TUSLA
An Ghníomhaireacht um Leanaí agus an Teaghlach
Child and Family Agency

# CASP
# Data Protection Guidance

Draft March **2021**

Note: This draft document is for the purpose of stakeholder consultation between April and June 2021 only.

# **CASP** Data Protection Guidance

## Contents


1. The purpose of **CASP Data Protection Guidance** ..... 4
2. Scope ..... 4
3. Legislation and other related policies, standards and guidelines ..... 5
4. Glossary of data protection terms as they apply to **CASP** ..... 5
   4.1. All glossary terms ..... 6
5. Data Protection Guidance ..... 6
   5.1. Ensuring lawful and fair processing in **CASP** ..... 6
      5.1.1. The legal basis ..... 6
      5.1.2. The status of consent from the data subject; seeking agreement from a data subject ..... 8
   5.2. Assessing and treating data protection risks in **CASP** ..... 10
      5.2.1. Risks and Risk Controls ..... 10
      5.2.2. Risk of Harm to a Data Subject ..... 11
      5.2.3. Risk of non-compliance with data protection legislation ..... 11
      5.2.4. The potential harmful impact on a data subject when a threat exploits a vulnerability in data processing ..... 12
      5.2.5. Vulnerability of a data subject ..... 13
      5.2.6. Vulnerability of an information asset ..... 13
      5.2.7. Risk evaluation ..... 13
      5.2.8. NB: Rules to follow when managing data protection risks ..... 17
   5.3. Fulfilling Data Protection Principles in **CASP** ..... 17
      5.3.1. Principle of Lawfulness, Fairness and Transparency ..... 18
      5.3.2. Principle of Purpose Limitation ..... 18
      5.3.3. Principle of Data Minimisation ..... 19
      5.3.4. Principle of Accuracy ..... 20
      5.3.5. Principle of Storage Limitation ..... 21
      5.3.6. Principle of Integrity and confidentiality ..... 22
      5.3.7. Demonstrating accountability for the Data Protection Principles ..... 22
   5.4. Upholding the Rights and Freedoms of Data Subjects in **CASP** ..... 22
      5.4.1. Rules to uphold the data subject rights ..... 22

5.4.2. The Right to Fair and Transparent Processing ..... 23
5.4.3. The Right to Information about the Processing ..... 24
5.4.4. The Right of Access ..... 24
5.4.5. The Right to Rectification ..... 25
5.4.6. The Right to Erasure (the 'Right to be Forgotten') ..... 25
5.4.7. The Right to Restriction of Processing ..... 26
5.4.8. The Right to Data Portability ..... 26
5.4.9. The Right to Object to Processing ..... 26
5.4.10. The Right not to be Subject to Automated Decision-making Including Profiling ..... 27
5.4.11. The Right to Lodge a Complaint with a Supervisory Authority ..... 27
5.4.12. Right to an effective judicial remedy against a controller or processor and related rights 27
5.4.13. Demonstrating accountability for the Data Subject Rights ..... 27
5.5. Ensuring that the data processing is necessary and proportionate to the purpose and applying safeguards to protect the data ..... 28
5.5.1. Overview ..... 28
5.5.2. General guidelines ..... 28
5.5.3. NB: Disclosing data safely ..... 29
5.6. Ensuring data protection compliance at each stage of the process ..... 34
5.6.1. Required data protection actions when carrying out **CASP** ..... 34
Appendix ..... 35
1. Full Glossary of Terms ..... 35
2. CASP Privacy Notice(s) ..... 47
3. Data Protection Reference Information ..... 47

# 1. The purpose of CASP Data Protection Guidance

The purpose of this **CASP Data Protection Guidance** is to provide guidance on data protection compliance as it applies to Child Abuse Substantiation Procedure (**CASP**) in reference to the documents **Child Abuse Substantiation Procedure (CASP)** and **Child Abuse Substantiation Practice Guidance and Review Procedure**. **CASP Data Protection Guidance** complements these core procedure and guidance documents for **CASP**. This guidance aims to fill the gap between **Tusla Privacy Policy** (and the associated data protection policy framework) which provides general direction and guidance for all data processing at Tusla and the specific requirements for implementing actions for data protection compliance in **CASP**.

# 2. Scope

**CASP Data Protection Guidance** refers solely to the data processing activity which supports **CASP**. For direction and guidance on related data processing activities, consult Tusla Privacy Policy or the Data Protection Unit.

**CASP Data Protection Guidance** should be followed by all Tusla employees or those acting on behalf of Tusla in the fulfilment of **CASP** and the data processing necessitated by the fulfilment of **CASP**.

This guidance is to be applied by social workers in their practice when conducting a substantiation investigation under **CASP** to support compliant decision making and provide information to data subjects.

The guidance should be followed for substantiation investigations and review process which may continue under the preceding 2014 policy, **Policy & Procedures for Responding to Allegations of Child Abuse & Neglect**.

**CASP Data Protection Guidance** does not provide introductory guidance on data protection and all employees, and others processing data on behalf of Tusla in the fulfilment of **CASP**, must consult Tusla Privacy Policy and must have carried out Tusla's mandatory data protection training.

**CASP Data Protection Guidance** does not provide guidance for data protection compliance in the governance of **CASP**. For example, this document does not provide guidance on data protection activities such as carrying out a Data Protection Impact Assessment, drafting a **Privacy Notice**, or recording the data processing activity in the Register of Data Processing Activities. Refer to Tusla Privacy Policy.

**CASP Data Protection Guidance** provides guidance, in particular, where the core procedure and guidance documents refer directly to data protection or Tusla Privacy Policy:

- **Child Abuse Substantiation Procedure (CASP)**
  - *1. Introduction*
  - *3. Key relevant legislation*
  - *5. The Procedure - Receiving a report*
  - *5. The Procedure - Screening and preliminary enquiry phase*
  - *5. The Procedure - Investigation of child abuse allegations where substantiation is required - Stage 1 - Action at the end of Stage 1:*
  - *5. The Procedure - Investigation of child abuse allegations where substantiation is required - Stage 2 - A PSAA has a right to:*

- **Child Abuse Substantiation Practice Guidance and Review Procedure**
    - *2. When to use the National Procedure and accompanying Practice Guidance*
    - *9. Receiving a report*
    - *10. Screening and preliminary enquiries*
    - *13. Investigation of child abuse where substantiation is required*
    - *17. Contacting an adult complainant as part of the preliminary enquiry*
    - *21. Management of records where a complainant decides not to engage in the first stage of the substantiation investigation.*
    - *23. Informing relevant third parties prior to the second stage of the substantiation investigation*
    - *25. Second stage of the substantiation investigation: engaging with the PSAA*
    - *26. Where the PSAA declines to engage*
    - *35. Where a PSAA resides in another jurisdiction*

The Data Protection Unit shall notify Tusla Operations when an update or change to the guidance is available, as approved by Tusla Operations, Tusla Office of Legal Services and National Policy Oversight Committee (NPOC). Tusla Operations and Tusla Office of Legal Services should notify the Data Protection Unit if an update is required.

## 3. Legislation and other related policies, standards and guidelines

Consult **Tusla Privacy Policy** and Tusla's Policy Frameworks for Data Protection, Information Security and Data Governance for broader direction and guidance as they apply agency wide. (A Policy Framework is a comprehensive set of Policies, Procedures, Protocols, Guidelines and Standards, and their organising principle, for an organisational capability.) These documents are available at Tusla Hub.

**CASP Data Protection Guidance** shall comply with the General Data Protection Regulation, Data Protection Act 2018 and Freedom of Information Act 2014 as they apply to how **CASP** operates within the legislative framework for Tusla's substantiation investigations, that is, Section 3, Child Care Act 1991, as amended, and related court judgments, Child and Family Agency Act 2013, Children Act 2001, as amended, Children First Act 2015, Criminal Justice (Withholding Of Information On Offences Against Children And Vulnerable Persons) Act 2012, National Vetting Bureau (Children and Vulnerable Persons) Act 2012, and other applicable legislation.

## 4. Glossary of data protection terms as they apply to CASP

Consult **Tusla Privacy Policy** for data protection definitions as they apply to agency-wide data protection compliance.

Please note that the assessment of data protection risks follows the structure of risk assessment as it applies to Tusla Child Protection and Welfare, and to the Quality Assurance and Risk function, but there is a distinct interpretation of the person as a data subject; how they are vulnerable in respect of how their data is processed; how the person may be harmed; what vulnerabilities and threats to data protection may present themselves; and how to uphold their rights and freedoms of data subjects.

Where a defined term is referenced in the guidance, please check its definition in the Glossary of Terms in the Appendix.

### 4.1. All glossary terms

Acknowledgement
Agreement from a Data Subject
Assent
Assent by a Child or Vulnerable Person
Consent
Consent as a Safeguard
Cross-Border Processing
Data Controller Obligations
Data Controller (Controller)
Data Processing (Processing, Process)
Data Processor
Data Protection Legislation
Data Protection Principles (GDPR Principles)
Data Protection Risk
Data Protection Risk Control (Data Protection Control)
Data Sharing
Data Subject Rights
Data Subject Rights in Balance with Other Fundamental Rights
Data Subject
Data Subject Request
Data Transfer
Filing System
Further Processing
Personal Data
Personal Data Breach
Disclosure
Information Security
Information Security Event
Information Security Incident
Information Security Risk Control (Information Security Control)
The Legal Basis for Processing
Data Transfers to a Third Country
Necessary and Proportionate Processing (Necessary and proportionate to the purpose of the processing)
**Privacy Notice** (Data **Privacy Notice**)
Profiling
Pseudonymisation
Recipient
Restrictions to GDPR (Restrictions to the Scope of Data Controller Obligations and Data Subject Rights)
Restriction of Processing
Risk of Harm to a Data Subject
Risk of Non-Compliance with Data Protection Legislation
Safeguards
Secrecy (Obligations of Secrecy)
Sensitive Personal Data
Sensitive Data in Health and Social Care (Social Work) Sector
Special Categories of Personal Data
Supervisory Authority
Third Party
Threat to a Data Subject
Threat Relating to an Information Asset
Transparency of Data Processing
Upholding the Rights and Freedoms of Data Subjects
Vulnerability of a Data Subject
Vulnerability of an Information Asset
White List



# 5. Data Protection Guidance

## 5.1. Ensuring lawful and fair processing in CASP

### 5.1.1. The legal basis

#### *5.1.1.1. The Legal Basis under the GDPR*

When Tusla processes Personal Data in the delivery of its services to children and families, it does so as a Data Controller acting in the exercise of its official authority for the provision and management of child and family services, and in the public interest.

The legal basis is:

> GDPR, Article 6 1(e): "*processing 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*".

The conditions for processing special categories of data (i.e., certain types of sensitive Personal Data) are:

> GDPR, Article 9: "*processing is 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 the conditions and safeguards referred to in paragraph 3;*"
>
> And additionally,
>
> "*processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;*"

#### *5.1.1.2. The legislative framework which determines this legal basis for data processing for Services to children and Families*

Tusla's data processing is on the basis of Irish laws which determine the authority of the Child and Family Agency, Child and Family services, and the legal obligations of the agency. Section 3, Childcare Act 1991 provides the basis for **CASP**. The following are other pieces of relevant legislation:

- Child Care Acts 1991 – 2015 - specifically, Section 3 of Child Care Act 1991 (as amended)
- Child and Family Agency Act 2013
- Children Acts 2001 - 2015
- Children First Act 2015
- Criminal Justice (Withholding Of Information On Offences Against Children And Vulnerable Persons) Act 2012
- National Vetting Bureau (Children and Vulnerable Persons) Act 2012

#### 5.1.1.3. *The legal basis for undertaking substantiation investigations*

Tusla undertakes substantiation investigations under Section 3 of the Child Care Act 1991, as amended, which imposes obligations on Tusla to investigate complaints of abuse and to mitigate any risks that are identified. Section 3 provides as follows:

> *(1) It shall be a function of the Agency to promote the welfare of children who are not receiving adequate care and protection.*
>
> *(2) In the performance of this function, the Agency shall—*
>
> *(a) take such steps as it considers requisite to identify children who are not receiving adequate care and protection and co-ordinate information from all relevant sources relating to children.*

Courts have made judgments which have clarified further Tusla's legal basis for carrying out substantiation procedures.

