TUSLA PRIVACY POLICY

Document Reference Number	
Revision Number	**1.5**
Approval Date	**18 May 2018**
Next Revision Date	**25 May 2019**
Document Developed By	**Data Protection Officer**
Document Approved By	**CEO and the Tusla Board**
Responsibility for Implementation	**All Staff**
Responsibility for Review and Audit	**Data Protection Officer**

Table of Contents

Introduction

The Child and Family Agency (Tusla) is the dedicated State agency responsible for improving wellbeing and outcomes for children. The Agency operates under the Child and Family Agency Act 2013, a progressive piece of legislation with children at its heart and families viewed as the foundation of a strong healthy community where children can flourish. Partnership and co-operation in the delivery of seamless services to children and families are also central to the Act. Tusla is committed to protecting the rights and privacy of individuals in accordance with European Union and Irish Data Protection Legislation and the other Acts to which Tusla is obliged to adhere.

Tusla needs to lawfully and fairly process personal data about employees, children, service users, suppliers and other individuals in order to achieve its mission and functions. Your personal data may be exchanged with other Government Departments and Agencies in certain circumstances where this is provided for by law. Your personal data will be processed in compliance with all relevant Data Protection Legislation and the other Acts to which Tusla is obliged to adhere.

The Data Protection Legislation confers rights on individuals as well as responsibilities on those persons processing personal data. This policy sets out how Tusla seeks to process personal data and ensure that staff and data processors of Tusla understand the rules governing their use of personal data to which they have access in the course of their work.

The EU General Data Protection Regulation (GDPR EU 2016/679) replaces the Data Protection Directive 95/46/EC and was designed to harmonise data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organizations across the region approach data privacy. The GDPR will be enforced from 25th May 2018 and this policy reflects the requirements of the GDPR and its Irish Statutory implementation, henceforth known as the 'Acts' along with any other legal requirements in the area of data protection.

The policy will be reviewed at minimum annually by the Data Protection Officer (DPO) to ensure alignment to appropriate risk management requirements and its continued relevance to current and planned operations, or legal developments and legislative obligations.

Further comments or questions on the content of this policy must be directed to the DPO. Any material changes to this policy will require approval by the Tusla Board or a delegate of the Board.

Purpose and Scope

This policy applies to all staff, contractors and third parties working with personal data under the control of Tusla. You must be familiar with this policy and comply with its terms.

This policy also applies to all of Tusla's personal data processing functions in relation to identified or identifiable natural persons, including those performed on customers', clients', employees', suppliers' and any other personal data Tusla processes from any source.

We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be communicated to staff.

Legislation and Other Related Policies, Standards and Guidelines

The below policies and standards are to be read and applied in conjunction with this policy

Title	Description
Charter of the Data Protection Officer	The Charter sets out the role, responsibilities, reporting lines, authority and independence of the Data Protection Officer
Data Subjects Records Request Standard	This standard sets out the regulatory obligations of Tusla in relation to records requests and the process within Tusla for same
Data Breach Standard **(TBD)***	This standard sets out the regulatory obligations of Tusla in relation to personal data breaches and the process within Tusla for same
Data Privacy Impact Assessment Standard **(TBD)***	This standard sets out the regulatory obligations of Tusla in relation to Data Privacy Impact Assessments and the process within Tusla for same
Record of Processing Activities Standard **(TBD)***	This standard sets out the regulatory obligations of Tusla in relation to documenting our Record of Processing Activities and the process within Tusla for same
Data Audit Standard **(TBD)***	This standard sets out the regulatory obligations of Tusla in relation to the performance of personal data audits and the process within Tusla for same
Data Processor Standard **(TBD)***	This standard sets out the regulatory obligations of Tusla in relation to the engagement of Data Processors and the process within Tusla for same
Data Sharing Standard **(TBD)***	This standard sets out Tusla requirements for data sharing with other organisations who would be deemed as Joint Data Controllers and the process within Tusla for same.
Privacy Notices Standard **(TBD)***	This standard sets out the regulatory obligations of Tusla in relation to transparency to data subjects of our processing and the achievement of same via privacy notices.
Data Security Standard **(TBD)***	This standard set outs the regulatory obligations of Tusla in relation to maintaining adequate organisational and technical security measures over the personal data we hold and the process within Tusla for same.

