OSAS Portals – Frequently Asked Questions- FAQ - Data protection and privacy

Introduction

This frequently asked questions (FAQ) is intended to give guidance and information for portal users of the Online System for adult safeguarding regarding data protection and privacy issues.

The HSE and the National Safeguarding Office recognise that there is a diverse range of individuals, services and organisations who will use these portals for submission and delegation purposes. Therefore some of the details in the FAQ maybe of more relevance to services who are subject to oversight under the HSE Adult Safeguarding policy using the delegation portal in addition to the adult safeguarding portal. Please note that some detailed questions in the FAQ may be fully addressed answered by reference to the substantive information contained in the Data Protection Impact Assessment and Appendix (HSE Privacy Impact Assessment Form).

For further specific enquiries, the enquiry email for the National Safeguarding Office is safeguarding.socialcare@hse.ie

What is personal data?

Personal data is defined by General Data Protection Regulation (GDPR) as any information relating to an identifiable person who can be directly or indirectly identified, in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

Personal data information relating to the referrer or the adult deemed at risk of abuse allows the HSE to identify the person, such as name & address, contact phone numbers and email address. The HSE handle personal data in line with the (GDPR) and in general we process personal data as the provider of health services, carried out in the public interest. This applies to both general personal data and any special categories of personal data.

Please also refer to DPC guidance: 190710 Data Protection Basics.pdf

The DPC glossary of terms is also available here: Definition of Key Terms | Data Protection Commission

Why is personal data collected as part of adult safeguarding?

Under the Safeguarding Vulnerable Persons at Risk of Abuse Policy - National Policy and Procedures (2014), the HSE has a regional network of Safeguarding and Protection Teams (SPTs) who receive community referrals and preliminary screenings regarding adults who may be at risk of abuse.

The HSE Safeguarding and Protection Teams needs to collect and use certain necessary personal information on the person making the referral when this person submits a referral or screening notification via a portal on the online system for adult safeguarding . Personal information is also collected on the person who is the subject of the referral as the person deemed at risk of abuse. This information is necessary for the Safeguarding Teams to undertake their adult safeguarding legitimate professional duties. System C [previously known of Liquid Logic], a UK based IT company have been contracted by the HSE to support the online case management system for adult safeguarding and are a processor of data regarding notifications on the system submitted via online portals. The system is known as the Online System for Adult Safeguarding (OSAS).

The DPIA reflect the necessary personal data flows and business flow of the patient/service user information

What is meant by special category data?

Special categories of data are defined by the GDPR and include things like racial or ethnic origin, religious or philosophical beliefs, genetic data, biometric data, health data, sex life details and sexual orientation. Personal data on adults at risk of risk stored on OSAS can include health data.

Please also refer to DPC guidance: 190710 Data Protection Basics.pdf

The DPC glossary of terms is also available here: Definition of Key Terms | Data Protection Commission

What is the portal for submitting adult safeguarding concerns and preliminary screenings to the HSE Safeguarding and Protection Teams?

A web portal is a custom made website the gathers information, from various sources, in a uniform way. It serves as a single point of contact and gives users personalised content. There is a portal for submitting community referrals and preliminary screenings to the HSE Safeguarding and Protection Teams as part of the OSAS system.

What is the delegation portal for communication of tasks between services who submit preliminary screenings and HSE Safeguarding and Protection Teams?

As part of the OSAS system the delegation portal serves as a single point of web based contact in a uniform way for communication and delegation between the HSE Safeguarding Teams and the services who are subject to oversight under the HSE Adult Safeguarding policy.

What personal data is collected via these portals?

The OSAS portal registration requires the person referring the concern to submit their name, email address, and other contact details, for verification and in order for the HSE Safeguarding and Protection Team as required to contact the person regarding the referral or screening notification.

The referral or screening notification is the information the referrer shares with the HSE Safeguarding Team about the safeguarding concern and the person who may be at risk of abuse. This notification contains personal information on the adult deemed at risk of abuse.

The personal data identifiers collected are referenced in in the DPIA.