The nature and extent of the duties imposed on the Agency by Section 3, Child Care Act 1991 were first considered in the case of MQ v Gleeson [1998] 4 I.R. 85.

The following case law is also relevant:

MI v HSE 2010 IEHC 159
P.D.P. v. Board of Management of a Secondary School & Another [2010] IEHC 189
E.E. v. Child and Family Agency [2016] IEHC 777
TR v CFA 2017 IEHC 595
WM v CFA [2017] IEHC 587
FA v CFA & Others [2018] IEHC 806
EOC v CFA & Others 2019 IEHC 843
CD v CFA 2020 IEHC 452

#### *5.1.1.4. The legal basis for data processing under fair procedures*

Court judgments have established that Tusla should carry out substantiation investigations under Section 3 of the Child Care Act 1991 and in doing so, be mindful to carry out child protection duties and ensure that fair procedures are afforded to the Person Subject to Abuse Allegations (PSAA). 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 an investigation in accordance with natural justice and constitutional justice.
- Tusla must provide fair procedures to the PSAA including the right to be informed of the complaints and the right to respond.
- Tusla must conduct an investigation based on natural justice to substantiate an allegation following a response from the PSAA.
- Tusla must provide all relevant materials which were assembled in substantiating an allegation to the PSAA.
- 
- The existence of a pending criminal prosecution against the PSAA does not alleviate Tusla's duty to investigate the allegations. Decisions on how to proceed in such circumstances should be made in consultation with An Garda Siochana.

### 5.1.2. The status of consent from the data subject; seeking agreement from a data subject

Consent does not apply as a legal basis at Tusla even where Tusla seeks agreement from the data subject to process data. The conditions for consent which are required by the GDPR, specifically the condition that consent is 'freely given', are unlikely to be fulfilled where the data subject is a citizen interacting with a public authority as the data controller. There is likely to be a power imbalance between the citizen and the public authority such that it is difficult to ensure that consent was freely given by the citizen.

Nevertheless, the data controller may afford the data subject some degree of autonomy by engaging the data subject in the data processing through some form of agreement, which we describe here as

- Acknowledgement
- Assent
- Consent

The social worker must record the agreement and must fully inform the data subject, verbally and in writing:

- what form of agreement the agency is seeking (acknowledgement, assent, consent);
- what are the rights of the data subject relative to the form of agreement;
- what are the consequences of agreeing and not agreeing for the data subject (and the process); and
- to what is the data subject agreeing. The data subject may agree to participate in a process, for a process to proceed, or to data processing relating to the process.

(See Full Glossary of Terms for definitions of Acknowledgement, Agreement from a Data Subject, Assent, Assent by a Child or Vulnerable Person, Consent, and Consent as a Safeguard).

#### *5.1.2.1. Acknowledgement*

Tusla may seek acknowledgement from a data subject that their data shall be processed in a certain manner (for example, acknowledgement that Tusla shall contact relevant third parties). If the data subject acknowledges that their data shall be processed in a certain manner with sufficient notice, they have an opportunity to object to the processing or to take measures themselves in their own interest. If acknowledgement is required by the procedure, the social worker must record the acknowledgement in the case records. The data processing may take place without the acknowledgement of the data subject or even if they have objected to the process (as long as Tusla shall have responded to the objection with a justification). (See Acknowledgement.)

#### *5.1.2.2. Assent*

Tusla may seek 'assent' from a data subject, which provides a limited degree of control to the data subject (more than acknowledgement but less than consent) by requiring that the data subject agree that certain data processing takes place but in the context where the social worker explains that if the data subject does not assent, then their refusal to assent shall have a substantial impact on the substantiation investigation. This may apply where Tusla seeks to contact a clinical practitioner and request information required for the substantiation investigation. The social worker should explain the data processing in detail and the consequences of not assenting, and should record the assent. The data processing shall not take place without the assent of the data subject. (See Assent.)

The data subject has the right not to assent, and to change their mind and remove their assent. (This does not affect any data processing that has already taken place so, for example, if Tusla has collected data by assent which has been included as relevant material to the substantiation investigation, it will continue to be processed in the investigation.)



#### *5.1.2.3. Consent*

Tusla may seek 'consent' from a data subject to engage in a process where the data processing is not necessitated by the process. Tusla may seek 'consent' from a data subject to a certain data processing where the data subject has the right to refuse to consent and this refusal shall not have an impact on the substantiation investigation to a degree that may be considered "substantial". The data processing shall not take place without the consent of the data subject.

#### 5.1.2.4. Assent by a Child or Vulnerable Person

Tusla should not seek 'consent' from a child and should not seek 'consent' from an adult who does not have the capacity to 'consent' (i.e. a vulnerable individual) to the data processing or participation in a process. In this case, a parent/guardian should provide consent while the child or vulnerable individual provides assent. Tusla should always seek 'assent' where the agency seeks 'consent' from a parent/guardian on behalf of a child or vulnerable individual. If the 'assent' is for participation in a process, this should be clear and the data subject should be informed that the data processing (and possibly the participation of the parent/guardian) may continue without the data subject's assent to participate in the process. (See Assent by a Child or Vulnerable Person.)

#### 5.1.2.5. Are there separate obligations regarding how we share information relevant to a child complainant versus how we share information relevant to an adult complainant?

**Data Protection Obligations or Guidance:** The GDPR requires that the Data Controller consider *specific protection measures* with the regard to the Personal Data of children as "*they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data*" (Recital 38, GDPR).

- Consent and assent - While the age of 'digital consent' (consent to access information society services offered directly to children) is set to sixteen under Data Protection Act 2018, Recital 38 notes that "*consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child*", which is relevant to Tusla Operations. When consent is applied as a safeguard to the data processing, the parental guardian should consent on behalf of a child up to the age of sixteen but Tusla should also seek the child's assent. Tusla may decide to act under the child's consent if the parental guardian is refusing to provide consent, but the child wants to give consent, and this is in the best interest of the child.
- Transparency and information about the processing – Tusla should inform children about the processing in a manner that is appropriate to the child's level of understanding so that the child understands to the best of their ability the risks, consequences, safeguards and their rights relative to how Tusla processes their data.
- This guidance also applies to adults who "*may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data*" (Recital 38, GDPR)."



## 5.2. Assessing and treating data protection risks in CASP

See Data Protection Risk Management Policy and Procedure for full details.

### 5.2.1. Risks and Risk Controls

- A data protection risk is a risk of harm to the data subject or a risk of non-compliance with data protection legislation.
- A Data Protection Risk Control is a measure to mitigate a risk to data protection. A **Privacy Notice** (see CASP Privacy Notice(s)) is an example of a risk control as it controls the risk that a data subject's right to information about the processing and about their data subject rights may not be fulfilled.

- An Information Security Control is a measure to mitigate the risk to the confidentiality, integrity and availability of information (or a particular information asset, such as a file or a database). Information security is the protection of the confidentiality, integrity and availability of information. Information security controls are important in protecting Personal Data and are therefore data protection risk controls (although they may protect information that is not Personal Data also). An example of an information security control is an encrypted, password-protected zipped folder for email attachments – this control protects against the risk of un-authorised access to data if an email was misdirected to an unintended recipient or was illegally intercepted in transit.
- Safeguards (which are synonymous with risk controls) are any measures which the Data Controller puts in place to ensure that the Personal Data is protected against a Personal Data Breach or a breach of compliance with data protection legislation.

#### 5.2.2. Risk of Harm to a Data Subject

A data subject may experience harm from non-compliance with data protection legislation or from a data breach. The harm from a data breach may be physical, material or non-material damage such as "*loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned". (GDPR, Recital 85).* The harm from non-compliance with data protection may include a lack of knowledge about the data processing or their data subject rights, and thereby, consequent inability to assert their rights which may have an adverse impact on them similar to that caused by a data breach. The risk categories are as follows:

- 03 A data subject may experience harm. GDPR Recital 85 provides examples of harm to a data subject.
- 03.01 A data subject may lose control over their personal data (GDPR Recital 85).
- 03.02 A data subject may experience limitation of their rights (GDPR Recital 85).
- 03.03 A data subject may experience discrimination (GDPR Recital 85).
- 03.04 A data subject's identity may be stolen or the data subject may be a victim of fraud (GDPR Recital 85).
- 03.05 A data subject may experience financial loss (GDPR Recital 85).
- 03.06 A data subject may experience harm if there is unauthorized reversal of pseudo-anonymization of their data, e.g. the harm of loss of confidentiality (GDPR Recital 85).
- 03.07 A data subject may experience harm to their reputation (GDPR Recital 85).
- 03.08 A data subject may experience loss of confidentiality of their personal data which has been protected by professional secrecy (GDPR Recital 85).
- 03.09 A data subject may experience a significant economic or social disadvantage (GDPR Recital 85).

#### 5.2.3. Risk of non-compliance with data protection legislation

If a risk to compliance with data protection legislation materialises, an adverse impact on data subjects is likely as detailed under **Risk of Harm to a Data Subject**. The risk of non-compliance with legislation may be categorised as follows:

- 05 There is a risk of non-compliance with Standards/Regulations/Legislation, specifically data protection legislation and associated standards, regulations, policies and procedures.
- 05.01 The organisation may not be compliant with GDPR Principles (Articles 5-11).
- 05.02 The organisation may not be compliant with GDPR Rights of the Data Subject (Articles 12-23)
- 05.03 The organisation may not be compliant with GDPR - Controller and Processor obligations (Articles 24-43).
- 05.04 The organisation may not be compliant with GDPR - Transfers of personal data to third countries or international organisations (Articles 45-50).
- 05.05 The organisation may not be compliant with GDPR - Provisions relating to specific processing situations (Articles 85-91) National law may apply - check other risk categories
- 05.06 The organisation may not be compliant with GDPR Recitals and other articles not categorised in 05.01-05.05.
- 05.07 The organisation may not be compliant with Data Protection Act 2018 (as amended).
- 05.08 The organisation may not be compliant with Data Sharing and Governance Act 2019 (as amended).
- 05.09 The organisation may not be compliant with S.I. No. 347/2019 - European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) (Amendment) Regulations 2019.
- 05.10 The organisation may not be compliant with GDPR generally if the data processing is not necessary, proportionate with sufficient safeguards to protect the data (general category - broad application through the articles).
- 05.11 The organisation may be non-compliant with the decisions, instructions or other regulatory communication of the Data Protection Commission issued to the organisation.
- 05.12 The organisation may be non-compliant with DPC decisions, official guidelines or other regulatory communication issued to data controllers in this sector or generally.
- 05.13 The organisation may be non-compliant with the decisions, official guidelines or other regulatory communication issued by the European Data Protection Board (EDPB) or its predecessor (Article 29 Working Party).
- 05.14 The organisation may be non-compliant with data protection legislation indicated by concerns which may be raised from the circumstances of a fine issued to a data controller in any member state of the European Union (for example, a fine to a hospital in Portugal regarding access control raised concerns for hospitals across the EU).

#### 5.2.4. The potential harmful impact on a data subject when a threat exploits a vulnerability in data processing

If there are vulnerabilities in the manner in which data is processed, this may expose the Personal Data of the Data Subject to threats which may be an actor or an event. (For example, if there is no risk control in place to check the veracity of an address, human error (vulnerability) may cause a letter to be sent to the wrong address which in turn may be opened by an unintended recipient (threat agent), which would cause a data breach (adverse impact on compliance) and possible harm to a data subject (adverse impact on the data subject, at a minimum, loss of confidentiality).

### 5.2.5. Vulnerability of a data subject

The GDPR requires an additional layer of protection for data subjects who may be vulnerable and makes specific provisions for children as vulnerable data subjects.

- Firstly, a data subject may be vulnerable based on their capacity to understand the data processing and assess risks to themselves, for example, a child. An adult may also be vulnerable due to their capacity to consent due to an intellectual disability, a mental health challenge, or a temporary loss of capacity to understand and assess, for example, due to significant distress or trauma. ("Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned with their rights in relation to the processing of personal data." Recital 38, GDPR)
- Secondly, a data subject may be vulnerable due a power imbalance between the data controller and the data subject (as applies to a citizen in relation to a public body, an employee in relation to an employer, and a regulated person in relation to a regulator).
- Thirdly, a data subject may be vulnerable if the data processing has the potential to have a significant impact on the data subject, such as where data is processed in order to carry out an assessment which concludes with a decision made about a data subject which has a significant impact on their lives; where the data processing has the potential to cause significant distress or even trauma to the data subject; or where errors, non-compliance or a data breach may cause a significant harm to the data subject due to the sensitive nature of the data or the sensitive context for the data processing.

