TUSLA

An Ghníomhaireacht um Leanaí agus an Teaghlach
Child and Family Agency

Data Protection Unit (DPU)

# The CASP Data Protection Guidance

21 March 2022

Public

| | |
|---|---|
| **Revision Number** | Final |
| **Approval Date** | 21 March 2022 |
| **Next Revision Date** | Annual |
| **Document Developed By** | Tusla Data Protection Unit |
| **Document Approved By** | Tusla Data Protection Officer |
| **Responsibility for Implementation** | Relevant Staff |
| **Responsibility for Review** | Tusla Data Protection Unit |

# 1. Introduction

The Child Abuse Substantiation Procedure (CASP) is designed to provide a framework for Social Workers in assessing allegations of abuse made against an individual which give rise to a concern that the individual may pose a potential risk of harm to identified or identifiable children.

The procedure sets out the principles that CASP Social Workers are expected to apply to ensure fair procedures are afforded to PSAAs when they are undertaking a substantiation assessment of disclosures of child abuse.

Tusla ('we' 'us' 'our') is the data controller for the personal data processed as required by CASP because this process is part of Tusla's statutory obligations to Service Users and is a public task and exercise of official authority vested in Tusla.

Tusla can and should collect, use, share, amend, transfer, store (all of these activities are called 'processing') information about individuals that is personal data **only** if this information is required for Tusla to perform its role in relation to CASP as prescribed by section 3 of the Child Care Act 1991 or otherwise required or permitted by law.

Much of the data processed by Tusla under CASP invariably includes special category personal data and due to the services provided by Tusla, sensitive personal data including, but not limited to, data relating to health, physical, psychological, emotional and mental factors, details of allegations of abuse (both current and retrospective) whether physical, emotional or sexual. This processing often involves the personal data of children and adults all of whom by the nature of their status as Service Users and their relationship with Tusla would be considered 'vulnerable' for the purposes of data protection. Both categories of data subjects require additional protections and safeguards because the severity of impact of risks to the rights and fundamental freedoms of these cohorts of data subjects is higher than that of an ordinary data subject.

The nature of Tusla's processing of personal data in relation to CASP is inherently sensitive. Its scope is extensive as it has statewide responsibility for child protection and welfare and CASP is a state-wide service. As an organ of the state any processing of personal data by Tusla in relation to CASP is an interference with the right of privacy of the individuals to whom that data relates and must be done strictly in accordance with the law and only as necessary and proportionate for the purpose of the processing.

A general duty of confidentiality also applies to much of the data. It is important for all staff to understand Tusla's obligations to data subjects whose personal data is processed by CASP and how to ensure that these obligations are discharged and these data subjects' personal data and rights in relation to that data are safeguarded throughout the CASP process.

# 2. Purpose

The purpose of the CASP Data Protection Guidance ('Guidance') is to provide staff with information that promotes good practice and compliance with data protection obligations, Tusla's duty of confidentiality and its obligations in relation to the right of privacy for all individuals whose personal data is processed under CASP.

# 3. Glossary of Terms and Definitions

| | |
|---|---|
| Personal Data | Any information relating to an identified or identifiable natural (living) person.[1] |
| Special Categories of Personal Data | Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.[2] |
| Sensitive Personal Data | Personal data which by its nature or given the context of processing is particularly private, confidential or sensitive. In general terms, processing of personal data in Tusla may relate to any of its data subjects some of whom are children and vulnerable adults and involving any of the categories of personal data processed by Tusla including special category data of a highly sensitive nature. This data merits specific protection as it poses an increased risk to the rights and freedoms of data subjects. |
| Data Subject | A person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[3] |
| Processing | Any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.[4] |
| Controller | A natural (living individual) or legal (body corporate) person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by EU or Irish law, the controller or the specific criteria for its nomination may be provided for by EU or Irish law. [5] |
| Information Owner | The individual responsible for the management of a directorate or service e.g. Service Director, National Director (or equivalent). |
| Data Protection | Data Protection means the protection of individuals with regard to the collection, use and other processing of personal data. In this context, personal data is any information relating to an identified or identifiable individual, regardless of whether the information is private, professional, or even publicly available. The GDPR sets out obligations for parties processing personal data, including the legal bases for processing, data protection principles, and accountability measures and defines rights for individuals. |
| Privacy | Privacy means an individual's right to maintain control over and be free from intrusion into their private life, family life, home and communications. The law derives from the European Convention on Human Rights, the EU Charter of Fundamental Rights, the ePrivacy Directive, as well as various national laws. |

[1] See Article 4(1) GDPR
[2] Art. 9(1) GDPR
[3] Article 4(1) GDPR
[4] Art. 4(2) GDPR
[5] Art. 4(7) GDPR

## 4. Scope

This Guidance applies to all employees, regardless of contract type and includes those whole-time, temporary, released and seconded employees who process personal data on instructions from Tusla under an arrangement in which the employee acts under the authority of Tusla and to members of the CASP Review Panel who perform reviews under instruction from Tusla.

## 5. Related Policies and Guidance

This Guidance should be read together with CASP and in conjunction with the following related policies and guidance.

| Title | Description |
|---|---|
| Data Protection and Privacy Policy | Provides staff with information that promotes good practice and compliance with the GDPR, Tusla's duty of confidentiality to Service Users and its obligations in relation to the right of privacy |
| Data Protection Impact Assessment Policy | Provides staff with information that promotes good practice and compliance with the GDPR, Tusla's duty of confidentiality to Service Users and its obligations in relation to the right of privacy and reflects the minimum requirements under the conditions of Article 35 of the GDPR and the criteria for DPIAs laid down by the European Data Protection Board (EDPB) and the Data Protection Commission (DPC). |
| Third Party Data Protection and Privacy Risk Management Policy | Provides staff with information that promotes good practice and compliance with the GDPR, Tusla's duty of confidentiality to Service Users and its obligations in relation to the right of privacy when sharing personal data with third parties. |
| Records Management Policy | Forms the basis of the Records Management Strategy; describe the way in which the organisation intends to meet its obligations; inform staff of their obligations; ensures the highest level of support for records management and defines records management as a dedicated and resourced capability. |
| Redaction Guidance | Mandates the application of redaction principles to personal data in the context of sharing personal data with third parties under Data Protection Legislation. Redaction is one of the 'organisational and technical measures' which Tusla uses to safeguard personal data and reduce the risk of unauthorised disclosures and personal data breaches. |
| Data Protection Guidance Practice Matter | Provides an overview of some of the systemic issues which are causing regular data breaches in Tusla and to provide |

| | |
|---|---|
| | initial high-level guidance to staff on what they need to do to address these issues in their daily practice. |
| Personal Data Breaches Information and Guidance | Provides guidance for staff on what to do if they become aware of a suspected personal data breach or data security incident, roles and responsibilities for personal data breach management in Tusla and resources for staff on personal data breach management. |
| Data Subject Requests Information and Guidance | Provides guidance for staff on rights afforded to individuals under the GDPR (Data Subject Rights) what to do if they receive a request from an individual in relation to any of these rights and roles and responsibilities for data subject rights requests in Tusla |
| Tusla Information Security Policy Set | A set of policies which are components of the Tusla IS027001 Information Security Programme. |

# 6. How Data Protection Principles Apply to CASP

Tusla has a range of obligations under data protection law, and in particular must comply with the principles of data protection, as found in Article 5 of the GDPR, ensuring personal data are:

- processed lawfully, fairly and transparently[6];
- processed for specific purposes[7];
- limited to what is necessary[8];
- kept accurate and up to date[9];
- stored for no longer than necessary[10]; and
- protected against unauthorised or unlawful processing, accidental loss, destruction, or damage[11].

