Privacy Policy

2018

Pact

Privacy Policy

Date	April 2019
Revision Number	1.0
Approval Date	
Next Revision Date	July 2020
Document Developed by	DPO
Document Approved by	Board of Directors
Responsibility for Implementation	All Staff
Responsibility for Review and Audit	DPO

Table of Contents

Introduction	4
Purpose and Scope	5
Responsibility for Policy	5
Data Protection Principles	5-7
1. Personal data must be processed lawfully, fairly and transparently	
2. Personal data can only be collected for specific, explicit and legitimate purposes	
3. Personal data must be adequate, relevant and limited to what is necessary for processing (data minimisation)	
4. Personal data must be accurate and kept up to date with every effort to erase or rectify without delay	
5. Personal data must be kept in a form such that the data subject can be identified, for as long as is necessary for processing only	
6. Personal data must be processed in a manner that ensures appropriate security	
Accountability	8
- Demonstrating Compliance	8
- Rights of Individuals Whose Data is Collected	8
- Right of Access by Data Subject	8
- Right to Rectification	8
- Right to Erasure (Right to be Forgotten)	9
- Right to Restriction of Processing	9
- Right to Data Portability	10
- Right to Object	10
- Right to Complain	10
***Pact* – Accountabilities & Responsibilities**	10
- Ensuring appropriate technical and organisational measures	10
- Maintaining a record of data processing	10
- Implementing Appropriate Agreements with Third Parties	10
- Transfer of Personal Data Outside of EU	11
- Data Protection by Design and by Default	11
- Personal Data Breaches	12
Freedom of Information	12
- Obligations	12
- Governance	12
- Data Protection Officer	12
Responsibilities of Staff under this Policy	13
Raising a Query about this policy	13
Conflicts with this Policy	13
Review and Audit	13
Glossary of Terms and Definitions	14- 15

Introduction

Pact is committed to protecting the rights and privacy of individuals in accordance with European Union and Irish Data Protection Legislation and within the terms of the Adoption (2010) Act and other relevant legislation to which the Agency must adhere.

Data Protection Legislation confers rights on individuals as well as responsibilities on those persons processing personal data. This policy sets out how *Pact* seeks to process personal data and to ensure that staff and data processors of *Pact*, understand the rules governing the use of personal data to which access is granted during work.

In order to achieve its mission, functions and effective service delivery, ***Pact*** will process personal data about employees and service users, suppliers, and other individuals, that is commensurate with the service(s) / agreement provided. All such processing will be done awfully and fairly and in accordance with the principles of The General Data Protection Regulation, (GDPR) 2018 Act and other governing legislation.

Personal data may be exchanged with other Government Departments and Agencies in certain circumstances where this is provided for by law. Personal data will be processed in compliance with all relevant Data Protection Legislation and the other Acts to which *Pact* is obliged to adhere. The General Data Protection Regulation (GDPR) came into force across the EU on 25th May 2018 replacing previous data protection legislation. *Pact*'s privacy policy reflects the requirements of the GDPR and will be reviewed annually by Bernie Griffiths, Data Protection Officer (DPO).

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 ***Pact*** 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 ***Pact***. Each must be familiar with this policy and comply with its terms. This policy also applies to all *Pact*'s personal data processing functions in relation to identified or identifiable natural persons, including those performed on service users, employees', suppliers', and any other personal data *Pact* processes from any source. *Pact* 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.

Responsibility for this Policy

All staff, contractors and relevant third parties are required to ensure this policy is implemented and adhered to. This policy will also be supplemented by Standards and operational procedures in place within each Service which enable compliance.

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 agreements, or the third-party agreement as applicable.

Data Protection Principles

Processing of personal data will 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 *Pact* is obliged to adhere, or the consent of the data subject at the time that the personal data is collected (in order to effect services provided to service users) . 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, *Pact* will make information available to the data subjects regarding the nature and extent of the processing at the time the personal data is collected.