### 5.2.6. Vulnerability of an information asset

An information asset (e.g. an IT system, a paper document, a template, a collection of records, Personal Data) may have a weakness, that is, a vulnerability, which can be exploited by a threat, and this may have an adverse effect on a data subject or the agency's data protection compliance. For example, if a system or organisational procedure does not provide controls to enable (or force) review of recorded data, then errors may occur and this would harm the integrity of the data, with consequent potential harm to the data protection compliance and/or potential harm to a data subject.

### 5.2.7. Risk evaluation

#### *5.2.7.1. Risk score*

In evaluating a data protection risk, follow the scoring in **Tusla's Organisational Risk Management Policy and Procedure** scoring on a scale of 1-5 for likelihood and 1-5 for impact. The risk score is calculated as "likelihood X impact".

| | Impact Score | | | | |
|---|---|---|---|---|---|
| **Likelihood** | **Negligible (1)** | **Minor (2)** | **Moderate (3)** | **Major (4)** | **Extreme (5)** |
| **Almost certain (5)** | **5** | **10** | **15** | **20** | **25** |
| **Likely (4)** | **4** | **8** | **12** | **16** | **20** |
| **Possible (3)** | **3** | **6** | **9** | **12** | **15** |
| **Unlikely (2)** | **2** | **4** | **6** | **8** | **10** |
| **Rare/Remote (1)** | **1** | **2** | **3** | **4** | **5** |

| **Colour code** |
|---|
| **High risk** |
| **Medium risk** |
| **Low risk** |

#### *5.2.7.2. Risk likelihood*

The likelihood of the risk materializing is evaluated within a timeframe of five years as illustrated in the table below (sourced from **Tusla's Organisational Risk Management Policy and Procedure** and referenced in the Data Protection Risk Management Policy and Procedure.

**Table 1: Risk Likelihood**

| | Rare / Remote | Unlikely | Possible | Likely | Almost Certain |
|---|---|---|---|---|---|
| **Likelihood Score** | 1 | 2 | 3 | 4 | 5 |
| **Actual Frequency** | Every 5 years or more | Every 2 – 5 years | Every 1 – 2 years | Bi-annually | At least monthly |
| **Probability** | 1% | 10% | 50% | 75% | 99% |

#### *5.2.7.3. Risk impact*

The potential impact is measured either as harm to a data subject (category 3) or to data protection compliance (category 5). (A risk relating to data protection may also be evaluated as an information security risk with the potential impact being measured based on harm to an information asset.) A data breach should be assessed as harm to a data subject. A risk under the category of data protection compliance risks should consider not just the impact of non-compliance but by the impact on a data subject of that non-compliance.

#### 5.2.7.3.1. Risk impact – potential impact to a data subject

The table below illustrates the factors to consider in evaluating the potential impact on a data subject. The examples should be used as an aid for a qualitative assessment of the combined factors. The overriding consideration is that a data breach or a breach of compliance relating to sensitive data about vulnerable individuals should score 4 out of 5.

Risk category 3: A data subject may experience harm. (The adverse impact on a data subject may also be the means of scoring a risk of non-

| **Impact** | **Negligible** | **Minor** | **Moderate** | **Major** | **Extreme** |
|---|---|---|---|---|---|
| | **1** | **2** | **3** | **4** | **5** |
| Volume of data | *A data item in a file* | *A small file of data* | *A full record* | *An extensive record over time* | *All data maintained by the agency about the individual and involving extensive records over time.* |
| Category of personal data | *Name or other identifier (not Medical or Social Care Record Number – special category) and limited information about the person (e.g. timetable); work contact information only* | *Contact information including home address, personal phone number and personal email address* | *Special category information* | *Special categories of information including health and social care information or criminal record information* | *Any information whose disclosure, particular to the individual, may cause moderate to extreme harm as defined in the Organisational* |
| Category of data subject | *An adult* | *An adult engaging with Tusla as a citizen* | *A child* | *A vulnerable child* | *A child at risk* |

| | | | | | |
|---|---|---|---|---|---|
| Impact on an individual – Safety | *Sample scenario* | *Sample scenario* | *The individual is fearful of their safety.* | The individual must be moved from their residence for their safety. | The individual is harmed due to disclosure of their residence. |
| Impact on an individual – physical or psychosocial | Irritation but no physical or psychosocial harm that might be recorded in a medical or social care assessment. | Damage to reputation, annoyance but no physical or psychosocial harm that might be recorded in a medical or social care assessment. | Physical or psychosocial impact confirmed by clinical practitioner | Clinical intervention required | Acute clinical intervention required (hospitalisation) |
| Impact on an individual – financial harm | | Loss of some income | Significant loss of income | Loss of earnings | Loss of income and/or earnings with impact also on future income/earnings |
| Impact on an individual – reputation | Irritation | Annoyance and damage to reputation with no material impact (not possible to define any actual impact other than annoyance) | Damage to reputation with material impact | Major damage to reputation to serious material impact | False incrimination |
| Number of individuals involved | 1+ | 2-50 | 50-250 | 250-1,000 | More than 1,000 |

#### *5.2.7.4. Risk tolerance*

Note that social work involves high risk data processing: low, medium and high risk evaluation are relative to the environment. High and medium risks must be treated with controls and monitored. Low risks may be treated and must be monitored. Often risk treatment may reduce the likelihood only but not the potential impact.

### 5.2.8. NB: Rules to follow when managing data protection risks

- **The social worker must identify, assess, treat and monitor data protection risks in daily data processing activities.**
- **The social worker shall only apply a temporary deferral in the fulfilment of data subject rights if the risk to the data subject, another person or other persons is high (i.e. a risk score of 16 or higher). This shall apply in whole or in part to the Right to Information about the Processing, the Right of Access and the Right to Restriction of Processing (Restrictions to the scope of the GDPR apply solely for "*the protection of the data subject or the rights and freedoms of others*". See Restrictions.)**
- **The social worker shall only apply a permanent restriction (or extended deferral of more than a year) in the fulfilment of data subject rights if the risk to the data subject, another person or other persons is extremely high (i.e. a risk score of 20 or higher). This shall apply in whole or in part to the Right to Information about the Processing, the Right of Access and the Right to Restriction of Processing (Restrictions to the scope of the GDPR apply solely for "*the protection of the data subject or the rights and freedoms of others*". See Restrictions.)**

## 5.3. Fulfilling Data Protection Principles in CASP

*Rules to fulfil principles*

- Ensure that Tusla processes data in a manner consistent with **CASP** and **CASP Guidance** and that data processing fulfils Data Protection Principles as defined in **CASP Data Protection Guidance** and **Tusla Privacy Policy**.
- Apply the same rules for any information format including spoken information, disclosure on site, and audio and video recording.
- Seek the guidance of the line management or the Data Protection Unit if in doubt as to how to proceed.
- Record any decision to process data where there was a degree of challenge to determining whether a certain principle was fulfilled.
- Record any decision to process data where Tusla applied a restriction to the scope of the obligations of the data controller to fulfil the data protection principles as laid out in the GDPR. (Restrictions to the scope of the GDPR apply solely for "*the protection of the data subject or the rights and freedoms of others*". See Restrictions.)
- Raise a concern through line management or directly to the Data Protection Unit if you perceive that there is a conflict between the data processing as defined in **CASP** Practice and Guidance documents and your understanding of data protection compliance.

### 5.3.1. Principle of Lawfulness, Fairness and Transparency

#### *5.3.1.1. Principle*

Personal data shall be *processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'); (GDPR, Article 5)*

#### *5.3.1.2. Rules to fulfil the principle*

- Ensure that Tusla processes data in a manner that is lawful and fair, according to its legal basis as defined in **CASP Data Protection Guidance** or **Tusla Privacy Policy**.
- Ensure that Tusla processes data in a manner that is fair, that is, as might be understood to be carried out in the public interest, follow the principles of natural justice, and would not surprise or concern the data subject.
- Ensure that Tusla processes data in a manner that is consistent with how the data processing is described to the data subject in the **Privacy Notice** (see CASP Privacy Notice(s)) or other information about the processing.

### 5.3.2. Principle of Purpose Limitation

#### *5.3.2.1. Principle*

Personal data shall be *collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');*

*(GDPR, Article 5)*

#### *5.3.2.2. Rules to fulfil the principle*

- Be aware of the purpose of the data processing as it is described in **CASP**, **CASP Guidance**, **CASP Data Protection Guidance**, and the **Privacy Notice** (see CASP Privacy Notice(s)) or other information provided to the Data Subject.
- Be aware of the purpose of each form which collects data and the purpose of each correspondence template that discloses data.
- Be aware of the purpose of collecting each item of data and the purpose of disclosing each item of data.
- Do not process data in a manner that extends the purposes of the data processing beyond the fulfilment of **CASP** or the further processing which has been defined and assessed as consistent with the processing or in the public interest in Tusla's exercise as an official authority and under legislation (in the provision and management of Child and Family Services, for child protection or fair procedures, for Tusla to fulfil a legal obligation in the public interest, or for the retention of records in the public interest).
- Do not process data beyond the purpose specification when collecting or disclosing data in consideration of a full record of data and each data item in the record.

#### *5.3.2.3. Specific directions*

- Always use a standard form when collecting information and keep the stated purpose in mind as you collect and input the data into the form.
- Always use the standard correspondence template when disclosing information in writing and keep the stated purpose in mind as you prepare the correspondence.

- Be familiar with the purpose of the data processing as described in the **Privacy Notice** and the policy and guidance documents.
- State the purpose of the data processing to the data subject at each stage of the process.
- Limit data processing in spoken information, disclosure on site, and audio or video recording to the purpose specified in the same manner as applying the principle to any written record.

### 5.3.3. Principle of Data Minimisation

#### *5.3.3.1. Principle*

Personal data shall be *adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'); (GDPR, Article 5)*

#### *5.3.3.2. Rules to fulfil the principle*

- Ensure that a person or organisation is informed of the purpose of the data processing when requested to disclose or send Personal Data but make sure to minimise Personal Data in the explanation of the purpose of the Data Processing.
- Do not collect more Personal Data than is necessary and proportionate to the purpose when you request information from a data subject.
- Do not request more Personal Data than is necessary and proportionate to the purpose when you request information from third parties, such as clinical practitioners.
- Always advise a person or organisation providing information to limit the data they disclose or deliver to what is necessary and proportionate to the purpose.
- If you receive more information that you required from a third party, avoid reviewing the information, make a record of what you received, send it back to the third party, do not use or reference the information in any data processing, except where required to disclose the set of 'relevant materials' and note exclusions (i.e. when disclosing 'relevant materials', it may be appropriate to note the files that were not deemed 'relevant materials').
- If the data subject voluntarily provides more information than was necessary and proportionate to the purpose, avoid reviewing the information, discuss with the data subject how you believe that the information is not necessary or proportionate and the consequences of the data being retained, take into account the opinion of the data subject on whether it is necessary and proportionate and reach an agreement on what to process, return the excess information to the data subject, make a record of what you received, do not use or reference the information in any data processing, except where required to disclose the set of 'relevant materials' and note exclusions (i.e. when disclosing 'relevant materials', it may be appropriate to note the files that were not deemed 'relevant materials').
- If another third party organisation provides more information than was necessary and proportionate to the purpose, avoid reviewing the information, discuss with the third party how you believe that the information is not necessary or proportionate and the consequences of the data being retained, take into account the opinion of the third party on whether it is necessary and proportionate and reach an agreement on what to process, return the excess information to the third party organisation, make a record of what you received, do not use or reference the information in any data processing, except where required to disclose the set of 'relevant materials' and note exclusions (i.e. when disclosing 'relevant materials', it may be appropriate to note the files that were not deemed 'relevant materials').

#### *5.3.3.3. Specific directions*

- Use the standard forms and correspondence templates to minimise the data collected or disclosed.
- Only request material from complainants or third parties which is likely to be relevant to the investigation. Questions and requests for information should be based on a reasonable line of enquiry which would depend on the facts and issues in the individual case, including any potential defence. For example, it may not always be necessary or appropriate to seek detail of a complainant's mental health, addiction issues or their hobbies.
- NB: See Disclosing data safely for detail.