Tusla must also be able to demonstrate compliance with these principles, under the principle of accountability[12]. The following section sets out each of the principles of data protection and how they apply to CASP.

## 6.1 Lawfulness, Fairness and Transparency

In data protection terms a 'legal basis' (also referred to as a 'lawful basis' or 'lawful reason') means the legal justification for the processing of personal data. A valid legal basis is required in all cases for a data subject's personal data to be lawfully processed in line with data protection law. Under the GDPR, there are six possible legal bases for processing personal data, found in Article 6, namely: consent; contractual necessity; compliance with a legal obligation; protecting vital interests; performance of an official or public task; and legitimate interests (this legal basis does not apply to public bodies like Tusla).

Public sector organisations like Tusla mostly derive their powers from sources such as Acts of the Oireachtas or statutory instruments which set them up, or from case law, or duties under common law, or other laws regulating their activities. Tusla is a public sector statutory body and must at all times have regard to the powers and duties conferred on it by statute and cannot, therefore, act *ultra vires* these powers. Tusla's legal basis (or

[6] Article 5(1)(a) of the GDPR
[7] Article 5 (1)(b) of the GDPR
[8] Article 5(1)(c) of the GDPR
[9] Article 5(1)(d) of the GDPR
[10] Article 5(1)(e) of the GDPR
[11] Article 5(1)(f) of the GDPR
[12] Article 5(2) of the GDPR

how it establishes lawfulness) for processing personal data relating to CASP is grounded on its public function to promote the welfare and protection of children and the management of social care systems and services.

### Tusla's Legal Basis for Processing - Public Function and Public Interest

*Article 6(1)(e) of the GDPR allows for the processing of personal data where it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. Section 38(1) of the Data Protection Act, 2018 gives further effect to the GDPR by allowing for the processing of personal data to the extent that such processing is necessary and proportionate for the performance of a function of a controller conferred by or under an enactment or by the Constitution.*

*The general rule under Article 9(1) of the GDPR is that the processing of special categories of personal data shall be prohibited. However, this prohibition shall not apply if one of the legal bases in Article 9(2) is satisfied.*
*Article 9(2)(h) of the GDPR provides for processing "necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to conditions and safeguards referred to in paragraph 3." Section 58 of the Data Protection Act 2018 provides for the processing of special categories of personal data shall be lawful where it is necessary …(d) for the provision of medical care, treatment or social care and (e) for the management of health or social care systems and services.*

*Tusla asserts Article 6(1)(e) of the GDPR and section 38 of the Data Protection Act 2018 as its lawful basis for processing personal data and Article 9(2)(h) and section 52 of the Data Protection Act 2018 as its lawful basis for processing special categories of personal data.*

Court judgments which interpreted Tusla's duties under section 3 of the Child Care Act 1991 provided further clarification of the nature and scope of these duties and helped shape requirements under CASP. These judgments have established that Tusla should carry out substantiation investigations under section 3 of the Child Care Act 1991 and in doing so, ensure that fair procedures are afforded to the Person Subject to Abuse Allegations (PSAA) while carrying out child protection duties. The court judgments establish the following:

- Tusla may disclose to a third-party information about a person subject to abuse allegations if this is required to protect children;
- Tusla should not disclose information to a third-party without first conducting a substantiation investigation, except where a child is at immediate serious risk;
- Tusla must conduct an investigation based on natural justice and afford fair procedures to the PSAA;
- Such fair procedures include the right to be informed of the allegations and the right to respond to them;
- Tusla must provide all relevant materials which were assembled in substantiating an allegation to the PSAA;
- The investigating social worker must remain impartial throughout the process ;
- The investigating social worker must remember that their role is to investigate the complaint and not to vindicate the Complainant or sanction the PSAA;
- The Complainant's account is required to be stress tested and conflicts of fact addressed;
- The PSAA is entitled to be heard in his/her own defence and to have the testimony of such persons who can give testimony on his/her behalf, relevant to the allegations in issue, heard and considered by the investigator;
- The existence of a pending criminal prosecution against the PSAA does not alleviate Tusla's duty to investigate the allegations;

- In order to establish that a complaint is "founded" the allegations must be established on the balance of probabilities, the civil standard of proof.[13]

**Note:** while we have referred above to the terms 'Complainant', 'relevant material', 'stress-tested' 'substantiation investigation' for the purposes of setting out Tusla's obligations as imposed by case law, CASP contains the following defined terms which replaces these terms respectively and which we will use for the remainder of this Guidance:

**Person making a disclosure (PMD):** A person – either a child or an adult – who has made a disclosure of child abuse.

**Person subject of abuse allegations (PSAA):** A person – either a child or an adult – who has had allegations of child abuse made against them.

**Referral (of child abuse):** for the purpose of the CASP, a referral of child abuse is known as a disclosure (of child abuse) up to the end of stage 1. If it passes into stage 2 it is known as an allegation (of child abuse).

**Relevant information and documentation:** Where an assessment moves to stage 2, the PSAA is entitled to receive all relevant information and documentation which the CASP social worker has gathered during the course of the assessment. Information and documentation are relevant if they disclose a fact or facts which, on their own or together with other facts, make the allegation appear more likely than not to have happened than would be without that information. (Factors which the CASP Social Worker must consider in assessing the relevant information assembled during the assessment for the purpose of determining whether the outcome is founded or unfounded are set out at section 18.2 of CASP.)

**Relevant third parties:**

1. Any person who is in a position of responsibility for a child or children's safety and wellbeing. It includes someone who is in a position of direct authority over a PSAA, if the PSAA is employed or if they volunteer in an organisation where they may have contact with children through their work. For example:

- the principal of a school who has authority over a teacher.
- the Chief Executive Officer of a non-governmental organisation who has authority over an employee.
- the leader of a children's sports or activity group with authority over a volunteer, and so on. (See 'relevant organisation' in Section 2 of the National Vetting Bureau (Children and Vulnerable Persons) Act 2012.)

2. Any registration or regulatory body, such as, Health and Social Care Professionals Council (CORU), Medical Council, Teaching Council, and so on.

**Reliability and accuracy check:** The thorough examination and testing of the reliability, plausibility, and consistency of a disclosure a person is making. This may involve exploring the extent to which the person's disclosure is consistent with any available evidence and may involve (at a later date) seeking the person's response to any denials made by, any alternative versions of events provided, or other issues raised by the PSAA.

**Substantiation assessment:** The process of examining and evaluating allegations of child abuse that arrives at a conclusion which includes an outcome as to whether the allegation is founded or unfounded on the balance of probabilities. If the allegation is founded, the conclusion will also determine what risk of harm to children, if any, is posed by the PSAA.