Title	Description
Information Classification and Handling Policy	This policy sets out the requirements for data classification within Tusla and the handling requirements for each classification of data
CCTV Policy	The CCTV policy sets out the regulatory obligations of Tusla in relation to the usage of CCTV and the process within Tusla for same
Clear Desk Policy	The clear desk policy sets out the requirements for Tusla staff to ensure that all data classified as confidential or highly confidential is securely stored at all times.
Acceptable Usage Policy **(TBU)****	This policy sets out the standards for usage of Tusla assets in an acceptable and secure manner
End User Information Security Policy **(TBD)***	The purpose of this document is to establish minimum standards and guidelines to protect against accidental or intentional damage or loss of data, interruption of Tusla services, or the compromise of sensitive information.
Removable Media Policy **(TBD)***	The purpose of this policy is to minimise the risk of loss or exposure of sensitive information maintained by Tusla and to reduce the risk of acquiring malware infections on removable media operated by Tusla
Physical Security Policy	This Physical Security Policy applies to all organisational information including and the physical protection of same
Consent Policy – A guide for patients and service users ****(TBU)**	This policy sets out the importance of obtaining consent from all service users where it is feasible to do so and the process for obtaining and documenting that consent
Consent Policy – A Guide for Young People ****(TBU)**	This policy sets out the importance of obtaining consent from all service users where it is feasible to do so and the process for obtaining and documenting that consent
Access Control Policy ****(TBU)**	The purpose of this policy is to define the access control protocols applied in the organisation
Administrative Access Policy – A Practical Guide for Staff *****(TBR)**	This staff guide is designed to explain the main provisions of Data Protection and Freedom of Information legislation

*TBD = To be Developed; **TBU = To be Updated as HSE Policy

Title	Description
Electronic Communications Policy **(TBU)	To provide clear guidance on the appropriate, safe and legal way in which to use the electronic communications, email and internet services.
Encryption Policy **(TBU)	The purpose of this policy is to define the acceptable use and management of encryption software and hardware
Information Technology Security Policy **(TBU)	The purpose of this Policy is to define the security controls necessary to safeguard and ensure the security, confidentiality, availability and integrity of the information held therein.
Mobile Phone Device Policy **(TBU)	To define the acceptable use and management of HSE mobile phone devices.
Password Standards Policy **(TBU)	To provide clear guidance and present best practice for the creation of strong passwords, the management and protection of those passwords, and the frequency of change.
Remote Access Policy **(TBU)	To define a standard for the remote connection to the organisations network.
Social and Digital Media Policy **(TBU)	The Social and Digital Media Policy and Guidance document, dated April 2012, provides guidance and direction to staff when utilising all types of online social media sites and networks. Misuse or abuse of social and digital media can cause significant injury to third parties and can also impact negatively on the credibility of the organisation.
Employee Handbook **(TBU)	This handbook sets out the terms and conditions of employment of staff of the organisation
Garda Vetting and Assessment of Existing Employees	This procedure sets out the process for Garda Vetting and the Risk Assessment of existing employees
Tusla Incident Management Policy and Procedure	It is the policy of the Agency that all incidents are identified, reported, communicated and investigated, where appropriate, through a robust incident management process.

*TBD = To be Developed; **TBU = To be Updated as HSE Policy; TBR – to be retired for that data protection element.

Glossary of Terms and Definitions

TERM	DEFINITION
Personal Data	Personal data is data relating to a living individual, whatever their nationality or place of residence, in a form that can be processed. It includes both electronic and paper based data.
Data Subject	A data subject is a living individual, whatever their nationality or place of residence.
Data Controller	A person who (either alone or with others) controls the contents and use of personal data. A data controller is the individual or the legal person who controls and is responsible for the keeping and use of personal information on computer or in structured manual files.
Data Processor	A person who processes personal data on behalf of a data controller but does not include an employee of a data controller who processes such data in the course of his employment. If an Agency or person holds or processes personal data, but does not exercise responsibility for or control over the personal data, then they are deemed to be a "data processor".
Data Protection Commissioner	The Data Protection Commissioner is responsible for upholding the rights of individuals as set out in the Acts, and enforcing obligations upon Data Controllers
Consent	Consent means any freely given, specific, informed and unambiguous indication of the data subjects wishes by which they, by statement or a clear affirmative action, signify agreement to the processing of their personal data. Consent may also be obtained by Tusla under the other Acts to which it is obliged to adhere and may not be required under these other Acts, to be freely given by the Data Subject.
Transparency	Data Controllers are mandated to be open and clear to data subjects that their data will be processed and the manner and extent of that processing.
Record of Processing Activities	A record of processing activities is a mandated schedule of processing activities carried out by the Data Controller and contains several core elements. Such as the data categories involved in processing, data sharing, retention periods, the purpose of processing etc.