### 5.3.4.Principle of Accuracy

#### *5.3.4.1. Principle*

Personal data shall be *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 ('accuracy');* (GDPR, Article 5), see Section 27 of the **CASP Guidance**.

#### *5.3.4.2. Rules to fulfil the principle*

- NB: Review **CASP Guidance** directions on ensuring the reliability and accuracy of data.
- It is essential that the Personal Data has an acceptable standard of data quality. The principle of accuracy depends on other attributes of data quality which ensures that the data is fit for its intended purpose (the quality of information or any asset may be assessed by whether it is 'fit for purpose').
- Data should be assessed on these data quality attributes:
    - Accurate – The data is free from error and up-to-date. The data should be consistent and avoid inconsistencies such as multiple identities or variations in the expression of terms.
    - Complete – The data should be sufficiently comprehensive (while proportionate) to fulfil the purpose. The data should maintain its integrity and completeness during transfer and in all locations.
    - Reliable – The data may be relied on for its intended purpose.
    - Relevant – The data should be relevant to its intended purpose. The data should conform to the requirements and standards as specified in the policy and guidance documents.
    - Timely – The data should be up-to-date or timestamped to its last update. It should be available for use at the time that it is required.
- Always verify records with the person who provided the information to confirm that any records that you have taken are an accurate and true account of the information provided to you.
- Always ensure that when you request information that you request information that is accurate and fit for purpose.
- Check the data for accuracy and data quality when you receive data from an information source.
- Check the data for accuracy and data quality before you disclose information to a recipient.
- Apply a review procedure to accuracy and data quality for all items and records of data.
- Apply an authorisation procedure to accuracy and data quality for all items and records of data.

#### *5.3.4.3. Specific directions*

- Be mindful that inaccurate contact details may cause an unauthorised disclosure, and effectively, a data breach.
    - Check contact details each time that you interact with a data subject, as appropriate to the sensitivity of the context.
    - Check contact details against reliable sources of information (e.g. Eircode).
    - Use the Eircode to ensure that the address is complete.
- Always use a blank form or template in Tusla Case Management System (TCMS) and never adapt a previously completed form or template as there is a risk that data may persist in the form from the previous use.

### 5.3.5. Principle of Storage Limitation

#### *5.3.5.1. Principle*

Personal data shall be *kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation'); (GDPR, Article 5)*

#### *5.3.5.2. Rules to fulfil the principle*

- Do not retain Personal Data for longer than is required to fulfil the specified purpose as defined in **CASP** and **CASP Guidance**, and in the Records Management Policy.
- 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).
- Tusla must retain records after their active use. These records should have restrictions on their access and edit, as determined by the ICT Directorate. NCCIS and TCMS shall apply the rules for restricted access. Ensure that files which are not held on NCCIS and TCMS have restrictions applied to them as appropriate.
- Tusla should hold records according to three levels of storage as defined in the Records Management Policy (Records Retention Policy and Schedule): active use, retained for reference after active use ('near archive'), and retained in archive for the purposes of accountability. Tusla Operations staff who have authorised access to records retained after active use for exceptional access for **CASP** should follow the Records Management Policy (Records Retention Policy and Schedule) as it applies to retained records and consult with the ICT Directorate where advice is required.
- Limit the proliferation of 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.

#### *5.3.5.3. Specific directions*

- If communicating with a colleague who also has access to the dedicated systems (TCMS or NCCIS), prefer referring the colleague to the dedicated 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 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.)
- If a file is not deemed 'relevant material' to an investigation, return it to its source.
- Follow Tusla's Information Security and Data Governance Policy Framework in respect of managing paper copies (notably, Acceptable Usage Policy and Information Classification and Handling Standard).

### 5.3.6. Principle of Integrity and confidentiality

#### *5.3.6.1. Principle*

Personal data shall be *processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')*. (GDPR, Article 5)

#### *5.3.6.2. Rules to fulfil the principle*

See Section 5.5 - Ensuring that the data processing is necessary and proportionate to the purpose and that safeguards are applied to protect the data.

### 5.3.7. Demonstrating accountability for the Data Protection Principles

#### *5.3.7.1. Principle*

*The controller shall be responsible for, and be able to demonstrate compliance with [the Data Protection Principles ('accountability').* (GDPR, Article 5)

#### *5.3.7.2. Rules to fulfil the principle*

- Keep a record of decisions on how the Data Protection Principles were applied and where restrictions to the scope of the obligations in respect of Data Protection Principles were applied. (Restrictions to the scope of the GDPR apply solely for "*the protection of the data subject or the rights and freedoms of others*". See Restrictions.)

## 5.4. Upholding the Rights and Freedoms of Data Subjects in CASP

### 5.4.1. Rules to uphold the data subject rights

- Ensure that Tusla upholds the rights of the data subjects by ensuring fair and lawful processing.
- Keep the data subject informed about the data processing and of their data subject rights at each stage of **CASP**.

- Fulfil a data subject request (rather than referring the data subject to the Data Protection Unit) where it is consistent with the department's policy and procedure, standard practices, in sensitivity to the needs of the data subject.
- Fulfil a data subject request (rather than referring the data subject to the Data Protection Unit) where it is appropriate to maintain the data subject's confidentiality and in sensitivity to the needs of the data subject.
- Refer the data subject to the Data Protection Unit where data protection specialists should fulfil a request, sensitive to the needs of the data subject and according to the preference of the data subject.
- Seek the support and advice of the Data Protection Unit if in doubt how to proceed.
- Maintain the anonymity of the data subject when liaising with the Data Protection Unit, and in sensitivity to the needs of the data subject.
- Record every data subject request and how it was fulfilled.
- Record every complaint from a data subject about how their data is processed and how it was dealt with.
- Record any decision to manage a data subject request where there was a degree of challenge to determining whether a certain right was fulfilled.
- Record any decision to manage a data subject request where Tusla applied a restriction to the scope of the obligations of the data controller to fulfil the data subject rights as laid out in the GDPR. (Restrictions to the scope of the GDPR apply solely for "*the protection of the data subject or the rights and freedoms of others*". See Restrictions.)
- Raise a concern through line management or directly to the Data Protection Unit if you perceive that there is a conflict between the data subject rights management as defined in the **CASP** and **CASP Guidance** documents, and your understanding of how data subject rights should be upheld.

#### *5.4.1.1. Data subject rights management in TCMS and Operations*

The data management system (as defined in CASP Data Management Plan) enables

- the provision of records to fulfil a **data subject access request;**
- the **amendment of a record** to fulfil a data subject's request;
- the restriction of processing of a record or a part of a record (e.g. restricted access) if required to fulfil the **right to restriction of processing** or restriction while the **right to object** is being addressed; and
- the erasure of a record or a part of a record to fulfil the right to erasure ('right to be forgotten').

- The department responsible shall provide the data subject with a **Privacy Notice** (see CASP Privacy Notice(s)) when the data subject submits a request.
- There is a record of an **amendment, restriction to processing or erasure of a record** (e.g. system logs).
- The department responsible has a defined authorization procedure for the **amendment, restriction and erasure of records.**

### 5.4.2.The Right to Fair and Transparent Processing

Data subjects have a right to fair, lawful and transparent processing and to receive a defined set of information about how their data is being processed. Where data is collected about a person but not

directly from that person, the data subject must be informed within one month of the data processing (Article 14, GDPR).

#### *5.4.2.1. Rules to uphold the data subject rights*

- Ensure that the data subject receives a **Privacy Notice** (see CASP Privacy Notice(s)) and information about the processing in a timely fashion and communicate with the data subject in a manner that they will clearly understand.
- If you seek consent / assent from the data subject (or their parental guardian) to collect data from a third party or otherwise process data, you must provide a form that fulfils the conditions for consent / assent. If you are seeking consent as a 'safeguard' the form must clarify that consent is a 'safeguard' and not the legal basis. If you are seeking consent from parental guardian on a child's behalf, the child should assent. Both the data subject and the parental guardian, if applicable, must receive a **Privacy Notice** at the time of reviewing the consent form. (See The status of consent from the data subject; seeking agreement from a data subject.)
- At every interaction with the data subject, make the **Privacy Notice** available and remind the data subject of their rights as follows.
    - Attach the **Privacy Notice** to every correspondence by letter or email.
    - Provide a printed **Privacy Notice** leaflet when meeting with the data subject face to face.
    - Make the general **Privacy Notice** available at Tusla contact points.
- Refer to the **Privacy Notice** (see CASP Privacy Notice(s)), **CASP Data Protection Guidance** and the **CASP** policy documents to support you in verbally providing the data subject with information about the processing and their rights.

### 5.4.3. The Right to Information about the Processing

- Inform a data subject about the data processing and their rights by providing a **Privacy Notice** (see CASP Privacy Notice(s)) to them, explaining to them otherwise the purpose and nature of the processing, and being prepared to answer their questions on the data processing and their rights as data subjects.
- Note that the **Privacy Notice** covers all the elements of information required under Articles 13-14 and it presents the information in a manner compliant with Article 12. A verbal explanation will further enhance the transparency on the data processing.
- If you are collecting Personal Data directly from the data subject, you must inform the data subject about the data processing and their rights when (or before) you are collecting their data.
- If you are collecting Personal Data from a source other than the data subject (e.g. when you collect information relating to a PSAA from the Complainant), you must inform the data subject about the processing and their rights within a reasonable period and no later than one month from first collecting the data.

### 5.4.4. The Right of Access

- If a data subject requests access to information held about them, carry out the request consistent with **CASP** practices but also ensure that the requirements in fulfilling a data subject request are being met.
    - Acknowledge the request promptly.

- Remind the data subject of their rights by providing a **Privacy Notice** (see CASP Privacy Notice(s)) to them.
- Fulfil the request promptly keeping the data subject informed of progress.
- Redact the records of other data subjects' data.
- Fulfil a data subject access without delay and no later than within 30 days.
- Seek assistance from the Data Protection Unit if fulfilling the request is complex and substantial.

#### 5.4.5. The Right to Rectification

- If a data subject requests rectification of information held about them, consider carrying out the request consistent with **CASP** practices but also ensure that the requirements in fulfilling a data subject request are being met.
  - Acknowledge the request promptly.
  - Assess the request and verify the accuracy and validity of the rectification.
  - Remind the data subject of their rights by providing a **Privacy Notice** (see CASP Privacy Notice(s)) to them.
  - Fulfil the request promptly keeping the data subject informed of progress.
  - Seek authorisation from line management if the request for rectification is significant.
  - Do not carry out the rectification without authorisation if the request is retrospective and the rectification has significant impact and requires several other actions to take place.
  - Fulfil the request without delay and inform the data subject when you have completed the rectification.
  - Seek assistance from the Data Protection Unit if fulfilling the request is complex and substantial.
  - If you considered that the rectification was not justified, discuss this with the data subject and record their objection if they do not agree with the information retained in the record.

#### 5.4.6. The Right to Erasure (the 'Right to be Forgotten')

- If a data subject requests erasure of information held about them, escalate the request unless this relates to a copy of a file which was not deemed 'relevant material'.
  - Acknowledge the request promptly.
  - Remind the data subject of their rights by providing a **Privacy Notice** (see CASP Privacy Notice(s)) to them.
  - Assess the request and the case for erasure as it applies to the Records Management Policy (Records Retention Policy and Schedule). Consider whether there are valid grounds for erasure.
  - Keep the data subject informed of progress in fulfilling the request.
  - Seek assistance from the Data Protection Unit who may support you in responding to the request or may handle the request directly, as preferred by the data subject and as agreed between Tusla Operations and the Data Protection Unit.
  - If you considered that erasure is not justified, discuss this with the data subject and record their objection if they do not agree with the information retained in the record.

- Consider a restriction to processing (e.g. locking the record and restricting access) if appropriate.
- Inform the data subject of your final decision regarding their request and remind them of their rights, including the right to complain to the Data Protection Commission.