What personal information is requested to register and engage on the OSAS portal?

We may collect and use the following personal data about the person making the referral:
• name
• address
• contact details
• phone number
• email address
• IP address
• information about use of the website

Why does the HSE use personal data for registering and using the portal?
Any personal data we collect will only be used to:
• keep our website secure
• validate identity to register an account on the portals of the online system for adult safeguarding
• contact the person in order to screen and access details in a safeguarding concern relating to an adult who may be at risk of abuse or neglect

What personal data on the person in a vulnerable situation at risk of being abused is sought and collected on OSAS? Information recorded in a Preliminary Screening process or Safeguarding Plan:

Name
Home Address details
Current Address details
Eircode
Phone No
Date of Birth
Gender
Individual Health Identifier (IHI) Number
Service Organisation that Person is attending (if applicable):
Service Type that person is attending (if applicable)

Description of the adult at risk of abuse
Communication support needs of the adult at risk of abuse
Other services that may be involved with the adult at risk of abuse
Capacity and consent information
Funding arrangements (out-of-area placements), if applicable
Contact details on any nominated person that the adult at risk of abuse wants services to contact (if applicable)
Details of safeguarding concern
Date that concern or incident was raised
Details on who raised the concern or incident
Reporting category of concern
Setting / Location of concern
Centre Identification OSV number of a HIQA Designated Centre where concern arose
Wishes of the adult at risk of abuse in relation to the concern
Immediate actions taken regarding the concern
Any links to other preliminary screenings
Risk determination and escalation
Outcome of the Preliminary Screening
Identity of the person causing concern where required
Detail of the protective actions contained in the Safeguarding Plan,
Wishes of the adult at risk of abuse regarding their desired outcomes of a safeguarding plan

Why is privacy important in adult safeguarding?

It is important that personal information is kept safe and shared appropriately in line with a legal basis. Personal information should be shared only when necessary and used for the intended purpose.

Please also refer to the HSE Privacy Statement available at: Privacy Statement HSE.ie - HSE.ie

What is the OSAS privacy statement?

A privacy statement relates to privacy practices regarding a person's engagement online. We are committed to protecting your privacy and take the security of your information very seriously. We aim to be clear and transparent about the information we collect about you and how we will use that information. A privacy statement is included in bottom bar of the Web page on the notification portal.

Is personal data submitted on the portal safe and secure?

The HSE are committed to ensuring that personal information submitted on the OSAS portals is secure with us and with System C /Liquid Logic who process the information on our behalf. We have a number of security precautions in place to prevent the loss, misuse or alteration of submitted information. All staff working for the HSE have a legal duty to keep information confidential and all staff are trained in information security and confidentiality. The HSE has strict information security policies and procedures in place to ensure that information is safe whilst held electronically.

System C/Liquidlogic is subject to external audits for ISO27001 and ISO9001. These audits include the data protection responsibilities within their scope and include audit meetings and reviews with

the DPO. System C/ Liquidlogic are using Microsoft Azure data centres and details of compliance can be found at: https://learn.microsoft.com/en-us/azure/compliance/offerings/ The Company fully completed the IT Security Questionnaire required by the HSE's Chief Information Security Officers office.

Firewall: The system will have at least three tiers and each tier is segregated with a network security group. Security management is provided by a number of systems including Sophos Intercept-X, Invati Patch Management, Azure management policies, Qualys vulnerability monitoring. These are reviewed as part of ISO 27001:2013 accreditation.

Will personal data be used for any other purpose than the stated adult safeguarding purpose?

We will not use the data we collect for any other purposes without seeking consent. The DPIA covers only the planned data processing activities. We may use anonymised statistical data to analyse, plan and improve our services.

This website uses session cookies. Session cookies are used to deliver the basic functions of a website i.e. to allow pages to remember technical changes or selections you may make between pages. Session cookies are temporary cookies and are generally erased when you close your browser. This website does not use any third party or persistent cookies. Sessional cookies do not track activity on the website. The IP addresses is used for website security purposes and this is kept separate. The system does not collect IP addresses for analytics purposes beyond monitoring user traffic with tracking software to assist website design and layout.

