy, it is recommended that terms for use and user agreements are put in place.

For data protection policy inspiration, see the Lighthouse Data Protection Policy v1.0 as an example, accessed as part of the Child House Toolkit.

For terms of use, see the sections concerning risks below. For user agreement, see the template provided at the end of this document.

What kind of information is stored and used centrally and for what purpose?

Core case data include the following:



Additional data is entered into a case timeline which records which activities or interventions were done, by which professional types, and under which conditions. Each of these variables is mapped in the statistics to show how actual practice in the service is or is not meeting the Barnahus Quality Standards.

Hub additionally collects brief data about consultations – that is, times they give advice about cases which have not yet come to the service – and also details about the management, coordination, and outreach of the service. Again, each of these variables is mapped in the statistics to show how actual practice in the service is or is not meeting the Barnahus Quality Standards.

Progress towards meeting the Barnahus Quality Standards

Drawing on the entries made by the service in their respective systems, the PROMISE Network will be provided with completely anonymised data summaries about practice in the services that use the Hub, the types of cases that Barnahus see in Europe, overall progress against the Barnahus quality standards.

The results may be used internally by the service for their own reporting and development needs. If the service wishes to be accredited as Barnahus, they may be used by the PROMISE Network for evaluating the service for accreditation based on the Barnahus Quality Standards. The PROMISE Network will not publish information specific to a single Barnahus without the consent of the concerned Barnahus.

Comparable European data on violence against children and their interventions

Drawing on the entries made by the Barnahus in their respective systems, the PROMISE Network will be provided with completely anonymised data summaries about practice in the services that use the Hub, the types of cases seen in Europe and overall progress against the Barnahus quality standards.

The data will be used for the purpose of providing an overview of the status and practice of Barnahus and similar services in Europe, and can be used to contribute to policy, law, and practice reform.

How is the data secured?

Data entered in the Hub is encrypted via transparent data encryption and ssl communication. The data is then stored in a dedicated database in a Microsoft Azure SQL pool. All communication with the database is made through stored procedures. The application and the Database is located in Microsoft Azures facilities on Northern Ireland.

What are the key user related risks when using the PROMISE Hub and how can they be reduced?

Login and security threats

The highest level of risk concerns unauthorized access to the PROMISE Hub due to inappropriate or incorrect management and storage of log in credentials. This concerns for example loss of login credentials, inadequate passwords (too simple) and irresponsible storage and/or sharing of passwords between authorized users and unauthorized persons.

The log in procedure of PROMISE Hub is managed through Microsoft’s Multi Factor Authentication (MFA) log in procedure. The use of MFA adds a layer of protection to the log in process. When logging in, users

have to provide additional identity verification through a separate device (phone). Alternatives may be provided if your organisation does not currently have Microsoft accounts or if there are organisational restrictions that would prevent you from following the MFA log in procedure.

To address risks related to log in, it is recommended that:

- Access to the PROMISE Hub is restricted. Access to the PROMISE Hub should be granted based on a thorough evaluation of the relevance and appropriateness of each user and be made conditional on acceptance of the organisational data protection policy and the user terms of the PROMISE Hub.
- Each user is made aware of that inappropriate or incorrect management and storage of log in credentials pose a high level of risk of unauthorized access to the PROMISE Hub and potential breach of data.
- An organisational policy for how passwords are allocated, renewed, managed and stored is put in place. This may, for example, involve using a password manager. The requirements set out in the policy can be included in the user terms.

Sharing a personal log in is should always be considered a breach against the user terms of the PROMISE Hub.

Inappropriate and incorrect entry of data

As noted above, the PROMISE Hub only prompts collection of information that is anonymised. Personal data that is not anonymous should never be inserted in the PROMISE Hub.

The GDPR assessment concluded that the possibility in the PROMISE Hub to add free text entries, may pose a risk that users use this feature for the purpose of adding personal data in the system that is not anonymous. To address this risk, it is recommended that:

- Each organisation develops user terms, which include clear guidelines on what type of information can or cannot be inserted in the Hub in the free text entries, including a prohibition to add any information that may lead to the disclosure of the identity of the persons implied in the cases recorded in the PROMISE Hub. This includes for example names, contact details such as address or phone number, national identity or social security numbers or any other details that may lead to the identification of the child and his/her family.
- Each user is made aware of the risks involved in adding personal data in the free text entries to data protection and privacy breaches.

User agreement template

This template is meant to be used by an organisation when setting up a new Hub account for an employee. The purpose is so the new user of Hub is aware of their responsibilities and the resources available to them.

In becoming a use of PROMISE Hub, I confirm that I have read this usage guidance in its entirety. I confirm that:

- I will not share my login credentials or let anyone else use my account to access the Hub.
- I will ensure that my login credentials cannot be accessed by unauthorised persons.
- I will immediately report suspicion that my user credentials have been compromised or are misused.
- I will follow the data protection policy and the Hub user terms, including on what type of information can or cannot be inserted in the Hub, including in the free text entries.
- I will never enter names, contact details, personal identification numbers, or any other details that may lead to the identification of a child and their family.
- I will immediately report suspicion that case entries in the Hub may be in breach of the data protection policy and/or the Hub user terms.

DATE

SIGNATURE

NAME

TITLE

ORGANISATION

PROMISE

Implementing the Barnahus Quality Standards throughout Europe

PROMISE is supporting Europe to adopt the Barnahus model as a standard practice for providing child victims and witnesses of violence rapid access to justice and care. We undertake this work to fulfil the PROMISE vision: a Europe where the human rights of children to protection from violence, support and to be heard are fulfilled.

A Barnahus provides multi-disciplinary and interagency collaboration to ensure that child victims and witnesses of violence benefit from a child-friendly, professional and effective response in a safe environment which prevents (re)traumatisation. With the formal support from national authorities, PROMISE provides opportunities to translate national commitment into action and engage internationally in the process. In addition, regular networking and strategic communications continually activate our growing network of professionals and stakeholders who are committed to introducing and expanding Barnahus services nationally.

The first PROMISE project (2015-2017) set European standards and engaged a broad network of professionals. The second PROMISE project (2017-2019) promoted national level progress towards meeting the standards and formalised the PROMISE Barnahus Network. The current project (2020-2022) is expand these activities to include University training, case management tools, with a view to establishing a European Competence Centre for Barnahus and laying the groundwork for an accreditation system for Barnhaus.

PROMISE is managed by the Children at Risk Unit at the Council of the Baltic Sea States Secretariat in close collaboration with Child Circle.

Access the PROMISE tools and learn more at www.barnahus.eu

This document has been produced with the financial support of the Rights, Equality and Citizenship (REC) Programme (2014-2020) of the European Union. The contents herin are the sole responsibility of project partnership and can in no way be taken to reflect the views of the European Commission.