### 5.4.7. The Right to Restriction of Processing

- If a data subject requests Restriction of Process of information held about them, consider carrying out the request consistent with **CASP** practices but also ensure that the requirements in fulfilling a data subject request are being met. Restriction of Processing may involve authorisation to lock a record for a period of time or to pause data processing until Tusla justifies the processing.
  - Acknowledge the request promptly.
  - Assess the request and consider the validity of restricting processing.
  - Consider temporary restriction of processing while assessing the request and responding to the data subject.
  - Remind the data subject of their rights by providing a **Privacy Notice** (see CASP Privacy Notice(s)) to them.
  - Fulfil the request promptly keeping the data subject informed of progress.
  - Seek authorisation from line management if the request for restricted processing is significant.
  - Do not carry out the restricted processing without authorisation if the request is has significant impact, e.g. hinders an investigation or requires several other actions to take place.
  - Keep the data subject informed of progress in fulfilling the request.
  - Seek assistance from the Data Protection Unit who may support you in responding to the request or may handle the request directly, as preferred by the data subject and as agreed between Tusla Operations and the Data Protection Unit.
  - If you considered that restriction of processing is not justified, discuss this with the data subject and record their objection if they do not agree with the information retained in the record.
  - Inform the data subject of your final decision regarding their request and remind them of their rights, including the right to complain to the Data Protection Commission.

### 5.4.8. The Right to Data Portability

- Although the R**ight to Data Portability** is not applicable to this data processing activity, aim to fulfil the principle that the data subject shall receive the data in the format convenient to the data subject as is practicable.

### 5.4.9. The Right to Object to Processing

#### *5.4.9.1. Rules to uphold the data subject rights*

- Seek the support of the Data Protection Unit to manage the right to object to processing as follows.
  - Liaise directly with the data subject or support the Data Protection Unit to liaise with the data subject;
  - acknowledge the objection and provide a **Privacy Notice** (see CASP Privacy Notice(s)) and explanation of how the object shall be managed;

- examine the objection in reference to Tusla policies and consulting with Tusla Office of Legal Services if required;
- restrict processing while the objection is being examined (the record may be locked on TCMS or NCCIS); and
- respond to the objection either by providing a justification to continue the processing or fulfil the data subject's request to restrict, amend or erase as appropriate for data protection compliance.

#### 5.4.10. The Right not to be Subject to Automated Decision-making Including Profiling

- The **right of the data subject not to be subject to automated decision making** is assured. Assessments and decisions which have a significant impact on an individual are always carried out by professionally trained individuals.
- Ensures that data is not used for profiling of data subjects (e.g. ensure that there is a defined purpose and procedure for the collection and use of data which may be vulnerable to misuse).
- Collect data on ethnicity for the purposes of human-rights based analysis and do not process other than for the purposes specified in a human-rights based framework.
- Collect data on nationality for the purposes of human-rights based analysis or to provide consulate assistance to the data subject if required under the Vienna Convention.

#### 5.4.11. The Right to Lodge a Complaint with a Supervisory Authority

- Provide the **Privacy Notice** (see CASP Privacy Notice(s)) to the data subject so that they may be informed of their right to lodge a complaint with the Data Protection Commission and have the contact details to lodge the complaint.
- Be prepared to verbally explain the data subject's right to lodge a complaint with the Data Protection Commission (DPC) and refer the data subject to the DPC's website, www.dataprotection.ie.
- Advise the data subject that may also make a complaint to Tusla's Data Protection Unit if they prefer.

#### 5.4.12. Right to an effective judicial remedy against a controller or processor and related rights

- Note that the data subject has the right to an effective judicial remedy against a controller or processor (and a supervisory authority) if they consider that their rights have been infringed by non-compliance with data protection legislation. (GDPR, Articles 78-79)
- The data subject may mandate an organisation to act on their behalf to lodge a complaint, exercise their rights. (GDPR, Article 80)
- The data subject has a right to compensation and liability if they have suffered material or non-material damage from an infringement of the GDPR. (GDPR, Article 82)

#### 5.4.13. Demonstrating accountability for the Data Subject Rights

- Maintain records of consent / assent / acknowledgement, data subject requests and data subject complaints.

## 5.5. Ensuring that the data processing is necessary and proportionate to the purpose and applying safeguards to protect the data

### 5.5.1. Overview

Tusla's Child Abuse Substantiation Practice Guidance and Review Procedures (**CASP**) assists social workers in safeguarding the rights of children, young people and those who have disclosed abuse whilst ensuring that those who have allegations made against them are afforded fair procedures that are transparent, fair and underpinned with the values of dignity and respect. The welfare of the child remains paramount throughout these processes.

Additionally, Tusla staff must fulfil data protection responsibilities fitting to the context of **CASP**. The General Data Protection Regulation and Data Protection Act 2018 recognise that the requirements of child protection and fair procedures may place certain restrictions (derogations from the scope of the obligations of the data controller) on the application of data protection principles and the rights of data subject. (Restrictions to the scope of the GDPR apply solely for "*the protection of the data subject or the rights and freedoms of others*". See Restrictions.) However, even in these circumstances, the processing of the information that forms part of the **CASP** investigation must be necessary and proportionate to that purpose and the information must be safeguarded. Where a restriction or derogation from a data protection principle or data subject right may apply, this should be defined in the record of data processing and in the **Privacy Notice** (see CASP Privacy Notice(s)).

This guidance includes **Privacy Notice**(s) (see CASP Privacy Notice(s)) which the social worker should make available to data subjects at the earliest opportunity. The social worker should be familiar with the Privacy Notice so that s/he may explain the data processing and the data subject rights verbally.

When carrying out **a substantiation investigation**, a social worker will have to make decisions on what data is collected, its relevance, how it is disclosed or how a data subject is informed about the processing of their data. These decisions may be

1. to fulfil data protection principles or data subject rights and freedoms
2. to restrict data protection principles and data subject rights where child protection, fair procedures, or another basis for the restriction applies relating always to "*the protection of the data subject or the rights and freedoms of others*".

For every decision made, the social worker should record the justification for that decision. This section guides the investigating social worker in making conscious and compliant decisions to protect personal data in this restricted context.



### 5.5.2. General guidelines

- **Necessary, proportionate, safeguarded**: The data processing must be necessary and proportionate to the purpose for which it's being collected and the data must be safeguarded. This principle persists even where there are restrictions and derogations to data controller obligations.
- **Risk-based decision making**: Data protection legislation recognises that there may be situations where confidentiality needs to be prioritized over transparency, disclosure over privacy, and

other human rights and protection of individuals take priority over data protection rights (i.e. "*the protection of the data subject or the rights and freedoms of others*"). The social worker should make decisions on data protection in a risk-based approach assessing potential harms against potential benefits to individuals and society, and putting the risk of harm to a child as a **first concern**, fair procedures as a **second concern** and data subject rights and freedoms as a **third concern** (evaluating likelihood and potential impact effectively). The social worker should be aware that the fulfilling data protection rights may fulfil child protection and fair procedure.

- **Restrictions**: Restrictions to the scope of the obligations of the data controller, in this case Tusla, regarding data protection principles and data subject rights apply to this data processing activity as defined in the General Data Protection Regulations and Data Protection Act 2018. The legal basis for the restrictions and how the restrictions are applied are defined in the **Privacy Notice** (see CASP Privacy Notice(s)). (Restrictions to the scope of the GDPR apply solely for "*the protection of the data subject or the rights and freedoms of others*". See Restrictions.)
- **Recording the application of data protection principles and rights**: Where a social worker makes a decision in compliance with data protection principles and data subject rights, the social worker must record the justification for the decision referring to the interpretation of the CASP Privacy Notice(s).
- **Recording the application of a GDPR restriction**: Where a social worker makes a decision in compliance with the restriction due to a prioritized concern - e.g. a risk to a child, fair procedures, a criminal investigation – the social worker must record the justification for the decision referring to the interpretation of the CASP Privacy Notice(s). (Restrictions to the scope of the GDPR apply solely for "*the protection of the data subject or the rights and freedoms of others*". See Restrictions.)
- **Support and advice from Data Protection Unit**: Where a social worker is unsure how to proceed, they should raise the matter to their line manager and through their line management to the region's Privacy Officer or to the Data Protection Unit (DPU).
- **Compliance with the Child Abuse Substantiation Practice Guidance and Review Procedures (CASP)**: A social worker should not find that a decision to comply with data protection conflicts with the Child Abuse Substantiation Practice Guidance and Review Procedures (**CASP**). If a social worker becomes aware of a potential or actual conflict, they should raise the concern immediately through line management to the Office of Legal Services and the Data Protection Unit so the concern may be assessed and addressed without delay.
- **Compliance with Tusla Data Protection Policy Framework**: Follow Data Protection policies, standards, procedures and guidelines (including **Redaction Policy**).
- **Preserve confidentiality, integrity and availability of data**: Personal data must be protected from threats to its confidentiality, integrity and availability.
- **Compliance with Tusla Information Security and Data Governance Policy Frameworks**: Follow the Information Security and Data Governance Policy Frameworks to ensure that you safeguard data sufficiently.



### 5.5.3. NB: Disclosing data safely

- The standard forms and templates in the **Child Abuse Substantiation Practice Guidance and Review Procedure** and Tusla's **Redaction Policy** guide social workers in disclosing data in a manner that is necessary and proportionate to the purpose of **a** substantiation investigation.

- The decision to disclose a file is independent of the decision to disclose each data item in a file: Where a file must be disclosed to an individual, the social worker must assess whether each data item in the file should be disclosed and redact every item which does not need to be disclosed.
- Disclose data as directed in the procedure and if not defined, at the time in which it is necessary and proportionate to the purpose of the disclosure (e.g. files should be disclosed to the PSAA for fair procedures at the start of stage two as per Section 5 **CASP and then there is an ongoing requirement to provide the PSAA with all relevant material assembled through the Stage Two process to the PSAA**): Where personal data of one data subject may be required to be disclosed to another data subject who is party to the **CASP** procedure, the personal data should be disclosed at the time in which it is necessary and proportionate to the purpose of the disclosure, that is, the latest stage that the personal data may be disclosed to fulfil **CASP** objectives (e.g. child protection, fair procedures, etc.). This will ensure that the data processing is necessary and proportionate.

#### *5.5.3.1. Redaction of templates and forms in Appendices 1-20*

When disclosing files to the PSAA, carry out the redaction as follows. The social worker may decide that an exception applies under certain circumstances, if so, the social worker should make a conscious decision to either not disclose based on data protection or disclose based on a restriction to the scope of the obligations of the data controller and record the justification for the decision. (Restrictions to the scope of the GDPR apply solely for "*the protection of the data subject or the rights and freedoms of others*". See Restrictions.)

##### 5.5.3.1.1. How do I decide what is "relevant material"?

The decision not to redact certain information will usually be to fulfil the obligation to provide the PSAA with information which is relevant to the substantiation investigation. As set out in **CASP Guidance**, a PSAA is entitled to receive all relevant material assembled in the substantiation investigation. The question of what material is relevant to the investigation is important when considering what must be disclosed to the PSAA and what can be redacted.

**Evidence is said to be relevant if it discloses a fact or facts which, on their own or in conjunction with other facts, tends to prove or disprove a live issue in the investigation.**

The key question for a social worker to consider is whether a particular item of evidence is logically probative or disprobative of a fact at issue. An item of evidence (a document / piece of information) is relevant if it renders the fact it seeks to establish slightly more or less probable then the fact would be without the evidence, through the application of everyday experience and common sense.

In considering what information is relevant, social workers should have regard to Section 32 of the **CASP Guidance** 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 complainant's statement and/or behaviour, contemporaneous documentation that supports the complainant's testimony, medical/psychological evidence of abuse/trauma as determined by an expert.

Requests for information or other materials in relation to the above factors should be based on a reasonable line of enquiry which would depend on the facts and issues in the individual case. For example, it may not always be necessary or appropriate to seek detail of a complainant's mental health or addiction issues. Care must be taken when

seeking details about the complainant's past emotional or behavioural difficulties or evidence of medical / therapeutic supports. Such issues may be of limited relevance to the investigation as they may only go so far as to confirm that a complainant has faced personal challenges which could be consistent with them having suffered past abuse.

If material is considered not to be relevant at Stage One of the process, there is no fair procedure obligation to disclose it. In fact, a blanket policy of disclosing all material considered, including exceptionally sensitive personal material, regardless of relevance would amount to a clear breach of a complainant's right to privacy and data protection.