Glossary of Terms and Definitions

TERM	DEFINITION
Privacy Notices	A privacy notices are published on client and employee facing forms, websites and in public areas and provide in clear and understandable language, to data subjects information on the personal data collected and the purposes and extent of the processing of that personal data.
Data Privacy Impact Assessments (DPIA)	A DPIA is a process designed to describe the processing, assess the necessity and proportionality of a processing and to help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data (by assessing them and determining the measures to address them).
Data Audits	Data Audits are independent reviews performed by the Data Protection Office in order to assess compliance with organisational obligations under the acts. These reviews raise actions for remediation, where appropriate to address issues noted during the reviews and are reported to the Board, or a sub-committee thereof as designated by the Board.
Data Portability	The principle of data portability states that the data subject has the right to receive their personal data in a structured or commonly used and machine readable format and has the right to transmit that data to another controller without hindrance. Tusla when considering such a request must also take account of the other Acts to which it is obliged to adhere.
Right to be Forgotten	The data subject has the right to obtain from the data controller the erasure of personal data concerning them, without undue delay under certain conditions. Tusla when considering such a request must also take account of the other Acts to which it is obliged to adhere.
Cross Country Data Transfers	A cross country transfer is the transfer of personal data by the data controller to an Agency in another country for the purposes of processing. These transfers shall only take place if certain strict conditions are met as set out in the Acts
Data Breaches	A 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. This includes breaches arising from both accidental and deliberate causes.

Glossary of Terms and Definitions

TERM	DEFINITION
Data Subject Records Requests	A data subject has the right to request copies of the data held about them, alteration to data held about them and / or the erasure of data held about them subject to certain conditions and the other Acts to which Tusla is obliged to adhere
Data Sharing	Data sharing is the disclosure of information, including personal data, by one public body to one or more public bodies
Secure Storage	Secure storage means that data, whether electronic or paper based, is stored in a manner to prevent theft, loss, leakage and destruction of that data and unauthorised amendments of that data
Data Retention	Data retention means that data is only retained by the data controller as long as consent from the data subject remains, and it is used only for the purposes for which it was collected. Once consent has been removed or the purpose for collection of the personal data no longer remains, then it must be destroyed unless an obligation of another Act to which Tusla is required to adhere mandates the further retention of the data.
Secure Disposal	Secure Disposal means that the personal data (electronic and paper based) is destroyed in such a manner that it cannot be retrieved or recreated post the destruction.
Special Categories of Data	Special Categories of Data, also known as sensitive data, are personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings—any use of sensitive personal data must be strictly controlled in accordance with this policy.

Responsibility for this policy

All staff, contractors and relevant third parties are required to ensure this policy is implemented and adhered too. The accountabilities and responsibilities for implementation of the various aspects of the policy are set out in the RACI table below.

This policy will also be supplemented by standards, as required, and each Service Unit and Support Function of Tusla is required to ensure that operational procedures are adopted to ensure compliance with this policy and associated standards.

Failure to adhere to this policy and its associated standards will be dealt with in the manner outlined in the staff employment handbook, the contractor's agreement or the third party agreement as applicable.

RACI Table

***Data Controller =** All Service Units and Support Functions under the control of Tusla

****Data Subjects =** The owners of the personal data. They are mainly, but not solely, consulted and informed via the DPIA process, privacy notices and this policy. Consultation can also take place through representative bodies or another party formally designated as a representative.

Process	Accountable	Responsible	Consulted	Informed
Policy	Data Controller*	Data Protection Office	Data Controller Legal Department Data Subjects**	Staff, Contractors and Relevant Third Parties Data Subjects**
Collection of Personal Data and the Obtaining and Maintaining of Consent (freely given or via a legislative basis)	Data Controller*	Data Controller*	Data Protection Office Legal Department Data Subjects**	Staff, Contractors and Relevant Third Parties Data Subjects**
Transparency of Personal Data Processing to Data Subjects	Data Controller*	Data Controller*	Data Subjects** Data Protection Office Legal Department	Staff, Contractors and Relevant Third Parties Data Subjects**

RACI Table (Continued)

***Data Controller =** All Service Units and Support Functions under the control of Tusla

****Data Subjects =** The owners of the personal data. They are mainly consulted and informed via the DPIA process and / or privacy notices. They can be also consulted via their representatives.

Process	Accountable	Responsible	Consulted	Informed
Processing of Personal Data	Data Controller*	Data Controller* Data Processors	Data Subjects** Data Protection Office Legal Department	Staff, Contractors and Relevant Third Parties Data Subjects**
Transfer of Processing of Personal Data to Data Processors	Data Controller*	Data Controller*	Data Subjects** Data Protection Office Legal Department	Staff, Contractors and Relevant Third Parties Data Subjects**
Personal Data Sharing	Data Controller* Joint Data Controller	Data Controller*	Data Subjects** Data Protection Office Legal Department	Staff, Contractors and Relevant Third Parties Data Subjects**

RACI Table (Continued)

***Data Controller =** All Service Units and Support Functions under the control of Tusla

****Data Subjects =** The owners of the personal data. They are mainly consulted and informed via the DPIA process and / or privacy notices. They can be also consulted via their representatives.