**TCMS:** Tusla Case Management System is a digital system which allows users to manage and record their activities with a specific module relating to a CASP substantiation assessment.

### 6.1.1 Data Protection Consent Does Not Apply to CASP

As set out above, under the GDPR, there are six possible legal bases for processing personal data, found in Article 6 one of which is the consent of the data subject.

**There is a significant difference between consent or agreement that Tusla might seek from a parent to provide interventions and supports in relation to a child and 'consent' under data protection legislation.**

[13] Extract from 'Why CASP?' document published on www.tusla.ie/casp-consultation

Article 4(11) of the General Data Protection Regulation ('GDPR') defines consent as: "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her." The GDPR prescribes that if the data subject has no real choice, feels compelled to consent or will endure negative consequences if they do not consent, then consent will not be valid.

Given the nature of the relationship between Tusla, its Service Users, employees and other data subjects, Tusla cannot adequately demonstrate that its data subjects had a free and genuine choice as to whether or not to consent to processing by Tusla in all of the circumstances surrounding this consent.

Taking into account the duty of care owed by Tusla to many of its data subjects and the potential vulnerabilities of these data subjects Tusla cannot meet the criteria set out by Article 6, 7 and 9 as they relate to consent or meet its accountability obligations under Article 24 as it relates to demonstrating compliance with these requirements and so consent is not a valid legal basis for Tusla to rely on or assert for the processing of personal data.

It should be noted that this data protection consent is not the same thing as a consent or agreement provided by a PMD (or in the case of a PMD who is a child, his or her parents or guardians) for the release of medical or health records, information or documentation.

During the course of a substantiation assessment a CASP Social Worker may need to obtain agreement from the PMD (or in the case of a PMD who is a child, his or her parents or guardians) to provide to the PMD's medical practitioner or counsellor in order to seek records or other information in cases where the CASP Social Worker has reasonable grounds for believing that such information is relevant to the substantiation assessment. The

Attention

Consent as a legal basis for processing personal data under GDPR and consent or agreement obtained by Tusla from parents in order to provide interventions or supports to children are two different things. Consent under GDPR "*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*."

Given the nature of the relationship between Tusla and participants in the CASP process, Tusla cannot adequately demonstrate that its data subjects had a free and genuine choice as to whether or not to consent to processing by Tusla in all of the circumstances surrounding this consent. Taking into account in particular the vulnerabilities of these data subjects Tusla cannot meet the criteria for consent under data protection legislation so consent is not a valid legal basis for Tusla to rely on or assert for the processing of personal data under CASP.

CASP Social Worker should use the relevant templates in TCM as they have been drafted solely for this purpose and comply with data protection legislation.

## 6.1.2 Transparency and the Requirement to Provide Data Protection Notices to CASP Data Subjects

Under the principle of transparency, Tusla must provide certain information to data subjects (e.g. the PMD, the PSAA, relevant third parties, witnesses and others) when they collect their personal data, such as: the identity of the controller; the contact details of the controller and (if they have one) their 'data protection officer' (DPO); the purposes and 'legal basis' for the processing; who the data will be shared with; how long the data will be stored; and the existence of the data subject's various rights including:

- the right to be informed (through, for example, the Data Protection Notice)
- the right of access (through the Subject Access Request process)

- the right to rectification
- the right to erasure
- the right to restrict processing
- the right to object

Tusla is only permitted to use personal data fairly and transparently and in line with the purposes only for which it obtained. If we are using personal data in any way that is not expected by an individual and they don't know about it, this is processing that is unfair and not transparent and will be a breach of data protection legislation.

Tusla is required to provide this information a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.

When Tusla collects personal data directly from a data subject, say for example in the case of CASP where a complaint is made directly to Tusla by a PMD, Tusla must, **at the time when personal data are collected**, provide that data subject with all of the following information:

1. the identity and the contact details of the controller, i.e. Tusla;
2. the contact details of the data protection officer;
3. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
4. the recipients or categories of recipients of the personal data, if any;
5. the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
6. the existence of the right to request from Tusla access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing;
7. the right to lodge a complaint with a supervisory authority.

Where personal data are not collected directly from the data subject, say for example in relation to CASP where Tusla receives a mandated report from a mandated person and therefore receives personal data of a PMD and PSAA indirectly or Tusla receives a report or referral directly from a PMD and receives personal data of the PSAA indirectly in that report or referral, Tusla must provide the PSAA with the information set out below **within a reasonable period after obtaining the personal data, but at the latest within one month** or where the personal data are to be used for communication with the PSAA, at the latest at the time of the first communication to the PSAA.

**Note: The CASP Social Worker should use the relevant templates in TCM as they have been drafted solely for this purpose and comply with data protection legislation**.

**There are exceptions to the requirement to provide this information to the PSAA where to do so would for example, place a child at immediate serious risk or would, in the opinion of An Garda Síochána (AGS), jeopardise a criminal investigation. These exceptions however restrict the PSAA's right to information so can only be exercised in limited circumstances and on a temporary basis and all requests to avail of these exceptions must be referred to the Tusla Data Protection Unit (DPU) for recording, tracking and processing.**

1. the identity and the contact details of the controller, i.e. Tusla;
2. the contact details of the data protection officer;
3. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
4. the categories of personal data concerned;
5. the recipients or categories of recipients of the personal data, if any;

6. the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
7. the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;
8. the right to lodge a complaint with a supervisory authority;
9. from which source the personal data originate, and if applicable, whether it came from publicly accessible sources.

**Attention**

In order to comply with the requirement of transparency in relation to CASP:

- The Tusla Data Protection Unit (DPU) has drafted purpose specific data protection notices for CASP. These are:
  i. the CASP PMD Data Protection Notice
  ii. the CASP PSAA Data Protection Notice
  iii. the CASP General Data Protection Notice (for all other data subjects)
- All staff operating the CASP process must familiarise themselves with the contents of these Data Protection Notices and be able to explain them to the relevant individuals so that they understand what will happen to their personal data, why and what their rights are in relation to their personal data
- Where personal data are collected directly from an individual by Tusla, the relevant Data Protection Notice must be provided to that individual before, or at the time, the personal data are collected;
- Where personal data are NOT collected directly from the individual by Tusla, the relevant CASP Data Protection Notice must be provided to the data subject as soon as possible after receipt of the personal data but no later than one month after Tusla receives the personal data; (see timetable at 7.0 in CASP for more guidance)
- The relevant CASP Data Protection Notice must be provided in printed hard copy to the individual when meeting in person and explain it to the individual;
- The relevant CASP Data Protection Notice must be attached to correspondence (attached as PDF to secure email correspondence and printed hard copy enclosed in registered postal correspondence)
- All versions of the CASP Data Protection Notice must be made available at all Tusla contact points (locations around the country)

### 6.1.3 Data Subject Rights Management

All data subjects whose personal data is processed under the CASP process, including but not limited to, PMDs, PSAAs and third parties have the following rights in relation to their personal data:

### The Right to Be Informed

This is the right to be provided with clear, transparent and easily understandable information about how we use their personal data and their rights. This information is contained in the relevant CASP Data Protection Notice.