This applies whether the personal data was obtained directly from the data subjects or from other sources. *Pact* will ensure that the information provides enough 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 *Pact* offices and buildings
- Websites under the control and management of *Pact* or offering *Pact* 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

Pact will only process personal data for the stated purposes for which it is collected under consent, or as required by legislation to which ***Pact*** is required to adhere.

All staff, contractors and relevant third parties are required to be alert to requests to process personal data for purposes other than for which it was collected.

This policy requires the processing of data only where the processing is in line with the purposes for which it was collected. Where that clarity is not evident, the processing must cease until a Data Privacy Impact Assessment (DPIA) has been completed to ensure compliance with *Pact*s legal obligations.

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

Pact 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. *Pact* 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

Pact respects data subject's rights to ensure that their data is accurate and complete. 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, for as long as is necessary for processing only

Pact 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

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

Accountability

Demonstrating compliance

Pact will maintain adequate records of its processing and evidence that it has complied with this policy and other related policies, guidelines, procedures in context of relevant Acts.

Responsibility for collecting and maintaining the evidence lies is with *Pact*'s administration support team, its social workers, and appointed data processors.

Rights of Individuals whose data is collected

Pact 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 under the Acts is observed.

Right of access by the data subject

Pact will implement procedures to ensure that requests from data subjects for access to their personal data will be identified and fulfilled within the 30 days permitted. All such requests must be notified to the DPO, immediately upon receipt. The DPO 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.

Right to rectification

Pact 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 to the DPO, immediately upon receipt. The DPO will then advise the Agency how to process the request. The DPO or a delegate appointed by the DPO 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)

Pact processes the personal data it collects because consent has been freely given by the data subject (in line with the service being provided by ***Pact***) and / or there is a statutory basis for the processing. Any request from a data subject must be notified immediately to the DPO. Such requests will be considered via the performance of an assessment by *Pact* under the guidance of the DPO as to whether the data can be erased without affecting *Pact*'s obligations under other legislation. *Pact*

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 ***Pact*'s** other statutory obligations. The DPO or a delegate appointed by the DPO 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

Pact 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 DPO upon receipt. The DPO will then advise how to process the request. Such requests will be considered via an assessment of *Pact* obligations under the Acts and its other statutory obligations. Where such an assessment agrees with the data subjects right to restricted processing, *Pact* will implement procedures to facilitate said restriction of processing in a manner compliant with the Acts. The DPO or a delegate appointed by the DPO 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 *Pact* has collected personal data by consent, or under its other statutory obligations those data subjects have a right to receive the data in electronic format to give to another data controller where that right is not superseded by other statutory obligations of *Pact*. Any such requests received must be notified to the DPO, immediately upon receipt. The DPO will advise the Agency on how to process the request. Such requests will be determined via an assessment of the request in the context of *Pact*'s obligations under GDPR and its other statutory obligations. Where such requests are determined to be appropriate, *Pact* will implement procedures to facilitate the transfer of the data to the identified alternate data controller in a manner which is compliant with its statutory obligations. The DPO or an appointed delegate, will then confirm in writing to the data subject, the outcome of the request and the implications of that outcome. All such correspondences and associated processes 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.

Pact will only undertake data processing on the clear basis of the freely given consent of the data subject or, where the legitimate interest arises through statutory obligations. Objections from data subjects received by ***Pact*** are required to be notified to the DPO for processing.

Objections to processing data will be determined via an assessment to determine its legitimacy considering the Acts and ***Pact*'s** other statutory obligations. Where an objection is determined to be legitimate, procedures will be implemented in accordance with the Acts. The DPO or a delegate appointed by the DPO will then confirm in writing to the data subject, the conclusions of the objection assessment and the decision and steps taken.

Right to complain

Pact will implement and maintain a complaints process, whereby complaints by data subjects can be made to DPO. The DPO 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 *Pact*

Ensuring appropriate technical and organisational measures

Pact will implement appropriate technical and organisational measures to ensure the adequate protection and use of personal data. Appropriate evidence of such measures must be available to be produced by the Agency upon demand.