Process	Accountable	Responsible	Consulted	Informed
Retention Periods of Personal Data	Data Controller*	Data Controller* Data Processor	Data Subjects** Data Protection Office Legal Department	Staff, Contractors and Relevant Third Parties Data Subjects**
Secure Storage of Personal Data	Data Controller*	Data Controller* Data Processor	Data Subjects** Data Controller Legal Department	Staff, Contractors and Relevant Third Parties Data Subjects**
Secure Disposal of Personal Data	Data Controller*	Data Controller* Data Processor	Data Subjects** Data Protection Office Legal Department	Staff, Contractors and Relevant Third Parties Data Subjects**

RACI Table (Continued)

***Data Controller =** All Service Units and Support Functions under the control of Tusla

****Data Subjects =** The owners of the personal data. They are mainly consulted and informed via the DPIA process and / or privacy notices. They can be also consulted via their representatives.

Process	Accountable	Responsible	Consulted	Informed
Data Portability	Data Controller*	Data Controller* Data Processor	Data Subjects** Data Protection Office Legal Department	Staff, Contractors and Relevant Third Parties Data Subjects**
Transfers of Personal Data to Another Country	Data Controller*	Data Controller*	Data Subjects** Data Protection Office Legal Department	Staff, Contractors and Relevant Third Parties Data Subjects**
Record of Processing Activities	Data Controller*	Data Controller*	Data Protection Office Legal Department	Staff, Contractors and Relevant Third Parties Data Subjects**
Data Subject Records Requests	Data Controller*	Data Controller* Data Processors	Data Subjects** Data Protection Office Legal Department	Staff, Contractors and Relevant Third Parties Data Subjects** Data Protection Commissioner

RACI Table (Continued)

***Data Controller =** All Service Units and Support Functions under the control of Tusla

****Data Subjects =** The owners of the personal data. They are mainly consulted and informed via the DPIA process and / or privacy notices. They can be also consulted via their representatives.

Process	Accountable	Responsible	Consulted	Informed
Data Privacy Impact Assessments	Data Controller*	Data Controller*	Data Subjects** Data Protection Office Legal Department Data Processors Joint Data Controllers	Staff, Contractors and Relevant Third Parties Data Subjects**
Data Breaches	Data Controller*	Data Controller* Data Processors	Data Protection Office Legal Department Data Subjects** Data Processors	Staff, Contractors and Relevant Third Parties Data Subjects** Data Protection Commissioner
Training	Data Controller*	Data Protection Office	Data Controller Legal Department	Staff, Contractors and Relevant Third Parties

***Data Controller =** All Service Units and Support Functions under the control of Tusla
****Data Subjects =** The owners of the personal data. They are mainly consulted and informed via the DPIA process and / or privacy notices. They can be also consulted via their representatives.

Process	Accountable	Responsible	Consulted	Informed
Technical Security Measures	Data Controller*	Information Technology Department	Data Subjects** Data Protection Office Data Controller	Staff, Contractors and Relevant Third Parties Data Subjects**
Organisational Security Measures	Data Controller*	Data Controller*	Data Protection Office Policy Estates Information Technology Legal Department	Staff, Contractors and Relevant Third Parties Data Subjects**
Data Audits	Data Protection Office	Data Protection Office	Data Controller* Data Processors Internal Audit Quality and Control	Staff, Contractors and Relevant Third Parties Data Processors

RACI Table (Continued)

***Data Controller =** All Service Units and Support Functions under the control of Tusla
****Data Subjects =** The owners of the personal data. They are mainly consulted and informed via the DPIA process and / or privacy notices. They can be also consulted via their representatives.

Process	Accountable	Responsible	Consulted	Informed
Regulatory Inspections	Data Controller*	Data Protection Commissioner Data Controller Data Processors	Data Protection Office Legal Department	Staff, Contractors and Relevant Third Parties Data Subjects**
Privacy Management Information	Data Protection Office	Data Protection Office	Data Controller Data Processors	Board Senior Management of the Data Controller
Records Management	Data Controller*	Data Controller Data Processors	Data Protection Office Legal Department Data Subjects**	Staff, Contractors and Relevant Third Parties Data Subjects**

Data protection principles

All processing of personal data must be conducted in accordance with the data protection principles set out in relevant legislation.

Personal data must be processed lawfully, fairly and transparently

Lawful – The basis for the collection and processing of personal data is based on legislation to which Tusla is obliged to adhere or the consent of the data subject at the time that the personal data is collected. This policy prohibits the collection and processing of personal data that has not met these requirements.

Fairly and Transparently – In order for processing to be fair, Tusla will make information available to the data subjects with regard to the nature and extent of the processing at the time the personal data is collected. The information made available to the data subjects will usually, but not always be, through the use of privacy notices. This applies whether the personal data was obtained directly from the data subjects or from other sources. Tusla will ensure that the information provides sufficient detail on the processing and that such notices use clear and plain language and are provided in a manner that makes them accessible and understandable.