Where material is considered to be relevant to the investigation it can only be withheld where there is a clear and continuing risk of harm to identifiable persons as a result of disclosure. Given the nature of issues involved, such a withholding could only be justified in the most extreme of cases and where the information is withheld to the least extent possible. All other possible options in respect to disclosure, such as anonymisation or independent drafted summaries of the evidence provided, would have to be considered before an ultimate decision to withhold could be justified. Any initial decision to withhold the information gathered at Stage One of the process would obviously have to be made before that information is disclosed to a PSAA at Stage Two of the process. That decision to withhold relevant information would have to be kept constantly under review and be reactive to any information that suggests that any initial perception of harm is no longer accurate. Therefore, in rare instances, it may be necessary to disclose information which had initially been withheld due to a risk of serious harm.

*Note:*

- *The directions on redaction below relate particularly to the disclosure of relevant material to the PSAA.*
- Restrictions to the scope of the GDPR apply solely for "*the protection of the data subject or the rights and freedoms of others*". See Restrictions.)

#### 5.5.3.1.2. Redaction – specific directions

**Redact – this information is always to be redacted.**

- Contact information including address, telephone number and email address; and
- Identifiers except for name, age, non-specific address (e.g. postal district). *(Note see further below: name, age, non-specific address may be retained if the identifier is required as 'relevant material' for fair procedure or child protection, if not required, redact.)*

**Redact - based on an assessed and recorded decision**

- Redact only the value/response in a field and not the field name so that it is clear to the recipient what type of information has been redacted. This enables the recipient to claim that disclosure is necessary and proportionate to a stated purpose (e.g. fair procedure).
- In letters, redact all references to individuals other than professionals carrying out **CASP** or make a decision to disclose based on a GDPR restriction (for "*the protection of the data subject or the rights and freedoms of others*") and record the justification for the decision.
- If the individual is concerned for 'secondary victimisation', this must be taken into account in redaction and should be referenced in the justification for decisions to protect personal data.

- Consider the purpose of disclosing identifying information. It may be necessary to the recipient to identify the individual (e.g. for child protection or fair procedure). If so, consider which identifiers Tusla may use to ensure that the identification is confirmed (e.g. name, date of birth, address). Avoid using more than three identifiers and use less than three if sufficient to the purpose. There should be no other purpose to receiving identifying information other than to identify the person.
- Redact all contact information except for the minimum information that may be required for the recipient to identify the individual. There is no permission for Tusla to provide contact information of one individual to another individual under **CASP** for the purpose of communication.
- Redact the response in the field 'ethnic identity' (if such a field appears in the file). This is collected for statistical purposes to ensure equality and not for the purposes of identification.
- Redact the response in the field 'PPSN' (if such a field appears in the file). This is collected for identification purposes with restricted permissions - a limited number of public bodies, including Tusla, are permitted under social protection legislation to process PPSN. PPSN may not be used as an identifier for general purposes other than under the legislation.
- Redact the response in the field 'proof of identity' as there is a risk of there being an identifier in the response (e.g. passport number) which should not be disclosed to the third-party individual.
- Redact the telephone number. The telephone number should not be used to facilitate a third-party data subject in identifying another data subject because of the potential harm of misuse. If it is necessary to confirm the identity to the third-party data subject with reference to the telephone number, the third party may give a phone number which Tusla may confirm or four digits of the phone number may be provided.
- Consider redacting the address partially or in whole. The address may provide one of three identifiers (name, date of birth, address) to confirm the identify to the third-party data subject but the risk of harm to the data subject may outweigh the necessity to provide the address as identifying information. If it is necessary to confirm the identity to the third-party data subject with reference to the address, the third party may give an address which Tusla may confirm or the local electoral area may be provided (or a partial address that is not sufficient for a third party to locate the data subject).
- Redact the email address when disclosing a form to a third-party data subject. The email address should not be used to facilitate a third-party data subject in identifying another data subject because of the potential harm of misuse. If it is necessary to confirm the identity to the third party data subject with reference to the email address, the third party may give an email address which Tusla may confirm or the first letter, number of characters and domain name of the email address.
- Consider redacting 'profession' if harm to the data subject may outweigh the necessity of disclosing the information.
- Redact the date of birth if it is not necessary to the recipient to identify the individual.
- Redact the identifying information and personal information of any individuals who are cited in the detailed information responses or other fields but are not primary data subjects in the record and/or are not aware of the **CASP** case or make a decision to disclose based on a GDPR restriction (for "*the protection of the data subject or the rights and freedoms of others*") and record the justification for the decision.

- The identifying information of Tusla employees who are involved in carrying out **CASP** or related procedures should remain on the record.
- The identifying information of professionals who are involved in carrying out **CASP** or related procedures should remain on the record except, in unlikely and exceptional circumstances, if the social worker makes a decision to redact based on data protection and records the justification for the decision.
- Redact the personal data of any individual, including the primary data subject of the record, in the detailed information responses in keeping with **CASP Data Protection Guidance** and record the justification for the decision.
- Redact Special Categories of Data in the detailed information responses (i.e. 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) or make a decision to disclose based on a GDPR restriction (for "*the protection of the data subject or the rights and freedoms of others*") and record the justification for the decision.
- Redact the form of abuse unless there is a purpose for disclosing this sensitive information. (The form of abuse is relevant material which shall be necessary to disclose to the PSAA.) Note that 'sexual abuse' is special category data. If making a decision to disclose based on a GDPR restriction (for "*the protection of the data subject or the rights and freedoms of others*"), record the justification for the decision.
- Redact personal data relating to alleged or prosecuted criminal offences or make a decision to disclose based on a GDPR restriction (for "*the protection of the data subject or the rights and freedoms of others*") and record the justification for the decision.
- Redact Pulse or other An Garda Síochána reference ID as this is criminal data and IDs which only An Garda Síochána may process. Make a decision to disclose **to An Garda Síochána only** based on a GDPR restriction (for "*the protection of the data subject or the rights and freedoms of others*") and record the justification for the decision. Pulse or other An Garda Síochána reference ID must never be disclosed to any party except An Garda Síochána.
- Redact all information about an impact on a person of an action or make a decision to disclose based on a GDPR restriction (for "*the protection of the data subject or the rights and freedoms of others*") and record the justification for the decision.
- Redact all information about personal supports, substance abuse, mental health, physical health, disability, literacy as these are 'data concerning health' and thereby special categories of data or make a decision to disclose based on a GDPR restriction (for "*the protection of the data subject or the rights and freedoms of others*") and record the justification for the decision.
- Redact all information about previous complaints or history with Tusla or involvement with other services as this is sensitive, social work data (possibly including Special Categories of Data), or make a decision to disclose based on a GDPR restriction (for "*the protection of the data subject or the rights and freedoms of others*") and record the justification for the decision.
- Redact all information about 'cultural or religious considerations' as these are special categories of data or make a decision to disclose based on a GDPR restriction (for "*the protection of the data subject or the rights and freedoms of others*") and record the justification for the decision.

#### 5.5.3.1.3. Who can I contact if I have a query about redaction in CASP?

Consult the guidance on the relevant standard form or template, **CASP Data Protection Guidance,** **Disclosing data safely** or Tusla's **Redaction Policy**. If you do not understand how to proceed, contact the area Privacy Officer or the Data Protection Unit. If you have a query about who should carry out redaction or how to manage substantial redaction, consult the **Redaction Policy** sections 6.3 Who Should Carry Out Redaction and 6.4 How to Manage Substantial Redaction.

## 5.6. Ensuring data protection compliance at each stage of the process

### 5.6.1. Required data protection actions when carrying out CASP

- Inform a data subject about the data processing and their rights by providing a **Privacy Notice** (see CASP Privacy Notice(s)) to them, explaining to them otherwise the purpose and nature of the processing, and being prepared to answer their questions on the data processing and their rights as data subjects.
- Note that the **Privacy Notice** covers all the elements of information required under Articles 13-14 and it presents the information in a manner compliant with Article 12. A verbal explanation will further enhance the transparency on the data processing.
- If you are collecting Personal Data directly from the data subject, you must inform the data subject about the data processing and their rights when (or before) you are collecting their data.
- If you are collecting Personal Data from a source other than the data subject (e.g. when you collect information relating to a PSAA from the Complainant), you must inform the data subject about the processing and their rights within a reasonable period and no later than one month from first collecting the data.
- If you seek consent / assent from the data subject (or their parental guardian) to collect data from a third party or otherwise process data, you must provide a form that fulfils the conditions for consent / assent. If you are seeking consent as a safeguard the form must clarify that consent is a 'safeguard' and not the legal basis. If you are seeking consent from parental guardian on a child's behalf, the child should assent. Both the data subject and the parental guardian, if applicable, must receive a **Privacy Notice** at the time of reviewing the consent form. (See The status of consent from the data subject; seeking agreement from a data subject for detail.)
- At every interaction with the data subject, make the **Privacy Notice** available and remind the data subject of their rights:
    - Attach the **Privacy Notice** to every correspondence by letter or email.
    - Provide a **Privacy Notice** leaflet when meeting with the data subject face to face.
    - Make the general **Privacy Notice** available at Tusla contact points.
- Refer to the **Privacy Notice**, **CASP Data Protection Guidance** and **CASP** and **CASP Guidance** documents to support you in verbally providing the data subject with information about the data processing and their rights.
- If a data subject requests access to information held about them, an amendment to a record or other request which indicates the assertion of data subject rights, carry out the request consistent with **CASP** practices but also ensure that the requirements in fulfilling a data subject request are being met.

- Acknowledge the request promptly.
- Remind the data subject of their rights by providing a **Privacy Notice** to them.
- Fulfil the request promptly keeping the data subject informed of progress.
- Fulfil a data subject access without delay and no later than within 30 days. Seek assistance from the Data Protection Unit if fulfilling the request is complex and substantial.

- When you request or source Personal Data, make sure to only collect the Personal Data that is necessary and proportionate to the purpose.
- When you disclose Personal Data, make sure to only disclose the Personal Data that is necessary and proportionate to the purpose.
- Use the standard forms and templates in **CASP Guidance** to ensure that you are minimising the data collected and the data disclosed.
- Note the purpose of each form or template and keep it in mind when inputting information as this should determine what is necessary and proportionate.
- Seek the support and advice of the Data Protection Unit where required.

#### *5.6.1.1. Timeframes for data protection actions*

Refer to Section 7. Timeframes for responses by social work area office in **National Child Abuse Substantiation Procedure** to see where data protection actions fit with **CASP** actions.



# Appendix

## 1. Full Glossary of Terms

- **Acknowledgement**: Tusla may provide a limited degree of control to the data subject by requiring that the data subject explicitly confirm their acknowledgement that a type of data processing may take place (e.g. a request for information from An Garda Síochána). This acknowledgement should be presented in a form with similar attributes to a consent form but clarifying to the data subject that the data processing does not depend on the data subject's consent. The data subject may assert their right to object to the data processing and the onus is on Tusla to justify the data processing and to restrict processing until that justification has been provided.
- **Agreement from a Data Subject**: There are three forms of agreement to data processing from a data subject in **CASP**, **Acknowledgement**, **Assent** and **Consent as a Safeguard** (consent as a legal basis for processing does not apply in **CASP**). These varying forms of agreement differ in the degree of control which the data subject has over the processing. The social worker should be conscious of, and record appropriately, which form of agreement applies each time the social worker seeks agreement from a data subject. The form of agreement should be clear and transparent to the data subject with a full justification from Tusla as to the choice of agreement type.
- **Assent:** Tusla may provide a limited degree of control to the data subject (more than acknowledgement but less than consent) by requiring that the data subject agree that certain data processing takes place but in the context where the social worker explains that if the data subject does not assent, then their refusal to assent shall have a substantial impact on the substantiation investigation. This 'assent' applies particularly where Tusla relies on the data subject for the data to be collected (either directly from the data subject or from a person or organisation whose contact

details the data subject provides, e.g. a clinical practitioner). It is difficult to fulfil the condition of 'freely given' in this case to a degree in which the data subject's agreement may be considered 'consent'. This 'assent' should be presented in an 'assent form' with similar attributes to a consent form but clarifying to the data subject that the refusal to assent shall have a substantial impact on the substantiation investigation. The data subject may assert their right to object to the data processing and the onus is on Tusla to justify the data processing but the data processing may not take place without the 'assent'.

