**The Care Trust Data Protection Policy**

**Policy Statement**

The purpose of this policy is to provide details regarding the Data Protection obligations of The Care Trust DAC (‘TCT’). This includes obligations in dealing with personal data, to ensure that the organisation complies with the requirements of the relevant Irish legislation, namely the General Data Protection Regulation (GDPR) 2018, the Irish Data Protection Act (1988), and the Irish Data Protection (Amendment) Act (2003), and with best practice in this area.

**Introduction**

The Care Trust was incorporated in 1974 and registered as a designated activity company in 2016. The Care Trust is a registered charity, raising funds from the general public on behalf of our charity partners, CRC, Rehab Group, and special charitable projects—all of which provide vital services and support for children and adults with disabilities, those who require support with learning, training and education and/or those require medical support.

The general public contribute to The Care Trust by regular periodic donations and by entering periodic lottery draws which take place every month. Contributions are primarily transacted by direct debit, standing order, debit card, or by cheque or cash. To facilitate the processing of contributions, The Care Trust only keeps personal data for purposes that are specific, lawful and clearly stated.

Every individual has the right to know what personal information is held about them. The Care Trust undertakes to ensure that all personal data, in hard copy and/or electronic format, is stored securely and provides internal and external auditors opportunity to vet its security systems and procedures on a regular and planned basis.

The Care Trust will not sell, trade, or otherwise transfer to outside parties personally identifiable information, except to trusted third parties who assist The Care Trust operating its websites, conducting its business, or servicing its Supporters, so long as those parties agree to keep this information confidential as part of their contract with The Care Trust.

Data Protection law places obligations on The Care Trust, and on all staff and Fundraising Representatives who keep personal information. Hereafter, references to ‘The Care Trust’ includes all staff and Representatives.

The Board and the Chief Executive (‘CEO’) of The Care Trust take responsibility to:

* Ensure compliance with data protection legislation;
* Have a clear procedure for handling requests for access to records;
* Ensure that appropriate procedures remain in place to support compliance including periodic review and audit and
* Examine the case for establishing databases and regulate such databases.

All staff members are not expected to be experts in relation to data protection. However, the key aim of this Policy is that staff be aware of their responsibilities and can identity where a data protection issue has arisen for consultation with the CEO.

**Definitions**

Data Protection is the safeguarding of the privacy rights of individuals in relation to the processing, storage and security of their personal data. Staff and Supporters supply information about themselves (for example, monthly direct debit details) to The Care Trust and thus, the legislation applies.

Data Controller means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. In general, the Controller is The Care Trust. However, it may interact with other bodies that also act as Data Controller.

A Data Subject is an individual who is the subject of personal data, and this term covers both staff and Supporters to The Care Trust. Data Protection legislation applies only to living persons.

Data is information in a form which can be processed and rights apply whether the information is held in electronic or manual format, or in photographs or digital images.

Personal data means any information relating to an identified or identifiable natural person (“Data Subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier.

Further relevant definitions are attached in Appendix 1 to this document.

**Data Protection Principles**

Data Protection Principles as set out by the Data Protection Act 2018.

* Obtain and process information fairly;
* Keep it only for one or more specified, explicit and lawful purposes; Use and disclose it only in ways compatible with these purposes; Keep it safe and secure;
* Keep it accurate, complete and up-to-date;
* Ensure that it is adequate, relevant and not excessive;
* Retain it for no longer than is necessary for the purpose or purposes; Give a copy of their personal data to that individual, on request.

Further clarification on each principle, and how they apply to The Care Trust, is set out below.

**Obtain and process information fairly**

To fairly process personal data it must have been fairly obtained, and the Data Subject must have given consent to the processing; or the processing must be necessary for one of a number of reasons including but not limited to:

* the performance of a contract to which the Data Subject is a party;
* compliance with a legal obligation, other than that imposed by contract; or
* for the purpose of the legitimate interests pursued by The Care Trust except where the processing is unwarranted in any particular case by reason of prejudice to the fundamental rights and freedoms or legitimate interests of the data subject.

**To Fairly Obtain Data**

The Data Subject must, at the time the personal data is being collected, be made aware of:

* The name of the Data Controller, e.g., The Care Trust;
* The purpose in collecting the data, e.g., The Care Trust fundraising on behalf of its charity partners;
* The identity of any representative nominated for the purposes of the Acts, e.g., name and ID number of Fundraising Representatives acting on The Care Trust’s behalf;
* The persons or categories of persons to whom the data may be disclosed, e.g., to trusted third-party providers such as auditors;
* Whether replies to questions asked are obligatory and the consequences of not providing replies to those questions;
* The existence of the right of access to their personal data;
* The right to rectify their data if inaccurate or processed unfairly; and
* any other information which is necessary so that processing may be fair and to ensure the Data Subject has all the information that is necessary so as to be aware as to how their data will be processed.