It is a requirement of this policy that privacy notices are at minimum made available via the following media:

- Client and Employee facing forms (electronic and paper based)
- Physical signage placed in public areas of Tusla offices and buildings
- Websites under the control and management of Tusla or offering Tusla services

Where privacy notices are not an appropriate method for communicating the nature and extent of processing to the data subject, e.g. the data subject has insufficient literacy skills to understand the privacy notices, other forms of communication are required by this policy to be undertaken.

This policy requires that when other forms of communication to data subjects are utilised that at minimum the following is documented and retained:

- The reason why the use of a privacy notice was not appropriate
- The alternative form of communication to the data subject that was utilised
- Written evidence that the data subject understood the alternative form of communication and agreed to the data processing

Personal data can only be collected for specific, explicit and legitimate purposes

Tusla must only process personal data for the stated purposes for which it is collected, under consent or other legislation to which Tusla is required to adhere. All staff, contractors and relevant third parties must be alert to requests for processing of personal data for purposes for which it was not collected; no matter how related the processing may appear. Where the processing is not clearly evident as being in line with the purposes for which the data was collected, then under this policy, processing must cease until a Data Privacy Impact Assessment (DPIA) has been completed. Please refer to the Data Privacy Impact Assessment Standard, a standard to this policy, for further information. **Insert Link to the Standard, Once Completed.**

Personal data must be adequate, relevant and limited to what is necessary for processing (data minimisation)

Tusla will ensure that in designing methods of data collection, via whatever medium that only the personal data required to provide the benefit or service requested will be processed. Tusla will undertake regular reviews of the data requested to ensure that the amount of personal data collected is minimised.

Personal data must be accurate and kept up to date with every effort to erase or rectify without delay

Tusla respects data subject's rights to ensure that their data is accurate and complete. Tusla also requires accurate and up-to-date data about data subjects in order to ensure that the correct benefits and services are provided to the correct recipients. All data collection procedures must be designed to ensure that reasonable steps are taken to update personal data where new data has been provided or is knowingly available. All changes to personal data must be shared with each third party with whom the previous data had been shared, unless the basis for the data sharing no longer exists, e.g. withdrawal of consent or withdrawal / amendment of the legislation providing the consent; the data sharing is no longer possible or requires a disproportionate effort.

Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing

Tusla will implement operational practices to ensure that personal data is retained only for the minimum period required to provide the benefit or services requested. Once that minimum period has expired the data must be securely disposed of, anonymised or handled in an appropriate method as designated under the acts.

Personal data must be processed in a manner that ensures appropriate security

Tusla will implement appropriate technical and Agency measures to ensure that appropriate security of the processing of personal data is implemented and adhered too.

Accountability for demonstrating compliance

Tusla will ensure that it maintains adequate records of its processing and evidence that it has complied with this policy, related policies, standards, guidelines and procedures as well as the Acts. Responsibility for collecting and maintaining the evidence is with Tusla's Service Units, Support Functions and their appointed their party processors.

Rights of Individuals whose data is collected

Tusla will design, maintain and adhere to appropriate policies, standards, guidelines and procedures in addition to providing appropriate training and other organisational and technical measures to ensure that the rights and freedoms of data subjects are respected and complied with the Acts is observed.

Right of access by the data subject

Tusla will implement procedures to ensure that requests from data subjects for access to their personal data will be identified and fulfilled in accordance with the Acts i.e. within the 30 days permitted. All such requests must be notified to the Data Protection Office, immediately upon receipt. The Data Protection Office will advise the Agency to process the request. Please refer to the Data Subject Records Request Standard, which is supplemental to this policy, for further information. **(Insert Link to Standard Once Drafted)**

Right to rectification

Tusla is committed to holding accurate personal data about data subjects and will implement processes and procedures to ensure that data subjects can have any identified inaccurate data rectified in an accurate and timely manner and in accordance with the requirements of the Acts. All such requests received from data subjects must be notified by the Agency to the Data Protection Office, immediately upon receipt. The Data Protection Office will then advise the Agency how to process the request. The Data Protection Office or a delegate appointed by the Data Protection Office will write to data subjects who have submitted such requests and confirm if the request has been actioned or denied and the reasons for same.

Right to erasure (right to be forgotten)

Tusla processes the personal data it collects because consent has been freely given by the data subject or there is a statutory basis for the processing. Where Tusla receives requests from data subjects, these requests must be notified immediately to the Data Protection Office who will advise the Agency on how to process the request. Such requests will be considered via the performance of an assessment by Tusla under the guidance of the Data Protection Office as to whether the data can be erased without affecting Tusla's obligations under other legislation. Tusla will implement appropriate procedures to carry out the assessment and where the right to erasure can be implemented then this will be done in a manner compliant with the Acts and Tusla's other statutory obligations. The Data Protection Office or a delegate appointed by the Data Protection Office will confirm in writing to the Data Subject, the conclusion of the assessment and the implications of that conclusion. All such assessments will be documented and retained for future evidencing purposes.