### The Right of Access

Data subjects have the right to:

- receive confirmation from us that their personal data is being processed so they're aware of and can check that we're using their personal data in accordance with data protection law;

- receive confirmation from us about the type of personal data we hold about them, why we use it, what we use it for and information about their rights (all of this is included in the CASP Data Protection Notice); and
- access to their personal data.

Data subjects can request copies of paper and electronic records (including recorded calls, where applicable) about them that we hold, share or use. To deal with their request, we can request proof of identity and enough personal data to enable us to locate the personal data they request.

When will access not be provided?

We can only provide data subjects with their personal data, not personal data about another person. Also, where access would adversely affect another person's rights, we are not required to provide this. Due to legal privilege, we may not be able to show them everything that we learned in connection with a legal claim or legal proceeding.

## The Right to Rectification

Data subjects are entitled to have their personal data corrected if it's inaccurate or incomplete. They have the right to obtain from us without undue delay the correction of inaccurate personal data concerning you. If they tell us that the personal data we hold on them is incorrect, we will review it and if we agree with them, we will correct our records. If we do not agree with them, we will let them know.

## The Right of Erasure

This is also known as 'the right to be forgotten' and enables data subjects to request the deletion or removal of their personal data where there's no compelling reason for us to keep using it. This is not an absolute right. We may have a right or obligation to retain the personal data, such as where we are under a legal or statutory obligation to do so or have another valid legal reason to retain it.

When can data subjects request erasure?

Subject to the section below, data subjects have a right to have their personal data erased, and to prevent processing, where:

- the personal data is no longer necessary for the purpose it was originally collected/processed;
- we have been processing their personal data in breach of data protection laws; or
- the personal data has to be erased in order to comply with a legal obligation.

When can we refuse erasure requests?

The right to erasure does not apply where personal data is processed for certain specified reasons, including where the processing is necessary for the performance of a task in the public interest or the exercise of official authority vested in Tusla or for the establishment, exercise or defence of legal claims.

## The Right to Restrict Processing

In certain situations, data subjects have the right to 'block' or suppress further use of information. When processing is restricted, we can still store the information, but may not use it further.

When is restriction available?

Data subjects have the right to restrict the processing of their personal data:

- where they disagree with the accuracy of the information, we need to restrict the processing until we have verified the accuracy of the information;
- when processing is unlawful and they oppose erasure and request restriction instead;
- if we no longer need the personal data but they need this to establish, exercise or defend a legal claim; or
- where they have objected to the processing and we are considering whether that objection is valid.

## The Right of Objection

Data subjects have the right to object to certain types of processing of their personal data. We will assess any objection and determine whether we may still process the personal data if we have a valid legal reason for doing so.

We will continue to process the personal data where it is necessary for research and statistical purposes carried out in the public interest as the right to object does not apply in this instance.

## 6.2 Purpose Limitation

Tusla must:

**Attention**

- The data subject rights set out above must be explained to data subjects when providing them with the CASP Data Protection Notice.
- These are fundamental protections afforded to data subjects under the GDPR and Tusla is required to comply in full with all requirements relating to these rights.
- Because these rights are so important, ALL requests relating to these rights must be referred to the DPU for recording, tracking and processing.
- The restrictions to these rights or the exceptions as set out above serve to deprive data subjects of these rights and so are applied on a temporary basis and in limited circumstances only, which is why it is important that the DPU oversee all responses to any data subject rights requests.
- Any individual can exercise their data protection rights by submitting a request to Tusla. This can be done in any way. For convenience, Tusla offers people the option of submitting their request via the Data Subject Rights Portal

- be clear from the outset why we are collecting personal data in relation to CASP and what we intend to do with it;
- comply with documentation obligations to specify our purposes in relation to CASP;
- comply with transparency obligations to inform individuals about our purposes; and
- ensure that if we plan to use or disclose personal data for any purpose that is additional to or different from the originally specified purpose, the new use is fair, lawful and transparent i.e. that we have a legal basis for processing, that we tell data subjects about this new use.

This requirement aims to ensure that we are clear and open about our reasons for obtaining personal data, and that what we do with the data is in line with the reasonable expectations of the individuals concerned.

**Attention**

In order to comply with the requirement of purpose limitation in relation to CASP:

- Use only approved forms and templates in relation to the CASP process;
- Be familiar with the purpose of the data processing as described in the CASP Data Protection Notices;
- Always use the correct approved form when collecting personal data and keep the purpose in mind as you collect and input the personal data into the form;
- Always use the correct approved correspondence template when disclosing personal data in writing and keep the purpose in mind as you prepare the correspondence;
- Limit data processing in spoken information, disclosure on site, and audio or video recording to the purpose specified in the same manner as you would to any written record;
- Comply in full with the requirements of CASP

## 6.3 Data Minimisation

Tusla must ensure that we only collect the minimum amount of information we need for the purpose of our processing i.e. that the personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

We must ensure therefore that all personal data we process is:

- adequate – sufficient to properly fulfil our CASP requirements;
- relevant – has a rational link to the requirements of CASP; and
- limited to what is necessary – we do not collect or hold more than we need for the requirements of CASP.

Compliance with the principle of data minimisation can be achieved by restricting personal data to only what is absolutely necessary to achieve the processing purpose. Data minimisation applies at all stages of processing including initial collection i.e. collect only what you need and no more, and sharing and disclosure i.e. disclosure the absolute minimum amount of personal data needed for the purposes of the sharing.

**WARNING!**

Caution must be exercised when corresponding with third parties in relation to abuse allegations.

**Disclosures of abuse are specific to the individuals who made them, therefore providing details of a disclosure may lead to identification of the PMD.**

Where it is absolutely necessary to provide details of the disclosure of abuse, staff members must ensure that the PMD (or any other third party) cannot be identified, either directly or indirectly, through the information provided in correspondence with third parties. For example, even if staff members do not disclose personal data which directly identifies the PMD (e.g., name, address etc.), the third party may still be able to identify the PMD, by other means such as the PMD's age and relationship to the PSAA so replacing these identifiers with [PMD NCCIS Identifier] (as set out in the standard forms and templates) helps to safeguard the data protection and privacy rights of PMDs.

Play your part by ensuring that you comply in full with the "Guidelines for informing Third Parties of child protection concerns arising out of an investigation by Tusla into allegations of child abuse and neglect under the Policy & Procedure for Responding to Allegations of Child Abuse and Neglect 2014 or the Child Abuse Substantiation Procedure & Guidance 2019"

## Data Minimisation and CASP

In order to comply with the data minimisation requirements relating to CASP, staff must:

### General Requirements

- Only request and collect the minimum amount of personal data needed for the relevant stages in the CASP process and be clear about why you need it. If you don't need it for any of the stages in the CASP process and all activities within each stages as set out in CASP you should not ask for it or keep it.
- If you receive more personal data than you need, return what you don't need;
- Use only the correct approved forms and correspondence templates to minimise the personal data collected or disclosed;
- When drafting correspondence only personal data which is strictly necessary to achieve the purpose of the correspondence should be included and only transmitted to the intended recipient once their identity and legal entitlement verified and contact details confirmed - any other personal data should be removed;
- Only the minimum amount of personal data required to be transmitted externally by post should be transmitted by post and post should only be used where in person or email transmission is not possible;
- Only the minimum amount of personal data required to be transmitted by email should be transmitted by email and email should only be used where in person transmission is not possible;
- Where it is not strictly necessary to disclosure the identity of individuals in correspondence, both direct identifiers (e.g. name and address) and indirect identifiers e.g. any other information that may identify individuals (e.g. relationships) should be removed;
- One useful way of removing personal data to protect the identity of individuals from unauthorised disclosure to third parties is pseudonymisation which involves replacing names and any other identifiers which are easily attributed to individuals with other references. You will note some of the TCMS template letters contain a [PSAA NCCIS identifier] or a [PMD NCCIS identifier] rather than the name of the PSAA or PMD with the name of the PSAA or PMD being disclosed in separate correspondence which contains only the [PSAA NCCIS identifier] or a [PMD NCCIS identifier] and name of the PSAA or PMD and no other information. The Tusla staff member can link this reference to the individual by accessing the PSAA or PMD person record on NCCIS), but as this additional information is not included in the correspondence if the correspondence was issued to the wrong recipient in error or intercepted by someone other than the intended recipient that someone would not be able to identify the PSAA or PMD from the correspondence alone – this is both a data minimisation and a data security control.
- Personal data of one individual (e.g. PMD) may only be disclosed to another individual or organisation (e.g. PSAA) under the CASP process if it is strictly necessary to discharge the requirements of CASP and must be limited only to the personal data strictly necessary to discharge that requirement. Ask yourself whether you need to disclose the personal data for any of the steps under CASP, if you can't answer yes don't share it and if unsure ask your line manager before sharing any personal data.

### Relevant Information and Documentation

- When disclosing personal data contained within 'relevant information and documentation' to the PSAA in order to afford fair procedures to the PSAA the question of what information and documentation is relevant to the substantiation assessment is important when considering what must be disclosed and what must be redacted.
- In considering what information is relevant, social workers should have regard to section 18.2 of CASP which sets out factors that may be relevant for consideration by social workers when making a determination of founded or unfounded. These factors include environmental details, contextual details, event details, emotional reaction consistent with abuse being described, witness statements consistent with the PMD's statement and/or behaviour, contemporaneous documentation that supports the PMD's testimony, medical/psychological evidence of abuse/trauma as determined by an expert.
- See detailed instructions in the table below on what personal data to redact before disclosure of 'relevant information and documentation' to the PSAA.

| Identifier | Redaction Instruction | Rationale |
|---|---|---|
| PMD's Name | Disclose but pseudonymise | Must be disclosed to PSAA for fair procedure purposes so PSAA can properly respond to allegation. In order to protect the data protection rights of the PMD follow the instructions in the CASP Standard Forms and Templates and replace the PMD's name in the relevant information and documentation with the PMD NCCIS Identifier when disclosing the relevant information and documentation to the PSAA. The PMD's name is disclosed in separate correspondence to the PSAA containing only the PMD's name. This is both a data minimisation and a data security control which helps to protect the PMD if the correspondence is sent to the wrong recipient or intercepted by someone other than the PSAA. |
| PMD's Age | Disclose | Must be disclosed to PSAA for fair procedure purposes so PSAA can properly respond to allegation |
| PMD's Address and Eircode | Redact | May not be required for fair procedures and potential for significant risk of harm to PMD if this information is disclosed. If the particular circumstances of a substantiation assessment are such that the CASP Social Worker considers it is necessary to disclose this information in order for the PSAA to properly respond to an allegation, the CASP Social Worker must (as set out in CASP) provide the information proposed to be disclosed to the PMD and afford the PMD the opportunity to object to the disclosure. If the PMD objects to this information being disclosed to the PSAA, the CASP Social Worker must refer the matter to a CASP Lead for decision who in turn may consult with Tusla Office of Legal Services as required. If the PMD raises objections on the grounds of concern for his or her safety, the CASP Social Worker should seek permission from the PMD to engage with AGS with a view to AGS establishing an APMD safety plan for his or her protection. |
| PMD's Telephone Number | Redact | Not required for fair procedures and significant risk of harm to PMD if this information is disclosed |
| PMD's Email Address | Redact | Not required for fair procedures and significant risk of harm to PMD if this information is disclosed |

| Identifier | Redaction Instruction | Rationale |
|---|---|---|
| PMD's Ethnicity | Disclose if 'relevant information and documentation'<br>Redact if NOT 'relevant information and documentation' | If not 'relevant information and documentation' not required to be disclosed for fair procedures so should not be disclosed as this is highly sensitive personal data and significant risk of harm may occur to PMD if this information is disclosed. Staff should be guided by section 18.2 of CASP "Factors to consider when reaching a founded or unfounded finding" when making a determination as to whether this information is 'relevant information and documentation'' and if a determination is made that this is 'relevant information and documentation' detail of this determination and the rationale for this determination should be recorded on the PMD's personal record prior to disclosure, the case record and the PSAA's personal record once disclosed. |
| PMD's PPSN | Redact | Not required for fair procedures and significant risk of harm to PMD if this information is disclosed |
| PMD's Proof of Identity | Disclose if 'relevant information and documentation'<br>Redact if NOT 'relevant information and documentation' | If not 'relevant information and documentation' not required to be disclosed for fair procedures so should not be disclosed as this is highly sensitive personal data and significant risk of harm may occur to PMD if this information is disclosed. Staff should be guided by section 18.2 of CASP "Factors to consider when reaching a founded or unfounded finding" when making a determination as to whether this information is 'relevant information and documentation'' and if a determination is made that this is 'relevant information and documentation' detail of this determination and the rationale for this determination should be recorded on the PMD's personal record prior to disclosure, the case record and the PSAA's personal record once disclosed. |
| PMD's Date of Birth (DOB) | Disclose if 'relevant information and documentation'<br>Redact if NOT 'relevant information and documentation' | If not 'relevant information and documentation' not required to be disclosed for fair procedures so should not be disclosed as this is highly sensitive personal data and significant risk of harm may occur to PMD if this information is disclosed. In some cases a PMD's DOB may be relevant for the PSAA in order for him or her to be able to identify who the PMD is. Staff should be guided by section 18.2 of CASP *"Factors to consider when reaching a* |

| Identifier | Redaction Instruction | Rationale |
|---|---|---|
| | | *founded or unfounded finding"* when making a determination as to whether this information is *'*relevant information and documentation'' and if a determination is made that this is 'relevant information and documentation' detail of this determination and the rationale for this determination should be recorded on the PMD's personal record prior to disclosure, the case record and the PSAA's personal record once disclosed. |
| PMD's Profession | Disclose if 'relevant information and documentation'<br>Redact if NOT 'relevant information and documentation' | If not 'relevant information and documentation' not required to be disclosed for fair procedures so should not be disclosed as this is highly sensitive personal data and significant risk of harm may occur to PMD if this information is disclosed. Staff should be guided by section 18.2 of CASP *"Factors to consider when reaching a founded or unfounded finding"* when making a determination as to whether this information is *'*relevant information and documentation'' and if a determination is made that this is 'relevant information and documentation' detail of this determination and the rationale for this determination should be recorded on the PMD's personal record prior to disclosure, the case record and the PSAA's personal record once disclosed. |
| PMD's Special Category Personal Data about personal supports, substance abuse, mental health, physical health, disability, literacy | Disclose if 'relevant information and documentation'<br>Redact if NOT 'relevant information and documentation' | If not 'relevant information and documentation' not required to be disclosed for fair procedures so should not be disclosed as this is highly sensitive personal data and significant risk of harm may occur to PMD if this information is disclosed. Staff should be guided by section 18.2 of CASP *"Factors to consider when reaching a founded or unfounded finding"* when making a determination as to whether this information is *'*relevant information and documentation'' and if a determination is made that this is 'relevant information and documentation' detail of this determination and the rationale for this determination should be recorded on the PMD's personal record prior to disclosure, the case record and the PSAA's personal record once disclosed. |
| PMD's Special Category Personal Data relating to previous complaints or history with Tusla | Disclose if 'relevant information and documentation'<br>Redact if NOT 'relevant information and documentation' | If not 'relevant information and documentation' not required to be disclosed for fair procedures so should not be disclosed as this is highly sensitive |