Will personal data collected by OSAS be used for research purposes?

We will not use individual personal data for research purposes. We may use anonymised statistical data to analyse, plan and improve our services. The purpose of the DPIA is to cover primary processing and secondary processing activities for personal data such as research is not planned. The DPIA covers only the planned data processing activities. Research is not in scope for the purposes of this DPIA.

Is there a Business flow document?

Business flows are documented in the DPIA and appendices to the DPIA.

What is a data controller on OSAS?

Please refer to DPC guidance and definition. A data controller is the legal entity that determines how and why personal data is collected and used. The HSE is the data controller for all personal data that is collected and used by the Online System for Adult Safeguarding. HSE and HSE funded agencies are both independent data controllers for the information they collect about users of their services. The DPIA (titled: *privacy-impact-assessment-editable form OSAS safeguarding Version 0.9*) does not contain any reference to 'Joint Controllers' and uses term "Independent Data Controllers"

What is data processing?
Processing of personal data in any operation or set of operations including – collecting, recording, organising, structuring, erasing, destroying, altering, combining, disclosing or sharing the data.

What is a data processor?

The data processor processes personal data only on behalf of the controller. The data processor is usually a third party external to the company. Please refer to DPC guidance/definition above.

Who is the data Processor of information submitted on the OSAS portals?

The data processor in relation to information submitted onto the OSAS portals is a contracted IT company called System C/ Liquid Logic. System C is carrying out data processing on behalf of and under instructions from the HSE. System C has engaged Microsoft Azure as a sub-processor, for hosting purposes, to comply with the HSE requirement for data to be hosted within the EU. System C is acting as a Processor and the HSE is the Controller for the data processing concerned. The HSE has a data processing agreement with System C. The HSE is a data controller and is not considered a data processor in terms of information submitted on the OSAS portals. (Please refer to the DPIA for further information.)

How long will HSE Safeguarding Teams retain personal data submitted on OSAS?

All personal data collected is retained in accordance with the HSE Record Retention Policy. The HSE adult Safeguarding data retention guideline for social work records is that personal data should be considered for deletion at closure plus eight years after the person's death.

Who is responsible for overseeing retention and data minimisation on the system?

The Safeguarding Principal Social Worker as functional Head of Department would have regional responsibility for overseeing data minimisation and retention as per the Records Retention policy. The System Administrator in the National Safeguarding Office would undertake retention and deletion actions following direction from the function Head.

Who will have access to personal data on OSAS?

Only HSE safeguarding staff and contractors who have legitimate involvement with adult safeguarding activity will have access to personal data. All HSE staff and contractors who have access to personal data are bound to the HSE by confidentiality and data protection agreements. They must keep personal data secure and to use it only for the purposes specified by the HSE. Access will be audited to monitor compliance.

The System C/Liquid logic security model dictates that each region can only see concerns that are within their geographic area - Users will have an appropriate security profile that limits what information they can access and update. Access to specific sensitive information can be restricted to maintain data integrity direct database access is not supported For those staff approved for report creation a data warehouse is available, this restricts access to the live data and ensures that running reports does not impact on response times of the system

HSE Funded agencies already have access to the personal data submitted on the portal as independent data controllers. (Please refer to the DPIA for further information.)

What are access controls on OSAS?

Access to personal data is required by certain adult safeguarding staff such as Safeguarding social workers and their administrative support staff to carry out their jobs in relation to adult protection. Access controls are in place depending on role. These are necessary to verify user identity, most commonly by a unique user identity and password. The HSE has a policy providing guidance and best practice to support the use of strong passwords, additionally the system has a list of banned passwords. Each user has a profile right, this defines the data they can access and the tasks they may perform. Further information in the DPIA and operational procedure on access control .

How is the adult safeguarding data processed following submission on the portals?