Right to restriction of processing

Tusla will implement and maintain appropriate procedures to assess whether a data subject's request to restrict the processing of their data can be implemented. All such requests received, must be immediately notified to the Data Protection Office by the service or functional unit upon receipt. The Data Protection Office will then advise the service or functional unit on how to process the request. Such requests will be considered via an assessment of Tusla obligations under the Acts and its other statutory obligations. Where such an assessment agrees with the data subjects right to restricted processing, Tusla will implement procedures to facilitate said restriction of processing in a manner compliant with the Acts. The Data Protection Office or a delegate appointed by the Data Protection Office will confirm in writing to the Data Subject, the conclusion of the assessment and the implications of that conclusion. All such assessments will be documented and retained for future evidencing purposes.

Right to data portability

Where Tusla has collected personal data on data subjects by consent or under its other statutory obligations then the data subjects have a right to receive the data in electronic format to give to another data controller as long as that right is not superseded by other statutory obligations of Tusla. Any such requests received by the Agency must be notified to the Data Protection Office, immediately upon receipt. The Data Protection Officer will then advise the Agency on how to process the request. Such requests will be determined via an assessment of the request in the context of Tusla's obligations under the Acts and its other statutory obligations. Where such requests are determined to be appropriate, following the assessment, Tusla will implement procedures to facilitate the transfer of the data to the identified alternate data controller in a manner which is compliant with the Acts. The Data Protection Officer or an appointed delegate of the Data Protection Office will then confirm in writing to the data subject, the outcome of the request and the implications of that outcome. All such assessments will be documented and retained for future evidencing purposes.

Right to object

Data subjects have a right to object to the processing of their personal data under the Acts. The processing must have been undertaken on the basis of public interest, the freely given consent of the data subject or the legitimate interest of Tusla under its other statutory obligations. All such objections from data subjects, received by the Agency must be notified to the Data Protection Office, immediately upon receipt. The Data Protection Office will then advise the Agency on how to process the objection. Such objections to processing will be determined via an assessment which will determine the legitimacy of the objection in light of the Acts and Tusla's other statutory obligations. If the objection is determined to be legitimate, then Tusla will implement procedures to facilitate the objection in a manner compliant with the Acts. The Data Protection Office or a delegate appointed by the Data Protection Office will then confirm in writing to the data subject, the conclusions of the objection assessment and the implications of those conclusions.

Right not to be subject to automated decision making

Under the Acts, data subjects have the right not to be subject to a decision based solely on automated processing, where such decisions would have a legal or significant effect concerning him or her. Tusla will ensure that where such automated decision making has been implemented then an appropriate right of appeal to a member or panel of staff is available to the data subject. All such objections by data subjects to automated decision making received

by the Agency must be notified to the Data Protection Office immediately upon receipt. The Data Protection Office will then advise the Agency on how to process the request. Such objections to automated decision making will be determined via an assessment which will determine the legitimacy of the objection in light of the Acts and Tusla's other statutory obligations. If the objection is determined to be legitimate, then Tusla will implement procedures to facilitate the objection in a manner compliant with the Acts. The Data Protection Office or a delegate appointed by the Data Protection Office will then confirm in writing to the data subject, the conclusions of the objection assessment and the implications of those conclusions.

Right to complain

Tusla will implement and maintain a complaints process whereby complaints by data subjects can be made to Data Protection Officer. The Data Protection Officer will work with the data subject to bring the complaint to a satisfactory conclusion for both parties. The data subject will be informed of their right to bring their complaint to the Office of the Data Protection Commissioner and their contact details.

Accountabilities and Responsibilities of Tusla

Tusla has accountability and is responsible for the following

Ensuring appropriate technical and organisational measures

Tusla will implement appropriate technical and organisational measures to ensure the adequate protection and use of personal data. Appropriate evidence of such organisational and technical must be available to be produced by the Agency upon demand. It is not the responsibility of Tusla's Service Units, Support Functions and its Processors to maintain and evidence these organisational and technical measures to the required standards.

Maintaining a record of data processing

Tusla's Service Units, Support Functions and its Processors will maintain a record of their data processing activities in the manner prescribed by the Acts. It is the responsibility of Tusla Service Units, Support Functions and its Processors to maintain the Record of Processing Activities (ROPA). The ROPA must be risk rated by the Agency so that the processing of highest risk to the rights and freedoms of data subjects are identified. The ROPA must be updated and supplied to the Data Protection Office by Tusla's Service Units, Support Functions and its Processors, upon request, but at minimum on an annual basis. The ROPA prior to being supplied to the Data Protection Office must be reviewed and signed off by senior management. Once requested by the Data Protection Office, the ROPA must be supplied no later than 60 days following the request.