- **Assent by a Child or Vulnerable Person**: Consent does not apply to a child because they may not be sufficiently mature to assess the risks to their personal data and thereby independently protect their rights and freedoms as data subjects. It is likely that 'assent' must apply in place of consent for a vulnerable person in the context of **CASP** given the high risks to data subjects.
- **Consent**: *'consent' of the data subject means 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;* (GDPR, Article 4). See also GDPR Article 7, 'Conditions for Consent'; further references to consent in Articles 6, 8, 9 and Recitals 32, 42, 43; and Guidelines 05/2020 on consent under Regulation 2016/679.
- **Consent as a Safeguard**: The GDPR does not consider that consent may be used as a legal basis for data processing *where there is a clear imbalance between the data subject and the controller, in particular **where the controller is a public authority, and it is therefore unlikely that consent was freely given** in all the circumstances of that specific situation (Recital 43, GDPR).* On the other hand, a data subject may consent to a service which requires the data processing or they may consent to data processing which has a legal basis other than consent (i.e. Tusla standard legal basis). In these cases, consent is applied as a '**Safeguard**', a measure to afford the data subject some level of control over the processing of their data even though this form of consent does not afford the data subject the same level of control as they would have if consent were applied as the legal basis. Tusla must fulfil the conditions for consent as detailed in the GDPR (Article 7 and supplemented with other references) even where applying '**Consent as a Safeguard**'. When applying consent as a legal basis or a safeguard, the removal of consent does not affect the lawful basis for processing which has taken place until the consent was removed. There may be aspects of data processing where Tusla should request an **Acknowledgement** or **Assent** from the data subject rather than consent - an acknowledgement should be required where the data processing shall take place with or without consent in any case and assent applies where the data subject understands that by not assenting, there shall be a substantial impact on the substantiation investigation.

The application of consent as a "safeguard" but not a legal basis is detailed in the context of scientific research in paragraph 154 of Guidelines 05/2020 on consent under Regulation 2016/679.

> *154. When consent is the legal basis for conducting research in accordance with the GDPR, this consent for the use of personal data should be distinguished from other **consent requirements that serve as an ethical standard or procedural obligation**. An example of such a procedural obligation, where the processing is based not on consent but on another legal basis, is to be found in the Clinical Trials Regulation**. In the context of data protection law, the latter form of consent could be considered as an additional safeguard**. At the same time, the GDPR does not restrict the application of Article 6 to*

*consent alone, with regard to processing data for research purposes. As long as appropriate safeguards are in place, such as the requirements under Article 89(1), and the processing is fair, lawful, transparent and accords with data minimisation standards and individual rights, other lawful bases such as Article 6(1)(e) or (f) may be available. This also applies to special categories of data pursuant to the derogation of Article 9(2)(j).*

- **Cross-Border Processing:** *'cross-border processing' means either:*
  - *processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or*
  - *processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.* (GDPR, Article 4)
- **Data Controller Obligations**: Tusla is the lead Data Controller in the Data Processing Activity, **CASP**. A Data Controller has certain responsibilities and obligations which are laid out in the GDPR (Article 24-43 and referring back to Articles 5-23) and further specified in Data Protection Act 2018. These may be summarised as the obligations to safeguard the Personal Data with 'technical and organisational measures'; ensure and demonstrate that the data processing is necessary and proportionate to the purpose; that the purpose is fair, lawful and specified; that the principles of data protection are fulfilled and that the rights and freedoms of data subjects are upheld; and that data protection compliance is met when data is shared with or transferred to another Data Controller or the Data Controller has commissioned a Data Processor to process Personal Data on the Data Controller's behalf.
- **Data Controller (Controller)**: *'controller' means the natural or legal 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 Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;* (GDPR, Article 4)
- **Data Processing (Processing, Process)**: *'processing' means any operation or set of operations which is 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;* (GDPR, Article 4)
- **Data Processor**: *'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;* (GDPR, Article 4)
- **Data Protection Legislation:** the Data Protection Act 2018 (the "**2018 Act**"), Data Protection Acts 1988 and 2003 (to the extent applicable), General Data Protection Regulation (EU) 2016/679 ("**GDPR"**), Directive (EU) 2016/680, Directive 2002/58/EC (as amended), European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (SI 336 of 2011) and any other laws and regulations relating to the processing of personal data and privacy which apply to a party and, if applicable, the guidance and codes of practice issued by the relevant supervisory authority as well as any other rules, procedures, standards and guidelines which applies to either party under law.

- **Data Protection Principles (GDPR Principles)**: Data Principles are listed and explained in Article 5 of the GDPR. They are Lawfulness, Fairness and Transparency; Purpose Limitation; Data Minimisation; Accuracy; Storage Limitation; and Integrity and Confidentiality. There is a seventh over-arching principle of Accountability to the six principles.
- **Data Protection Risk**: A data protection risk is a risk of harm to the data subject or a risk of non-compliance with data protection legislation.
- **Data Protection Risk Control** (**Data protection control**): A Data Protection Risk Control is a measure to mitigate a risk to data protection.
- **Data Sharing**: Data may be shared between two or more Data Controllers who are responsible to determine the purposes and means of processing. There must be a legal basis for this data sharing, a
    - Data sharing between public bodies is inherent in the multi-agency approach to child protection.
    - Tusla may share data with organisations involved in the care of children who are subject to Children First Act 2015 (schools, voluntary organisations, etc.) and with regulatory councils of these organisations (collectively, these are referred to as Relevant Third Parties in **CASP**).
- **Data Subject Rights**:
    - *The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her. (GDPR, Recital 1)*
    - *The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons. (GDPR, Recital 2)*
    - The GDPR defines particular data subject rights and how they should be managed:
        - The Right to Fair and Transparent Processing
        - The Right to Information about the Processing
        - The Right of Access
        - The Right to Rectification
        - The Right to Erasure (the 'Right to be Forgotten')
        - The Right to Restriction of Processing
        - The Right to Data Portability
        - The Right to Object to Processing
        - The Right not to be Subject to Automated Decision-making Including Profiling
        - The Right to Lodge a Complaint with a Supervisory Authority
- **Data Subject Rights in Balance with Other Fundamental Rights:** The GDPR recognises that the right to data protection is not an absolute right and may need to be balanced with other fundamental rights. This applies as a condition for GDPR restrictions under Artice 23, i.e. "*the protection of the data subject or the rights and freedoms of others*". This is pertinent in **CASP**

when balancing the data protection rights of one person with the rights to fair procedures of another person

- In providing the PSAA with all relevant data assembled in the investigation Tusla will have due regard to the privacy interests of the complainant or any other person affected by the disclosure. However, relevant material can be disclosed to the PSAA notwithstanding confidentiality and privacy where there is a valid public interest to do so. Children First National Guidance for the Protection and Welfare of Children, 2017 page 47 states that "The child's welfare is the paramount consideration and, in a situation where a child is deemed to be at immediate and serious risk, Tusla will take all necessary steps to ensure the child's immediate safety." This is consistent with "*the protection of the data subject or the rights and freedoms of others*".

  Relevant information assembled during the substantiation investigation can only be withheld from the PSAA where there is a clear and continuing risk of harm to identifiable persons as a result of disclosure. Given the nature of issues involved, such a withholding could only be justified in the most extreme of cases and where the information is withheld to the least extent possible. All other possible options in respect to disclosure, such as anonymisation or independent drafted summaries of the evidence provided, would have to be considered before an ultimate decision to withhold could be justified."

  The standard test of relevance will be strictly applied, that is to say if it is reasonably possible that something is relevant to the substantiation investigation and there is no other obstacle to disclosure, the balance is in favour of disclosure.

  Note:

  > *The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.* (GDPR, Recital 4)

- **Data Subject**: *an identified or identifiable natural person ('data subject'); an identifiable natural 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*; (GDPR, Article 4)
- **Data Subject Request**: means a request by a Data Subject for the exercise of the rights laid down in Chapter III of the GDPR.

- **Data Transfer**: Tusla may transfer data to a joint Data Controller, another Data Controller, a Data Processor, or an individual involved with a case.
- **Filing System**: 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis; (GDPR, Article 4)
- **Further Processing**: Further processing is processing which is not the primary purpose for which the data was collected. It is allowable where the further processing is compatible with the purposes for which the personal data were initially collected and therefore the legal basis shall also be applicable to the further processing. The social work team shall carry out further processing to fulfil associated Child Protection and Welfare duties of Tusla Operations. For example, data may be processed to carry out a substantiation investigation but it may be further processed to carry out a review of the investigation. Data collected for the substantiation investigation may be processed for Child Protection and Welfare services, for the purposes of Safeguarding or for notifying the National Vetting Bureau of a 'bona fide concern'. This further processing is known and each data processing activity has its own, related legal basis consistent with the legislative framework for **CASP**. Additionally, the data may be processed for statistical purposes, which is deemed compatible processing. The data shall be retained in archive in the public interest and under the provisions of the Child Care Act 1991. This archiving shall be compatible with the data processing. All further processing compatible with the processing should be described in the **Privacy Notice**. The data controller should assess that the further processing would be consistent with the reasonable expectations of the data subject. Further processing relating to the legitimate interest of a data controller to indicate possible criminal acts or threats to public security should be prohibited *if the processing is not compatible with a legal, professional or other binding obligation of secrecy*. (See Recital 50, GDPR.)
- **Personal Data**: *'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural 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;* (GDPR, Article 4)
- **Personal Data Breach**: *'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;* (GDPR, Article 4)
- **Disclosure**: The Data Controller may disclose Personal Data to another Data Controller, a Data Processor or to an individual as required by **CASP**. Tusla should choose the most secure manner to disclose the Personal Data in a manner that mitigates the risk of a breach or of misuse by an authorised recipient.
- **Information Security**: *preservation of confidentiality, integrity and availability of information* (ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary)
- **Information Security Event**: *identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that can be security relevant.* (ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary)

- **Information Security Incident**: *single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.* (ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary)
- **Information Security Risk Control** (**Information security control**): *measure that is modifying risk*
    - *Note 1 to entry: Controls include any process, policy, device, practice, or other actions which modify risk.*
    - *Note 2 to entry: It is possible that controls not always exert the intended or assumed modifying effect.* (ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary)
- **The Legal Basis** (**The Legal Basis for Processing**): The Legal Basis for Processing at Tusla is where the Data Controller
    - Fulfils a legal basis under Article 6 of the GDPR (in Tusla's Operations, this is "processing 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;");
    - Fulfils conditions for processing special categories of data under Article 9 of the GDPR if such processing is taking place (in Tusla's Operations, this is primarily "processing is 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 the conditions and safeguards referred to in paragraph 3;" or "*processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject*;".
    - Fulfils the conditions for where restrictions to the scope of the obligations and rights provided for in Articles 5 (Principles), 12-22 (Rights of the Data Subject) may be necessary under Article 23 in order to safeguard certain interests where such restriction "respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society" (in Tusla's Operations, this may be "*a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority* …" and in the event of competing interests in the fulfilment of data subject's rights, "*the protection of the data subject or the rights and freedoms of others*".
    - Fulfils the legal basis as defined further in Data Protection Act 2018 (in Tusla's Operations, as applies particularly to regulatory bodies and the management of "health and social care services")
    - Justifies the legal basis under Data Protection Laws in reference to national and international laws
    - Has identified that a legislative measure (statutory or case law) which provides for a restriction to the scope of the obligations and rights has provided provisions as to how the data shall be processed, how data subject rights shall be managed and how restrictions apply (as detailed in GDPR Article 23, 2.)

- In the absence of sufficient provisions in the legislation to specify the data processing and restrictions, fulfil this aspect of the legal basis through official policy documents and protocols, data protection agreements, and propose updates to the legislation.
- Has identified the legal basis and has recorded this in the Register of Data Processing Activities and the **Privacy Notice**(s) that may apply to the data processing.