| Identifier | Redaction Instruction | Rationale |
|---|---|---|
| or involvement with other services | | personal data and significant risk of harm may occur to PMD if this information is disclosed. Staff should be guided by section 18.2 of CASP *"Factors to consider when reaching a founded or unfounded finding"* when making a determination as to whether this information is 'relevant information and documentation'' and if a determination is made that this is 'relevant information and documentation' detail of this determination and the rationale for this determination should be recorded on the PMD's personal record prior to disclosure, the case record and the PSAA's personal record once disclosed. |
| ALL OTHER Special Category Personal Data not referred to above relating to the PMD<br>(data relating to physical or mental health, sexual life or orientation, racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership) | Disclose if 'relevant information and documentation'<br>Redact if NOT 'relevant information and documentation' | If not 'relevant information and documentation' not required to be disclosed for fair procedures so should not be disclosed as this is highly sensitive personal data and significant risk of harm may occur to PMD if this information is disclosed. Staff should be guided by section 18.2 of CASP *"Factors to consider when reaching a founded or unfounded finding"* when making a determination as to whether this information is 'relevant information and documentation'' and if a determination is made that this is 'relevant information and documentation' detail of this determination and the rationale for this determination should be recorded on the PMD's personal record prior to disclosure, the case record and the PSAA's personal record once disclosed. |
| PMD's PULSE ID or Other Garda Identifier | Redact | Tusla should not have this information and should NEVER disclose this information to anyone |
| PMD's Criminal Conviction or Offence Data<br>(including offences and alleged offences) | Redact | Not required for fair procedures, highly sensitive and significant risk of harm to PMD if this information is disclosed |
| Details of Form of Abuse Alleged | Disclose | This is information that is relevant and required to be disclosed to the PSAA in order to afford fair procedures and to allow the PSAA to properly respond to the allegation |
| Abuse Event Details | Disclose | This is information that is relevant and required to be disclosed to the PSAA in |

| Identifier | Redaction Instruction | Rationale |
|---|---|---|
| [details of where and when the alleged abuse took place; the nature, frequency and duration; and, if relevant, any details of how the PSAA maintained the victim's compliance and/or secrecy (i.e. through coercion, threats, bribes, etc.)) | | order to afford fair procedures and to allow the PSAA to properly respond to the allegation |
| Mandated Persons Profession | Disclose | This is information that is relevant and required to be disclosed to the PSAA in order to afford fair procedures and to allow the PSAA to properly respond to the allegation. **WARNING: ALL OTHER PERSONAL DATA RELATING TO THE MANDATED PERSON SHOULD BE REDACTED AS PSAA IS NOT ENTITLED TO KNOW THE IDENTITY OF THE MANDATED PERSON ONLY HIS OR HER ROLE.** |
| Witness<br>Name, Age and Geographical Area | Disclose | This is information that is relevant and required to be disclosed to the PSAA in order to afford fair procedures and to allow the PSAA to properly respond to the allegation. |
| Witness<br>All other personal data and special category personal data (everything relating to the witness excluding name, age and geographical area) | Disclose if 'relevant information and documentation'<br>Redact if NOT 'relevant information and documentation' | If not 'relevant information and documentation' not required to be disclosed for fair procedures so should not be disclosed as this is highly sensitive personal data and significant risk of harm may occur to the person if this information is disclosed. Staff should be guided by section 18.2 of CASP *"Factors to consider when reaching a founded or unfounded finding"* when making a determination as to whether this information is 'relevant information and documentation'' and if a determination is made that this is 'relevant information and documentation' detail of this determination and the rationale for this determination should be recorded on the case record and the PSAA's personal record once disclosed. |
| Person to whom abuse was disclosed<br>Name, Age and Geographical Area | Disclose | This is information that is relevant and required to be disclosed to the PSAA in order to afford fair procedures and to allow the PSAA to properly respond to the allegation. |
| Person to whom abuse was disclosed<br>All other personal data and special category personal data (everything relating to the | Disclose if 'relevant information and documentation'<br>Redact if NOT 'relevant information and documentation' | If not 'relevant information and documentation' not required to be disclosed for fair procedures so should not be disclosed as this is highly sensitive personal data and significant risk of harm may occur to the person if this information |

| Identifier | Redaction Instruction | Rationale |
|---|---|---|
| person excluding name, age and geographical area) | | is disclosed. Staff should be guided by section 18.2 of CASP *"Factors to consider when reaching a founded or unfounded finding"* when making a determination as to whether this information is 'relevant information and documentation'' and if a determination is made that this is 'relevant information and documentation' detail of this determination and the rationale for this determination should be recorded on the case record and the PSAA's personal record once disclosed. |
| Other alleged victim or identified child at risk<br>Name, Age and Geographical Area | Disclose | This is information that is relevant and required to be disclosed to the PSAA in order to afford fair procedures and to allow the PSAA to properly respond to the allegation. |
| Other alleged victim or identified child at risk<br>All other personal data and special category personal data (everything relating to the person excluding name, age and geographical area) | Disclose if 'relevant information and documentation'<br>Redact if NOT 'relevant information and documentation' | If not 'relevant information and documentation' not required to be disclosed for fair procedures so should not be disclosed as this is highly sensitive personal data and significant risk of harm may occur to the person if this information is disclosed. Staff should be guided by section 18.2 of CASP *"Factors to consider when reaching a founded or unfounded finding"* when making a determination as to whether this information is 'relevant information and documentation'' and if a determination is made that this is 'relevant information and documentation' detail of this determination and the rationale for this determination should be recorded on the case record and the PSAA's personal record once disclosed. |
| All other third party (anyone who is not a PMD, PSAA, other alleged victim or identified child at risk, witness, person to whom the abuse was disclosed, mandated person) personal data and special category personal data including but not limited to:<br>- Name<br>- Address<br>- DOB<br>- Age<br>- Telephone Number<br>- Email Address<br>- Ethnicity<br>- Proof of Identity<br>- PULSE ID<br>- Profession | Redact | Not required for fair procedures, highly sensitive and risk of harm to third party if this information is disclosed |

| Identifier | Redaction Instruction | Rationale |
|---|---|---|
| - Criminal Conviction Data (offences and alleged offences)<br>- Special Category Personal Data (health, sex life, sexual orientation, racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership)<br>- Special Category Personal Data relating to previous complaints or history with Tusla or involvement with other services<br>- Special Category Personal Data about personal supports, substance abuse, mental health, physical health, disability, literacy | | |
| Name and work contact details of Tusla staff members carrying out the CASP process | Disclose | Public servants do not have a general right of privacy the context of their performing a public task (doing their job) and for fairness and transparency purposes PSAA should have this information. |

## 6.4 Data Accuracy

Tusla must ensure that all personal data that we process is accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. Personal data are inaccurate if they are incorrect or misleading as to any matter of fact. There is an obligation on Tusla to demonstrate accuracy.