It is the responsibility of *Pact*'s Services Units and its Processors to maintain and evidence these organisational and technical measures to the required standards.

Maintaining a record of data processing

Pact's services will maintain a record of its data processing activities in the manner prescribed by the Acts. It is the responsibility of *Pact* Services to maintain the Record of Processing Activities (ROPA).

The ROPA is risk rated so that processing to ensure the highest risk to the rights and freedoms of data subjects are identified. The ROPA must be updated and supplied to the DPO by ***Pact*'s** Services upon request, but at minimum on an annual basis. The ROPA prior to being supplied to the DPO must be reviewed and signed off by the Board of Directors. Once requested by the DPO, the ROPA must be supplied within 60 days.

Implementing appropriate agreements with third parties

Pact's Services will implement appropriate contractual arrangements or agreements (as applicable), based on corporate templates that have been signed off by the Board of Directors and with all third parties with whom it shares personal data. All proposed data sharing with Third Parties by *Pact*'s Service Units, are required to be notified immediately to the DPO. 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 DPO and Board of Directors. 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 are required to be notified to the DPO by *Pact*'s Services and Support Functions for tracking purposes. In addition, *Pact*'s Services 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 DPO and the Legal Department.

Transfers of personal data outside of the European Economic Area

Pact 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 are adequate data protection measures in place as set out in the Acts. All such proposed transfers must be notified to the DPO prior to the transfer of the data and such transfers are only permitted upon receipt of written approval by the DPO and Board of Directors.

Data protection by design and by default

All personal data processing activities within *Pact* Service Units 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.

Personal data breaches

Pact 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. *Pact* 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 *Pact* to be a data breach.

It is a requirement of this policy, that all potential data breaches are notified to the DPO by *Pact*'s Service Units, Support Functions, and its Processors as soon as they become aware of same.

Notification must be made to datacontroller@*pact*.ie using the forms and providing the details set out in the Data Breach Standard which is supplemental to this policy. ***Pact*** is obligated under the Acts to report any/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 there is a risk to the rights and freedoms of the data subjects at the centre of the breach.

Freedom of Information

Obligations

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.

Governance

Pact will monitor its compliance with the Acts through the Principal Social Worker who in turn reports to the Board or a designated sub-committee thereof.

Data Protection Officer (DPO)

- Monitoring the compliance of *Pact* with the Acts in addition to providing advice on GDPR requirements
- Opining on the need for DPIAs and adequacy of the DPIAs performed by *Pact*
- 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

All persons involved in the processing of personal data on behalf of *Pact* are obliged to comply with the requirements of this Policy and to seek immediate clarification or guidance on its application if necessary, to ensure compliance. For the purposes of clarity that includes ***Pact*** staff, contractors working in *Pact*, Data Processors engaged by *Pact* and any other party which processes personal data under the control of ***Pact***.

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

If you cannot find the answer to your query within this policy then do not hesitate to contact the Agency directly on: dataprotection@pact.ie or by calling: 1850 67 3333 or (01) 2166 300

Conflicts with this Policy

Where conflicts are noted between this Policy and another policy, 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 DPO 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.

Glossary of Terms and Definitions

Term	Definition
Personal data	Personal data is data relating to an identifiable 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 during his employment.
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 *Pact* 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.
	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.
	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 are independent reviews performed by the DPO 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 subcommittee 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. *Pact* when considering such a request must also take account of the other Acts to which it is obliged to adhere.
The 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. *Pact* when considering such a request must also take account of the other Acts to which it is obliged to adhere.
Cross Country 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.
	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 *Pact* 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 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 if 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 *Pact* 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.

Approvals and sign offs	
Date this policy comes into effect	25 May 2018
Date approved	2018
Approved by Board or a Designated Sub-Committee	2018
Next review date	Upon significant change to the Policy or at minimum annually from inception date