Implementing appropriate agreements with third parties

Tusla's Service Units and Support Functions will implement appropriate contractual arrangements or agreements (as applicable), based on corporate templates that have been signed off by the Data Protection Office and the Legal Department with all third parties with whom it shares personal data. All proposed data sharing with Third Parties by Tusla's Service Units, Support Functions and its Processors, are required to be notified immediately to the Data Protection Officer.

These Third Parties include Data Processors, Data Sharing Arrangements with other Public Authorities and Data Sharing with other authorised parties. No other contractual arrangements for the sharing of personal data with Third Parties are permitted under this policy without the prior written approval of both the Data Protection Office and the Legal Department. Post the implementation of GDPR (25 May 2018) all such agreements must be implemented in writing prior to the commencement of the transfer of the data. The agreement shall specify the purpose of the transfer, the requirement for adequate security, right to terminate processing, restrict further transfer to other parties, ensure that responses will be given to requests for information and the right to audit.

Any data sharing arrangements in place prior to the implementation of GDPR (25 May 2018) are required to be notified to the Data Protection Office by Tusla's Service Units and Support Functions for tracking purposes. In addition, Tusla's Service Units, Support Functions and its Processors are required under this policy to implement new contractual arrangements or agreements (as applicable), based on corporate templates that have been signed off by the Data Protection Office and the Legal Department.

Transfers of personal data outside of the European Economic Area

Tusla will not transfer the personal data of its data subjects outside of the European Economic Area unless there is a statutory basis for that transfer, or the consent of the data subject provided for that transfer and unless there is adequate data protection measures in place as set out in the Acts. All such proposed transfers must be notified to the Data Protection Office prior to the transfer of the data and such transfers are only permitted upon receipt of written approval by the Data Protection Office and the Legal Department.

Data protection by design and by default

All personal data processing activities within Tusla Service Units, Support Functions and its Processors are required to implement controls which protect the rights and freedoms of data subjects and which enshrine the principles of privacy by design. These controls are required to be considered at the time of determining the means of processing as well as when the actual processing takes place.

Data protection impact assessments

Tusla's Service Units, Support Functions and its Processors are required to implement procedures whereby any new process or any changes to existing processes involving personal data are notified to the Data Protection Office. The Data Protection Office will then issue a Data Privacy Impact Assessment Screening Questionnaire which is required to be completed and returned to the Data Protection Office within ten days. The Data Protection Office will then opine on whether a full Data Privacy Impact Assessment (DPIA) is required to be completed.

Where such a DPIA is required to be completed, it is the responsibility of Tusla's Service Units, Support Functions and its Processors to complete same. The Data Protection Office will provide the DPIA template for completion. The performance of the DPIA can be outsourced to a suitably qualified individual and / or organisation. It is a requirement of this policy that all DPIAs take into account the views of data subjects and / or their representatives and any Data Processors or other Third Parties involved in the process.

The Data Protection Office must be sent a copy of the completed DPIA along with supporting evidence and they will then opine if they agree with the conclusions of the DPIA. If a disagreement is noted between the Data Protection Office and the conclusions of the DPIA, then this must be documented and submitted to the Board, or a designated sub-committee thereof for a final decision.

For new processes, processing must not commence until the DPIA process has been finalised.

Please refer to the Data Privacy Impact Assessment Standard, which is supplemental to this Policy for more detailed information on the DPIA process. **(Insert a Link to the DPIA Standard Once Drafted)**

Personal data breaches

Tusla defines a 'personal data breach' as meaning 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. Tusla deems any theft, loss leakage of personal data as well as unauthorised access to and amendment of personal data in paper or digital format to be a personal data breach. A lack of availability of personal data which has

the potential to affect decision making in relation to data subjects is also deemed by Tusla to be a data breach.

It is a requirement of this policy, that all potential data breaches are notified to the Data Protection Office by Tusla's Service Units, Support Functions and its Processors as soon as they become aware of same. Notification must be made to datacontroller@tusla.ie using the forms and providing the detailed set out in the Data Breach Standard which is supplemental to this policy. **(Insert a Link to the Data Breach Standard Once Drafted)**

Tusla is obligated under the Acts to report all breaches within 72 hours of becoming aware of same to the supervisory authority, the Data Protection Commissioner of Ireland, and to Data Subjects where this is a risk to the rights and freedoms of the data subjects at the centre of the breach.

Freedom of Information

Obligations under the Freedom of Information Act are not the subject of this policy and are dealt with under a separate policy with its own requirements. **(Insert Link to FOI Policy)**

Governance

Tusla will monitor its compliance with the Acts through the Data Protection Office which in turn reports functionally to the Board or a designated sub-committee thereof and administratively to the Office of the CEO.

Please refer to the Charter of the Data Protection Officer, for further details on Tusla's governance arrangements for the Data Protection Office.