### Second Review (4-Eye Review) Process for CASP

A 'second review' is a process of having at least two people check a document or record to ensure that the right content is contained within that document or record.

The following are minimum mandatory requirements relating to CASP:

- ✓ When opening a Case Record in relation to an Investigation on TCMS one person (doer) creates the record and inputs the relevant information and a second person (reviewer) checks to make sure that the information is correct;
- ✓ When opening a Person Record for a PSAA on NCCIS one person (doer) creates the record and inputs the relevant information and a second person (reviewer) checks to make sure that the information is correct;
- ✓ When opening a Person Record for a PMD on NCCIS one person (doer) creates the record and inputs the relevant information and a second person (reviewer) checks to make sure that the information is correct;
- ✓ When preparing all correspondence with the PMD and before the correspondence is issued, one person (doer) prepares the correspondence and a second person (reviewer) checks to make sure that the information contained in the correspondence is correct and that it is being sent to the right person at the right address;
- ✓ When preparing all correspondence with the PSAA and before the correspondence is issued, one person (doer) prepares the correspondence and a second person (reviewer) checks to make sure that the information contained in the correspondence is correct and that it is being sent to the right person at the right address;
- ✓ When preparing all correspondence with third parties and before the correspondence is issued, one person (doer) prepares the correspondence and a second person (reviewer) checks to make sure that the information contained in the correspondence is correct and that it is being sent to the right person at the right address
- ✓ When preparing all notifications to relevant third parties and before the correspondence is issued, one person (doer) prepares the correspondence and a second person (reviewer) checks to make sure that the information contained in the correspondence is correct and that it is being sent to the right person at the right address
- ✓ All correspondence which has already been reviewed as part of the standard process does not require a second review of the content, but does require a second independent review of the name and address before it is posted (e.g. CASP notification of allegations that has already been reviewed by two of the following: Principal Social Workers, Team Leader or Social Worker).
- ✓ All correspondence which is standardised, such as a template letter (which has been written using a BLANK TEMPLATE) only requires a second review of the name and address to confirm the correspondence will issue to the correct recipient.
- ✓ All correspondence which has any other additional personal data contained within it, either of the addressee or of another data subject, must have a second review of the name, address and the content

## Second Review (4-Eye Review) Process for CASP (continued)

- ✓ When individuals are being sent correspondence as part of the CASP process it is critical that those recipients only receive the information that they are entitled to receive and that all other information that they are not entitled to receive is redacted. If you are ever unsure on how to redact any personal data, you must inform your line manager prior to issuing any correspondence.
- ✓ Where a second independent review is not possible (e.g. Lone working), mitigating procedures must be put in place, e.g. Delayed Posting or Batch Checking. This is where correspondence is prepared for post and delayed for a period of time to allow for a further appropriate check by the same person (name/address/content depending on requirements) before it is posted

The following are minimum mandatory requirements relating to CASP Review:

The area manager will be asked to complete the following within 15 days of being notified of the review panel's appointment:

- ✓ Ensure all relevant information and documentation has been appropriately redacted before sending to the review panel

  The relevant information and documentation that is to be provided to the review panel will have been appropriately redacted by the original CASP social worker during the substantiation assessment process in accordance with the guidance contained in the CASP Data Protection Guidance. Before supplying the relevant information and documentation to the Review Panel, the area manager will assign a team member to check the redactions are correct. The area manager will ensure this step is completed before providing his or her final sign off to provide the booklet and links to the review panel. Evidence of this action will be recorded on Tusla Case Management System (TCMS).
- ✓ Supply a booklet of all relevant information and documentation to the review panel

  One booklet containing all relevant information and documentation gathered by the CASP social worker in the substantiation assessment must be provided to the Review Panel. This booklet should include copies of all records concerning the assessment and decision-making, including any submissions or representations submitted by the PSAA. The pages of the records should be sequentially numbered for ease of reference. This booklet is to be provided to the PSAA by the review panel.
- ✓ Supply Electronic Links to this information for each review panel member

  The area manager will also be asked to provide a link to each member of the review panel to TCMS (Tusla Case Management System) where the relevant information and documentation gathered as part of the substantiation assessment can be reviewed. The link should provide access to all relevant information and documentation which was gathered by the original CASP social worker during the substantiation assessment. As above, relevant information and documentation includes copies of all records concerning the assessment and decision-making, including any submissions or representations submitted by the PSAA. The area manager will ensure that the booklet and links are transmitted to the review panel securely in the manner prescribed in CASP Data Protection Guidance.
- ✓ Once appointed, the review panel shall ensure that all submissions, records, reports, and interactions with the PSAA, the area manager or other parties relating to the review are recorded by the review panel on Tusla Case Management System (TCMS).
- ✓ The review panel will ensure that all correspondence, written records of interviews and reports issued by the review panel are created using the templates on TCMS and that a record of each document issued is retained on the TCMS case record, and that all correspondence is transmitted securely as prescribed in CASP Data Protection Guidance.
- ✓ All correspondence, written records and reports should be drafted by one panel member using the templates on TCMS, and the other member of the review panel should perform a four eyed review to ensure that the draft document is correct and contains all the information required. They should also confirm that it complies with the requirements for the content and format of the relevant TCMS template.

## Attention

A significant number of personal data breaches have occurred in Tusla due to inaccuracies in data processed by Tusla.

Data transmitted externally by post must be accurate, complete and up to date and particularly names and addresses of recipients must be those of the intended recipient given the high risk of unauthorised disclosure due to incorrect name and address being entered on correspondence either because this information is transcribed incorrectly from sources such as NCCIS or because the information contained on those sources is inaccurate or out of date.

Everyone must play their part in safeguarding personal data by:

- ✓ Ensuring that all databases containing contact details of Service Users and third parties are accurate and kept up to date
- ✓ Regularly verifying addresses when engaging with Service Users and ensuring that the correct address is entered on NCCIS or other databases
- ✓ Regularly verifying addresses and contact details obtained from third party sources with the intended recipient before sending any correspondence
- ✓ Only use BLANK templates when creating correspondence. NEVER use previously populated correspondence as a template for new correspondence
- ✓ NEVER handwrite an address on an envelope. Use windowed envelopes only and fold the letter correctly in the envelope so that only the name and address of the recipient is visible through the window and no other information is visible
- ✓ Transmit CASP correspondence in person if possible.
- ✓ If in person transmission is not possible, use secure electronic transmission. This means that all correspondence must be password protected and attached to an email and emailed to the recipient and the password must be disclosed to the recipient over the phone. NEVER include any CASP correspondence or data in the body of the email.
- ✓ If in person and email transmission is not possible, use registered or couriered post only. NEVER use ordinary post to transmit CASP correspondence. Retain a receipt of the register or courier to help track and trace the correspondence in the event of a personal data breach.