In addition, where personal data is not obtained from the Data Subject, either at the time their data is first processed or at the time of disclosure to a third party, the above information is provided to the Data Subject and they must also be informed of the identity of the original Data Controller from whom the information was obtained and the categories of data concerned.

The Care Trust has a Data Privacy Policy which provides all the specific information necessary for individuals, potential Supporters and existing Supporters to ensure all processing activities are transparent. This is available at all times on The Care Trust’s website.

**Data Subject Must Have Given Consent**

Consent means any freely given, specific, informed and unambiguous indication of the wishes by which the Data Subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed.

Consent must reflect the Data Subject's genuine and free choice. If there is any element of compulsion, or undue pressure put upon the Data Subject, consent is not valid.

Consent must be specific. Blanket consent that does not specify the exact purpose of the processing is not valid consent. In order to be specific, consent must be intelligible.

Consent must be informed. The Data Subject must be provided with sufficient information to enable them to understand what they are consenting to.

The Care Trust aims to clearly and precisely explain the scope and the consequences of the data processing, via its Fundraising Representatives (in person), its website, and all documentation provided to Supporters by hand, post, or email.

**Method of Consent**

Consent must take the form of an affirmative action or statement. This agreement can take any appropriate form (e.g., signature, tick-box, verbal consent, etc.), The Care Trust understands that it must be affirmative in nature; mere silence, passive acquiescence or failure to opt-out does not constitute valid consent.

The Data Subject's consent to the processing of their personal data will not be tied to other matters. Consent can be provided by any appropriate method enabling a freely given, specific, informed indication of the Data Subject's wishes. It generally cannot be obtained from a third party. In completing and signing a mandate (debit card or direct debit), Supporters give consent to The Care Trust to process their contributions via direct debit from their bank account, and to contact them in an appropriate manner to discuss same.

The request for consent is presented by The Care Trust in a manner that is clearly distinguishable from the other matters, in an easily accessible form, using clear language. The Care Trust understands that if the Data Subject is asked to consent to something inconsistent with GDPR requirements that consent will not be binding.

**Keep it only for one or more specified, explicit and lawful purposes**

Data is only kept for purposes that are specific, lawful and clearly stated and the data is only be processed in a manner compatible with that purpose(s) agreed with the Data Subject. Supporters of The Care Trust have a right to question the purpose for which their data is held. The Care Trust gives a commitment to Supporters that data will not be passed onto third parties.

To comply with this rule:

* The Data Subject should know the reason/s why The Care Trust is collecting and retaining their data, e.g., to process contributions for draws and/or prize draws;
* The purpose for which the data is being collected should be a lawful one; and
* The Care Trust must be aware of the different data sets kept and the specific purpose of each Data Subject.

**Use and disclose it only in ways compatible with these purposes**

Any use or disclosure must be necessary for the purpose(s) or compatible with the purpose(s) for which The Care Trust collect and keep the data. (This requirement can be lifted in certain restricted cases, in keeping with legislation.) Any processing of personal data by a Data Processor on behalf of The Care Trust must be undertaken in compliance with the data protection legislation.

**Keep it safe and secure**

Appropriate security measures are taken by The Care Trust against unauthorised access to, or alteration, disclosure or destruction of the data, and against its accidental loss or destruction. The nature of security used by The Care Trust may take into account what is available technologically, the cost of implementation and the sensitivity of the data in question.

**Keep it accurate, complete and up-to-date**

It is in the interests of The Care Trust to ensure data is accurate for reasons of efficiency and effective decision-making. In addition, The Care Trust may be liable to an individual for damages, if The Care Trust fails to observe the duty of care provision in the Act applying to the handling of personal data which tends to arise substantially in relation to decisions or actions based on inaccurate data. (The accuracy requirement does not apply to back-up data.)

**Ensure that it is adequate, relevant and not excessive**

It is essential that The Care Trust seek and retain only the minimum amount of personal data needed to achieve their purpose(s). The information sought and held by The Care Trust is:

* Adequate in relation to the purpose/s for which it is sought.
* Relevant in relation to the purpose/s for which it is sought and
* Not excessive in relation to the purpose/s for which it is sought.