- **Data Transfers to a Third Country**: A Data Transfer to a Third Country applies if Tusla sends Personal Data outside of the jurisdictions where the GDPR applies (i.e. outside the European Union or European Economic Community) and is of particular concern if the data transfer is to a country which has not been assessed as 'adequate', in the sense that its data protection legislation meets the standards of the GDPR. The countries of note to which this applies are the United Kingdom and Northern Ireland, and the United States. There are certain safeguards from which Tusla may select to ensure that the data shall be processed in accordance with the GDPR, Standard Contract Clauses, in particular. A Data Transfer Agreement must be put in place where the transfer is to a Data Processor, a Joint Data Controller, or to agree the terms of transfer from Data Controller to Data Controller. If Tusla is sending the Personal Data of a Data Subject to the Data Subject whose address is in a Third Country, this is not subject to the requirements of Data Transfers to a Third Country but safeguards in respect of secure transfer should apply to safeguard the data. For data transfers to public bodies, see Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies.
- **Necessary and Proportionate Processing (Necessary and proportionate to the purpose of the processing)**: All data processing must be necessary and proportionate to the stated purpose of the data processing even where restrictions apply to the scope of the obligations of the data controller. Necessary and proportionate encompass the principles of Purpose Specification and Data Minimisation. Restrictions to the scope of the obligations of the data controller and processing that is based on reasons of substantial public interest restriction must respect *the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society (GDPR, Article 23).* These terms, 'necessary' and 'proportionate' appear several times in the GDPR as does 'appropriate safeguards'.
- **Privacy Notice** (**Data Privacy Notice**): A **Privacy Notice** fulfils the requirements for information about how a data subject's data is processed and the rights of a data subject. It should also fulfil the requirements for how the data controller communicates this information to the data subject in a manner that they can access and clearly understand. (See GDPR Articles 12-14 on the Rights to Information about the Processing.)
- **Profiling**: *'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;* (GDPR, Article 4)
- **Pseudonymisation**: *'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;* (GDPR, Article 4)

- **Recipient**: *'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing*; (GDPR, Article 4)
- **Restrictions to GDPR** (**Restrictions to the Scope of Data Controller Obligations and Data Subject Rights**): Under certain circumstances, the scope of the obligations of the data controller and the scope of data subject rights may be restricted. This is laid out in Article 23 and further detailed in Data Protection Act 2018 and in several GDPR articles relating to derogations. These Restrictions apply to an extent for the data processing under **CASP**.

  Restrictions to the scope of the obligations and rights provided for in Articles 5 (Principles), 12-22 (Rights of the Data Subject) may be necessary under Article 23 in order to safeguard certain interests where such restriction "respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society" (in Tusla's Operations, this applies solely for the "*the protection of the data subject or the rights and freedoms of others*" (GDPR, Article 23, (1)(i)) in the event of competing interests in the fulfilment of data subject's rights.

- **Restriction of Processing**: *'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;* (GDPR, Article 4)
- **Risk of Harm to a Data Subject**: A data subject may experience harm from non-compliance with data protection legislation or from a data breach. The harm from a data breach may be physical, material or non-material damage such as "*loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned". (GDPR, Recital 85)*. The harm from non-compliance with data protection may include a lack of knowledge about the data processing or their data subject rights, and thereby, consequent inability to assert their rights which may have an adverse impact on them similar to that caused by a data breach. The risk categories are as follows:
  - 03 A data subject may experience harm. GDPR Recital 85 provides examples of harm to a data subject.
  - 03.01 A data subject may lose control over their personal data (GDPR Recital 85).
  - 03.02 A data subject may experience limitation of their rights (GDPR Recital 85).
  - 03.03 A data subject may experience discrimination (GDPR Recital 85).
  - 03.04 A data subject's identity may be stolen or the data subject may be a victim of fraud (GDPR Recital 85).
  - 03.05 A data subject may experience financial loss (GDPR Recital 85).
  - 03.06 A data subject may experience harm if there is unauthorized reversal of pseudo-anonymization of their data, e.g. the harm of loss of confidentiality (GDPR Recital 85).
  - 03.07 A data subject may experience harm to their reputation (GDPR Recital 85).
  - 03.08 A data subject may experience loss of confidentiality of their personal data which has been protected by professional secrecy (GDPR Recital 85).

- 03.09 A data subject may experience a significant economic or social disadvantage (GDPR Recital 85).

- **Risk of non-compliance with data protection legislation**: If a risk to compliance with data protection legislation materialises, an adverse impact on data subjects is likely as detailed under **Risk of Harm to a Data Subject**. The risk of non-compliance with legislation may be categorised as follows:
  - 05 There is a risk of non-compliance with Standards/Regulations/Legislation, specifically data protection legislation and associated standards, regulations, policies and procedures.
  - 05.01 The organisation may not be compliant with GDPR Principles (Articles 5-11).
  - 05.02 The organisation may not be compliant with GDPR Rights of the Data Subject (Articles 12-23)
  - 05.03 The organisation may not be compliant with GDPR - Controller and Processor (Articles 24-43).
  - 05.04 The organisation may not be compliant with GDPR - Transfers of personal data to third countries or international organisations (Articles 45-50).
  - 05.05 The organisation may not be compliant with GDPR - Provisions relating to specific processing situations (Articles 85-91) National law may apply - check other risk categories
  - 05.06 The organisation may not be compliant with GDPR Recitals and other articles not categorised in 05.01-05.05.
  - 05.07 The organisation may not be compliant with Data Protection Act 2018 (as amended).
  - 05.08 The organisation may not be compliant with Data Sharing and Governance Act 2019 (as amended).
  - 05.09 The organisation may not be compliant with S.I. No. 347/2019 - European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) (Amendment) Regulations 2019.
  - 05.10 The organisation may not be compliant with GDPR generally if the data processing is not necessary, proportionate with sufficient safeguards to protect the data (general category - broad application through the articles).
  - 05.11 The organisation may be non-compliant with the decisions, instructions or other regulatory communication of the Data Protection Commission issued to the organisation.
  - 05.12 The organisation may be non-compliant with DPC decisions, official guidelines or other regulatory communication issued to data controllers in this sector or generally.
  - 05.13 The organisation may be non-compliant with the decisions, official guidelines or other regulatory communication issued by the European Data Protection Board (EDPB) or its predecessor (Article 29 Working Party).
  - 05.14 The organisation may be non-compliant with data protection legislation indicated by concerns which may be raised from the circumstances of a fine issued to a data controller in any member state of the European Union (for example, a fine to a hospital in Portugal regarding access control raised concerns for hospitals across the EU).
- **Safeguards**: Safeguards (which are synonymous with risk controls) are any measures which the Data Controller puts in place to ensure that the Personal Data is protected against a Personal Data Breach; against a breach of the confidentiality, integrity and availability of data; that the data subjects rights and freedoms are upheld.
- **Secrecy (Obligations of Secrecy)**: *Member States may adopt specific rules to set out the powers of the supervisory authorities laid down in points (e) and (f) of Article 58(1) in relation to controllers or*

*processors that are subject, under Union or Member State law or rules established by national competent bodies, to an obligation of professional secrecy or other equivalent obligations of secrecy where this is necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy. Those rules shall apply only with regard to personal data which the controller or processor has received as a result of or has obtained in an activity covered by that obligation of secrecy.*

- **Sensitive Personal Data**: Sensitive Personal Data includes Special Categories of Data; Social Work records including **CASP** or Child Protection and Welfare records; data relating to criminal offences; Personal Data that a data subject would not normally disclose to another person or would only disclose on the understanding of confidentiality.
- **Sensitive Data in Health and Social Care Sector**:
    - *Special categories of personal data which merit higher protection should be processed for health-related purposes only where necessary to achieve those purposes for the benefit of natural persons and society as a whole, in particular in the context of the management of health or social care services and systems, including processing by the management and central national health authorities of such data for the purpose of quality control, management information and the general national and local supervision of the health or social care system, and ensuring continuity of health or social care and cross-border healthcare or health security, monitoring and alert purposes, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, based on Union or Member State law which has to meet an objective of public interest, as well as for studies conducted in the public interest in the area of public health.* ***Therefore, this Regulation should provide for harmonised conditions for the processing of special categories of personal data concerning health, in respect of specific needs, in particular where the processing of such data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy****. Union or Member State law should provide for specific and suitable measures so as to protect the fundamental rights and the personal data of natural persons. Member States should be allowed to maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health. However, this should not hamper the free flow of personal data within the Union when those conditions apply to cross-border processing of such data.* (Recital 53, GDPR)
- **Special Categories of Personal Data**: Special categories of data are: *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*. (GDPR, Article 9) The Data Controller must ensure that it fulfils the conditions for processing this Personal Data and does not process it in a manner that is not fair and lawful. These special categories of data may be susceptible to misuse where the data is processed unlawfully to discriminate against a person.
- **Supervisory Authority**: For the purposes of processing Personal Data in Ireland, the Supervisory Authority is the Data Protection Commission of Ireland.

- **Third Party**: *'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;* (GDPR, Article 4)
- **Threat to a Data Subject**: If there are vulnerabilities in the manner in which data is processed, this may expose the Personal Data of the Data Subject to threats which may be an actor or an event. (For example, if there is no risk control in place to check the veracity of an address, human error (vulnerability) may cause a letter to be sent to the wrong address which in turn may be opened by an unintended recipient (threat agent), which would cause a data breach (adverse impact on compliance) and possible harm to a data subject (adverse impact on the data subject, at a minimum, loss of confidentiality).
- **Threat relating to an information asset**: *potential cause of an unwanted incident, which can result in harm to a system or organization* (ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary)
- **Transparency of data processing**: The Principle of Transparency (Lawfulness, Fairness and Transparency) is detailed further under the rights of the data subject to transparent information in order to assert their rights as data subjects. Tusla must inform the data subject about the purpose and nature of the processing and about the data subjects' rights and do so in a manner that is "*concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child*". (GDPR, Article 12). Tusla shall achieve deliver this transparency by providing **Privacy Notice**s to the data subjects in a timely manner (and compliant with timelines required in Articles 13 and 14 of GDPR); by explaining the purpose and nature of the processing to the data subject using standard correspondence templates; and by being prepared to verbally provide information about the processing and data subject rights when this is required by the data subject.
- **Upholding the rights and freedoms of data subjects**: Tusla shall uphold the rights and freedoms of the data subjects through data protection compliance; keeping data subjects informed of their rights so that they may assert them if they so wish; and defining procedures for informing data subjects of their rights and for managing and recording data subject requests.
- **Vulnerability of a data subject**: The GDPR requires an additional layer of protection for data subjects who may be vulnerable and makes specific provisions for children as vulnerable data subjects.
    - Firstly, a data subject may be vulnerable based on their capacity to understand the data processing and assess risks to themselves, for example, a child ("*Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned with their rights in relation to the processing of personal data*." Recital 38, GDPR)
    - Secondly, a data subject may be vulnerable due a power imbalance between the data controller and the data subject (as applies to a citizen in relation to a public body, an employee in relation to an employer, and a regulated person in relation to a regulator).
    - Thirdly, a data subject may be vulnerable if the data processing has the potential to have a significant impact on the data subject, such as where data is processed in order to carry out an assessment which concludes with a decision made about a data subject which has a significant impact on their lives; where the data processing has the potential to cause significant upset or even trauma to the data subject; or where errors, non-compliance or a

data breach may cause a significant harm to the data subject due to the sensitive nature of the data or the sensitive context for the data processing.

- **Vulnerability of an information asset**: *weakness of an asset or control that can be exploited by one or more threats* (ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary)
- **White List**: A White List is an authorised list which may apply in **CASP** to a White List of Authorised Sources for Contact Tracing where Tusla needs to contact a person to inform them that they are a Person Subject to Abuse Allegations. (See Tusla ICT site at Tusla Hub and Tusla ICT policies for acceptable information sources and applications). A White List shall also apply in Tusla to authorised applications for communication (for example, Microsoft Teams is authorised for videoconferencing).

## 2. CASP Privacy Notice(s)

The Child Abuse Substantiation Procedure and Guidance provides **Privacy Notice**s for the child complainant, the adult complainant, and the PSAA.

## 3. Data Protection Reference Information

- General Data Protection Regulation (EU) 2016/679 (known as GDPR): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679
- Data Protection Act 2018: http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html
- European Data Protection Board: https://edpb.europa.eu/edpb_en
- Guidelines 05/2020 on consent under Regulation 2016/679: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en
- Guidelines 07/2020 on the concepts of controller and processor in the GDPR: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en
- Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b_nl
- Guidelines 4/2019 on Article 25 Data Protection by Design and by Default: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en
- Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679: https://edpb.europa.eu/our-work-tools/our-documents/directrices/guidelines-22018-derogations-article-49-under-regulation_en
- Guidelines on Transparency under Regulation 2016/679 (wp260rev.01): https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227
- Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01): https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053