Personal Data Audits

The Data Protection Office will develop and implement a risk based personal data audit plan which is subject to approval and review by the Board.

All of Tusla's Service Units, Support Functions and its Processors are required to co-operate fully with the Data Protection Office if selected for a Personal Data Audit and provide all requested evidence in a timely manner.

All audits will be subject to Terms of Reference which will set out the scope of the audit.
Draft findings will be issued to the management of area under audit for factual accuracy and management response purposes.

All final findings are required to have an accountable senior management owner assigned with a clearly defined action plan and due dates which are not later than 12 months out from the date of the finding. It is the responsibility of Tusla Management to provide these owners, action plans and due dates to the Data Protection Office.

Further details are set out in the Personal Data Audit Standard which is supplemental to this policy. **(Insert a Link to the Personal Data Audit Standard Once Drafted)**

The Data Protection Officer (DPO)

The role, authority, responsibilities and independence of the Data Protection Officer (DPO) are as set out in the Charter of the Data Protection Officer and this policy defers to that Charter.

At a high level the DPO is an independent function with responsibility for:

- Monitoring the compliance of Tusla with the Acts in addition to providing advice on GDPR requirements
- Opining on the need for DPIAs and adequacy of the DPIAs performed.by Tusla
- Co-operating with Supervisory Authorities and acting as a point of contact for same

Please read the Charter for more detailed information on the role, authority, responsibilities and independence of the DPO.

Responsibilities of staff and similar parties under this Policy

Anyone involved in the processing of personal data on behalf of Tusla has an obligation to comply with the requirements of this Data Protection Policy. For the purposes of clarity that includes Tusla staff, contractors working in Tusla, Data Processors engaged by Tusla and any other party which processes personal data under the control of Tusla.

Training

It is a requirement of this Policy that any party directed by Tusla to undertake training associated with Data Protection do so within the time limits set out by that direction. When training is required to be undertaken, parties will receive formal notification of same. Training requirements will also be published on the Data Protection Officer page on the Intranet and staff of Tusla as well as contractors working within Tusla are required to check this page regularly to ensure that they have completed all of the required training.

Failure to complete required training is a breach of this policy and will be reported to senior management as well as subject to the measures outlined in the staff employment handbook, contractors' agreements and Data Processor agreements (as applicable).

Where to go if you have queries about the data protection policy

The Data Protection Office has a dedicated page on the intranet which has resources available such as templates, answers to Frequently Asked Questions (FAQs) and you should refer to these in the first instance.

If you cannot find the answer to your query on the website then do not hesitate to contact the Data Protection Office on datacontroller@tusla.ie or alternatively at 01 771 8500.

Exceptions to this Policy

There are no exceptions to this policy. In extreme circumstances, exceptions may be possible but only after a formal request has been made to the Data Protection Office and such requests have been approved in writing by the Data Protection Office, the Legal Department and the Board or a designated sub-committee thereof.

Conflicts with this Policy

Where conflicts are noted between this Policy and another policy, standard, charter, guideline or procedure as they relate to personal data, then this policy will take precedence unless Legal opinion has been obtained to the contrary.

Any such conflicts identified, must also be notified in writing to the Data Protection Office and the owner of the policy which conflicts with this policy.

Review and Audit

This policy will be reviewed at minimum annually or upon a requirement of significant change to the policy, whichever comes first.

Compliance with the policy will be monitored via the Data Protection Officer activities as set out in the DPO Charter.

Approvals and sign offs

This policy comes into effect on 25 May 2018.

Document Control	
Approved By	**Data Protection Officer**
Date approved	**03 March 2018**
Approved by	**Chief Executive Officer**
Date approved	**29 March 2018**
Approved by	**Board or a Designated Sub-Committee**
Date approved	**29 March 2018**
Approved by	**NPOC**
Date approved	**N/A**
Next review date	**Upon significant change to the Policy or at minimum by May 2019.**

Version Control Table

Version	Date	Changes made by	Change Description
1.0	03 March 2018	Data Protection Officer (Jason Finnerty)	Initial draft of Tusla GDPR Privacy policy document
1.1	12 March 2018	Director of Corporate Services (Laura Slevin)	Review of initial draft GDPR Privacy Policy – comments and suggested amendments noted and incorporated and approval in principal
1.2	16 March 2018	Legal Affairs (Pamela Benson)	Review of draft GDPR Policy – comments and suggested amendments noted and incorporated and approval in principal
1.3	29 March 2018	Board	Review of draft GDPR policy – comments and suggested amendments incorporated and approval in principal
1.4	29 March 2018	External Counsel (Paul Anthony McDermott	Review of draft GDPR policy – comments and suggested amendments incorporated and approval in principal
1.5	**XXXXXX**	**NPOC**	**XXXXXX**