**Retain it for no longer than is necessary for the purpose or purposes**

Under the legislation, personal data collected for one purpose cannot be retained once that initial purpose has ceased. Equally, as long as personal data is retained the full obligations of the Acts attach to it. If The Care Trust no longer holds the information, then the Acts don’t apply.

The Care Trust applies a policy of retaining all documents for no longer than six years, in line with Revenue guidelines for financial records. Where there is a need to retain Supporters’ data after this period e.g., to analyse payment trends, The Care Trust employ appropriate anonymisation of personal data, as permitted by the Acts. This involves the removal of any and all personal sensitive data that would allow current and lapsed Supporters to be identified.

**Destruction**

Once the period of use expires, THE CARE TRUST have processes in place for the secure destruction and disposal of data. This involves the following:

* Shredding of all hard copy documents containing personal data. THE CARE TRUST avails of a contracted shedding service, whereby hard copy documents are confidentially shredded on-site.
* Redacting/deleting from the IT systems all electronic personal sensitive data and the computer recycle bin emptied .
* Regular checks of all computers and devices to ensure that no personal data is retained in this way.
* Giving copies of personal data to individuals, on request

On making an access request, any individual about whom The Care Trust keeps personal data is entitled to:

* A copy of the data maintained about them; for example, a scanned copy of the Supporter’s direct debit mandate
* Know the categories of their data and the purpose/s for processing it
* Know the identity of those to whom you disclose the data
* Know the source of the data, unless it is contrary to public interest
* Know the logic involved in automated decisions and
* Data held in the form of opinions, except where such opinions were given in confidence and even in such cases where the person’s fundamental rights suggest that they should access the data in question.

Clear coordinated procedures, which are available for internal and external auditor scrutiny, are in place in The Care Trust to ensure that all relevant manual files and IT systems are checked for the data in respect of access requests.

**Right to Rectification, Erasure, Restriction, Data Portability**

Every individual about whom The Care Trust keeps personal information has the right to have the information rectified or erased, to have data taken off a direct marketing / mailing list and has the right to complain to the Data Protection Commissioner.

**The following rights are also observed by The Care Trust:**

* Data subjects have the right to restrict processing in certain cases, i.e., a controller may store but not further process data. The Care Trust undertake to notify the subject before lifting such a restriction.
* Data subjects have the right to object to the processing of data in certain instances, such as direct marketing / profiling.
* GDPR also introduces a right to portability of personal data that an individual has provided to a Controller. This enables individuals to obtain their data, and have it transmitted to another controller without hindrance, where technically feasible. THE CARE TRUST understands that data transmitted should be in a structured, commonly used and machine-readable format. (This provision only applies where automated processing is carried out and is based on consent.) This right does not extend to data generated by the Controller. The Care Trust will provide a comprehensive Supporter Profile Report as fulfilling this requirement.

In each of the instances detailed above (Rectification, Erasure, Restriction, Data Portability), The Care Trust undertake to provide information arising from any such request to the Data Subject without undue delay, and at the latest within one month of the receipt of the request.

**Data access requests**

To make an access request the data subject must:

* Apply to The Care Trust in writing (including email);
* Give any details which might be needed by The Care Trust to help identify and locate all information maintained about them.

In response to an access request The Care Trust will:

* Supply the information to the individual without undue delay and within 30 days of receiving the request;
* Ensure that any changes to the data requested are implemented within 30 days of receiving the request; and
* Provide the information in a form which will be clear to the ordinary person.
* The Care Trust will not charge a fee, unless further copies are requested, in which case a reasonable administrative cost may be applied.

Where no information is kept, the individual making the request will be informed within the 30 days. If the individual’s right of access is restricted in accordance with legislation, The Care Trust will notify the Data Subject in writing within 30 days and will state reasons for refusal. The Care Trust will inform the individual of his/her entitlement to complain to the Data Protection Commissioner.

**Redaction**

Where it is deemed that not all the content in a particular document is of relevance to the individual making the data request, The Care Trust may redact certain information in the records being disclosed. Redaction is carried out on the original/scanned document and must be applied thoroughly and consistently.

Details of all redactions identified and agreed with the CE0 are recorded, and a copy of the scanned document retained. Legislation also permits that a summary of the document can be prepared, if the extent of redaction renders the resulting document incomprehensible. The Care Trust accept that the data subject can appeal such redaction decisions.