There is a defined business process and stages in the adult safeguarding procedure as set out in the HSE Safeguarding Vulnerable Person at Risk of Policy 2014 which encompasses the collection and processing of necessary personal data on adults at risk of abuse. The HSE Safeguarding Teams have a legitimate role in relation to oversight of preliminary screenings and safeguarding plans submitted by services. Please see the Appendix to the Data Protection Impact Assessment for the stages and business flow chart.

What is the lawful basis for processing adult safeguarding information?

The HSE handles any all adult safeguarding data shared with us in line with the General Data Protection Regulation (GDPR). The HSE process adult safeguarding personal data as the provider of health services, carried out in the public interest. This applies to both general personal data and any special categories of personal data.

The HSE legal bases for processing adult safeguarding personal data includes tasks carried out in public interest vested in the data controller and vital interests. The HSE Adult Safeguarding system does not rely on consent as the legal basis to process personal or special category data when it relates to providing adult safeguarding services. The HSE has a legal basis to process the adult safeguarding data for this activity reliant on Article 6(1) (e), public interest, in conjunction with Article 9(2) (h).

What is the legal obligations of funded agencies as independent data controllers of adult safeguarding data?

While the HSE cannot advise other independent data controllers, these independent data controllers [for example HSE funded services] may seek to rely on the same lawful basis as the HSE. For this processing activity, the HSE relies on Articles 6(1)(e) and 9(2)(h) of the GDPR.

What is the data sharing agreement between the HSE and funded agencies for sharing information on the OSAS portals?

The purpose of the Data Sharing Agreement (DSA) between HSE funded agencies submitting preliminary screenings and the HSE is to set out the framework for the sharing of adult safeguarding data, including Personal Data and Special Categories of Personal Data, between each other as Independent Data Controllers. It defines the principles and procedures that the Parties shall adhere to and the responsibilities the Parties owe to each other. The HSE has prepared a Data Privacy Impact Assessment (DPIA) and drafted the Data Sharing Agreement as part of the administrative suite of safeguards under GDPR.

Is a Data Sharing Agreement (DSA) a legal requirement between the HSE and HSE funded agencies?

Both the DPIA and accompanying DSA are part of the administrative suite of safeguards under GDPR. The HSE has a standard template for a DSA which is an appropriate safeguard under GDPR. Whilst the Data Sharing Agreement is not a defined legal requirement it is viewed as a good governance and good practice between two independent data controllers in this context.

What is responsibility on the HSE to comply with the Data Sharing Governance Act (DSGA) and develop and register a Data Sharing Agreement with those agencies covered by the DSGA?

The DSGA is relevant where only personal data is shared between public bodies. In this instance, both personal and special category data is shared / processed on the system and the DSGA is therefore out of scope as a lawful basis.

Can a person be identified directly or indirectly from the data and at what stage in the processing?

Yes, the identification of a person who is deemed at risk of abuse is necessary for adult safeguarding by Safeguarding staff during the preliminary screening and follow up safeguarding planning purposes.

Who has systems administrative control over the system?

Please refer to the DPIA which sets out the procedures in place for systems administration including central administrator in the National Safeguarding Office as well as local management and administrator of data received by the regional Safeguarding and Protection Teams. Standard OSAS operational related questions may be answered by the regional Safeguarding team such as possible errors or incorrect details on submissions whilst specific overall system operational queries should be sent to the Senior Researcher or Systems Administrator in the National Safeguarding Office. The enquiry email for the National Safeguarding Office is safeguarding.socialcare@hse.ie

Is personal data going to be accessed for Inspection and health audit purposes?

Personal data can be accessed during Inspections by HIQA and the Mental Health Commission under regulatory legislation and for commissioned enquiry purposes commissioned by the Regional Executive Officer.

The HSE Internal Audit Charter gives Internal Audit (Healthcare Audit) full access to the records and resources to achieve the objectives on the audit as approved by the HSE Audit and Risk Committee. Internal Health Care Auditors are bound by the requirements of GDPR legislation and the HSE data protection policy. Healthcare Auditors may access personal records either in hard or soft copy at inspection sites, however they do not take these or copies of these from the sites and do not collect personal identifiers (name, address, age etc.). They only collect information that is necessary to achieve the purpose of the audit, all information is anonymised, and no information can be identified as related to any specific individual. Regarding clinical audit it should be noted that only pseudonymised data is entered into the national clinical audit system, MEG, and the data cannot be re-identified by NCCA or the third party provider.