## 6.5 Storage Limitation (Retention)

Tusla must ensure that personal data are kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) of the processing.

In deciding how long we need to keep this data (our retention criteria) we must take into account fulfilling any legal/statutory retention requirements and identifying business or service needs for retention from experience. Tusla is also required to keep retention periods to a strict minimum by establishing and periodically reviewing time limits[14], which must be included in records of processing where possible[15].

14 GDPR, Rec 39

15 GDPR, Art 30(1)(f)

### Storage Limitation Rules for CASP

- ✓ Delete temporary and local copies of files without delay so that files are always held in their dedicated location (e.g. files for CASP should be held in TCMS)
- ✓ Destroy hard copy files once the file has been scanned and uploaded to TCMS
- ✓ Limit making copies of files by accessing information in its dedicated location and referring others to the dedicated location (e.g. TCMS). For example, if communicating with a colleague who also has access to the dedicated systems (TCMS or NCCIS), prefer referring the colleague to the system to source information instead of downloading and sending a file by email
- ✓ Ensure that you delete local copies of CASP files from your computer desktop or from the network drive.
- ✓ If it is necessary to print a copy of a file, dispose of the copy promptly and securely after use through shredding.
- ✓ If you see files unattended in your work area, return them to a secure location or shred paper files which are evidently copies of electronic master copies. Report a potential data breach if appropriate, such as if files are unattended in a public area or an area where there may be unauthorised access to the files.
- ✓ Follow Tusla's Information Security Policy Framework and Records Management Policy

### Attention

- ✓ Tusla is not permitted to apply indefinite retention periods to personal data without exception or limitation or without any objective criteria linking the retention period with the objective pursued, i.e.. the purpose of the processing.
- ✓ Ensuring that we erase or anonymise personal data when we no longer need it will reduce the risk that it becomes irrelevant, excessive, inaccurate or out of date. Apart from helping Tusla to comply with the data minimisation and accuracy principles, this also reduces the risk that we will use such data in error.
- ✓ Personal data held for too long will, by definition, be unnecessary and Tusla is unlikely to have a lawful basis for retention.
- ✓ Tusla must also respond to subject access requests for any personal data we hold which becomes more difficult if we are holding old data for longer than we need.
- ✓ Good practice around storage limitation, with clear policies on retention periods and erasure, is also likely to reduce the burden of dealing with queries about retention and individual requests for erasure.

**Play your part by complying with Tusla's Records Management Policy**

## 6.6 Integrity and Confidentiality (Security)

Attention

The collecting, recording, processing, storing and sharing personal data required by CASP involves the processing of Tusla's records or document relating to PMDs, family members, PSAAs and other data subjects and involving any of the categories of personal data processed by Tusla including special category data of a highly sensitive nature. These data subjects include children and vulnerable persons to whom Tusla owes a duty of care and in many instances a duty of confidentiality.

The breach the subject of Inquiry IN-19-12-8 ('1 x breach inquiry') under the Section 3 Policy resulted from Tusla's failure to redact personal data of complainants from a safeguarding letter issued to a relevant third party to inform and advise her of safeguarding procedures to ensure the ongoing safety of a child at risk. The letter contained the names of the complainants who made the allegations and details of the allegations made. The relevant third party subsequently shared a photograph of the safeguarding letter on social media. The Data Protection Commission (DPC) found that this personal data breach created a risk to the rights and freedoms of the complainants and that unauthorized disclosure of this type of personal data has an inherent capacity to seriously infringe the rights and freedoms of the complainants. The likelihood of psychological damage or harm to the complainants was aggravated by the fact that the letter was subsequently published on a social media platform.

The impact of a personal data breach on any individual involved in the CASP process can be very severe. CASP processes the most sensitive personal data of individuals in the State and particularly private and confidential personal data of PMDs and PSAAs. PMDs are particularly vulnerable and it is really important that all staff understand the potential impact of a personal data breach on a PMD who is subject to the CASP process and is by virtue of his or her status as a service user 'vulnerable' from a data protection perspective and who, therefore, must be afforded special protections in addition to those afforded to an ordinary data subject. In addition to his or her status as a 'vulnerable' data subject, it has to be acknowledged that PMDs must also considered 'vulnerable' in the ordinary sense of the word given the nature of the disclosures being made and the fact that he or she will most likely revisit certain traumas during the course of making a disclosure and engaging with Tusla in the CASP process. In addition to the harm that might result to a PMD, a personal data breach may cause significant harm to a PSAA who also has data protection and privacy rights in addition to the right to vindicate his or her good name and the right to fair procedures.

The potential for harm to such individuals (and indeed other individuals who are involved in the CASP process including mandated persons) arising from a personal data breach or any inappropriate or unlawful processing of his or her personal data must be uppermost in the minds of all Tusla staff who operate the CASP process.

Articles 33(5) and 5(2) of the GDPR require Tusla to document and notify personal data breaches.
The GDPR defines a personal data breach as "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data*". If a personal data breach is likely to present risk to affected persons' rights and freedoms, Tusla is obliged by Article 33(1) GDPR to notify the DPC no later than 72 hours after becoming aware of it. Security incidents that typically meet the GDPR's definition of a personal data breach include:

- issuing emails or letters containing personal data to unintended recipients.
- sharing of personal data or third-party information with unauthorised recipients;
- loss of personal data or a device containing personal data (e.g. work phones or laptops);
- unauthorised or inappropriate access to electronic files/portals holding personal data;
- temporary or permanent loss of control over personal data, and;
- unauthorised alteration of personal data.

### What to do when a personal data breach happens

As soon as you become aware of it, you must immediately report any incident that you suspect or know to be a personal data breach Tusla's Data Protection Unit (DPU).

Even if you are unsure, or if you don't have the full details, you must report the incident to the DPU. Failure to immediately report can result in:

- Inquiries, fines, or sanctions by the Data Protection Commission; and
- Loss of confidence and reputational damage among Tusla Service Users and the public.

Reports should be made to the DPU by emailing datacontroller@tusla.ie

Guidance on sharing personal data safely is available at https://tusla.sharepoint.com/:u:/r/sites/home/SitePages/Sharing-personal-data-safely.aspx

## 6.7 Accountability

### Attention

The rule of thumb in relation to the Principle of Accountability is that if it is not documented, it wasn't done. This means that not only is Tusla required to comply with all data protection rules relating to CASP, Tusla must be able to demonstrate that these rules have been complied with.

Make sure to document all decisions, the reasons for these decisions, transactions, interactions with individuals correctly on TCMS and NCCIS so that if required we can demonstrate that we did what was required to protect and uphold the data protection rights of all individuals involved in the CASP process.

# 7. References

General Data Protection Regulation (Official Text)s

https://gdpr-info.eu/

Data Protection Act 2018 (Official Text)

http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html

TUSLA

An Ghníomhaireacht um Leanaí agus an Teaghlach

Child and Family Agency