Regarding HSE non health internal audit, the Internal Audit Division (or agents of the Internal Audit Division, in the case of ICT Audit - which would include Mazars auditors who act on behalf of the HSE) noted that they have full right of access to all management information needed to carry out its work. For further information please refer to HSE Internal Audit Charter and HSE's Internal Audit Process Guide prepared by the Office of the Chief Internal Auditor.

Who has responsibility for education on data privacy?

HSE and HSE funded agencies as data controllers both have responsibility to ensure that all their staff have adequate training to ensure all who use the system are aware of their responsibility and comply with the GDPR and security requirements.

The fundamentals of GDPR training course is available on HSELanD. Other healthcare providers can request access to HSELanD to complete same.

Is there guidance materials on using OSAS Portals?

Guidance document have been prepared to assist HSE and HSE funded services along with recorded webinars. Information can be sought from the National Safeguarding Office or by following link https://www.hse.ie/eng/about/who/socialcare/safeguardingvulnerableadults/report-an-adult-safeguarding-concern-online.html

Where is the business process map for adult safeguarding?

The business process map is available as an Appendix to the DPIA

What is a Super User?

Super user is a term to describe a person who engages and assists other users learning a new system. It is envisaged that a network of support will evolve for internal safeguarding teams utilising the case management system and among Designated Officers / Service Managers as per 2014 HSE Safeguarding Policy and Procedures within services who make regular submissions on the portals.

Are Mobile apps being used as part of OSAS?
At this stage of development of OSAS a mobile App is not part of the system

What arrangements are in place for informing data subjects?

Service users and persons supported who are data subjects are informed of processing via the Adult Safeguarding system preliminary screening and assessment process. Prompts are embedded in the Preliminary Screening Form regarding the necessity to inform and consult with the user/ patient on data processing requirements. This includes information to the patient/ service user to inform on how their information is being used and processed under the HSE adult safeguarding policy and procedure.

The direction to service providers is that there is a consistent principle and message on data privacy statement as the specific privacy notice format can take a variety of mediums dependent on the cognitive capacity and communication needs of the relevant users of services (i.e. easy read notice leaflet, use of video or animation explainer). Further work will be undertook by services to develop user friendly easy read privacy notice materials.

What is the role of the HSE Data Protection Office (DPO)?

The role of a DPO may be referred to in general in regard to the GDPR (see Articles 37, 38 and 39).The HSE has appointed a Data Protection Officer to oversee the HSE's compliance with its data protection obligations.

Contact details are available here: Data Protection Officer and Deputy Data Protection Officer contact details - HSE.ie

What are data subject's rights?

If you would like further information on data subject's rights, how to make an access request and how the HSE protects and manages personal data please use the following link:

https://www.hse.ie/eng/gdpr/gdpr-faq/hse-gdpr-faqs-public.pdf

How can a person make a complaint about how their personal data is being handled?

The HSE have legal obligations under the EU General Data Protection Regulations (GDPR) and the Data Protections Acts 1988 – 2018 to ensure all personal data which it collects and processes belonging to its patients, clients, staff and others is kept confidential and secure. To comply with these legal obligations the HSE have implemented a number of technical and organisational measures to protect the personal data it collects against unauthorised or unlawful processing, accidental loss, destruction or damage.

In the event that you wish to make a complaint about how your personal data is being processed by the HSE, or how your complaint has been handled, you have the right to lodge a complaint directly with the Data Protection supervisory authority and the HSE Data Protection Officer:

If you are not satisfied with how the HSE is processing your personal data, contact the HSE's Data Protection Officer .The HSE Data Protection Officer (DPO) can be contacted directly at dpo@hse.ie . If we are unable to resolve your complaint, you have the right to lodge a complaint directly with our supervisory authority, the Data Protection Commission.