**Use of CCTV systems**

The Care Trust is aware that recognisable images captured by CCTV systems are personal data and therefore are subject to the provisions of the Acts. The Care Trust does not currently use CCTV in any aspect of its business. The Care Trust will only install a CCTV camera/system if satisfied that the use of such a camera/system is necessary, relevant and proportionate.

The Care Trust staff members working in an environment with CCTV will be advised that CCTV is to be installed. Storage and retention of material collected by means of CCTV will be in accordance with The Care Trust’s Data Retention Policy for all other documents.

**Direct Marketing**

Direct Marketing can be defined as communication addressed to an identifiable individual that is asking them to exchange something of value for potential benefit.

Under GDPR, direct marketing is defined as a ‘legitimate interest’ of a Data Controller. This means that The Care Trust may use personal data for direct marketing purposes, where specific regulations (EU Privacy Directives and Data Protection Acts) are met.

**Direct Marketing to Existing Supporters**

Under EU Privacy Directives, existing Supporters may receive marketing messages electronically (i.e., by emails/SMS) if:

* Data Protection rules were observed when sourcing data in the first place; The product / service being marketed is The Care Trust’s own product / service;
* The product / service marketed is similar to that originally bought; and Supporters consistently have the opportunity to refuse / opt – out.

The Care Trust will not use electronic mail/SMS to send a Supporter a message for a non-marketing purpose which includes direct marketing information without explicit consent.

Where The Care Trust uses electronic mail / SMS messages for direct marketing, the message will clearly state The Care Trust’s contact details and will provide a mechanism for recipients to respond and request a communication block. It is not required to provide a reason to cease communications. If a Supporter objects to receiving communications, this will be noted immediately by The Care Trust and they will not be contacted again.

The Care Trust understands that eMarketing consent has an expiry date of 12 months, after which time data cannot be used and must be deleted. That is, details must have been collected within the previous 12 months or the individual / Supporter has received a marketing electronic mail within the previous 12 months to which they did not unsubscribe, using the cost-free method provided.

**Direct Marketing to Potential Supporters Electronic Communications**

The Care Trust understands that individuals are only to be contacted by electronic mail / SMS messages to mobile phone for the purpose of direct marketing once their express prior consent has been obtained (i.e., the individual has ‘opted- in’). This consent can be withdrawn by the individual at any time.

**Other Communication Methods**

Individuals may be contacted by other means (e.g., post or phone call to a landline) without obtaining their consent beforehand once:

* Data Protection rules were observed when sourcing data in the first place;
* Individuals have not previously objected to the receipt of marketing communications by such means (i.e., they have not ‘opted out’), and
* Each time they are contacted they are given the opportunity to object to same in a cost-free easy manner, i.e., in the manner easiest for them.

If The Care Trust proposes to make unsolicited calls to individuals for marketing purposes, it is legally required to consult the Irish National Directory Database to ensure agreement.

**Data Breaches**

A Data Breach is the scenario in which a third party gains unauthorised access to data, including personal data. This can lead to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

The Care Trust will notify the Data Protection Commissioner of any data breaches without undue delay and within 72 hours of becoming aware of the breach. The only exemption to this mandatory obligation is where the breach is unlikely to result in a risk to the rights and freedoms of natural persons.

The Care Trust will also notify the Data Subjects affected of any data breaches where the breach is likely to result in a high risk to the Data Subject. This may not be necessary if the data has been rendered unintelligible by The Care Trust and / or subsequent measures have been taken to minimise the risk. Where this would involve disproportionate effort, public communication will be used instead.

Responsibility for reporting any such data breaches rests with the CEO of The Care Trust, acting in consultation with the SMT and the Board.

The Care Trust is committed to ensuring the implementation of appropriate technical and organisational measures to protect data or render it unintelligible to any unauthorized users. This includes pseudonymisation of data; ongoing vigilance around processing systems and services; a current Business Continuity Plan for the testing, accessing and evaluation of security measures. The Care Trust undertakes to maintain a record of any data breaches, including its effects and the remedial action taken.

**Use of Images by The Care Trust**

Any photograph, video or audio recording of a person constitutes their Personal Data and may, therefore, be subject to the provisions of the Data Protection Acts. Images created purely for personal use are exempt from the Data Protection Acts.

Photographs, videos or audio recordings taken of people for official use may be covered by the Data Protection Acts, and those people (and, where applicable, their parent/guardian) should be advised and consent sought.

Official Use of Images may include:

* Photographs of staff/stakeholders taken for identification purposes. These are likely to be stored electronically with other personal data and the terms of the Data Protection Acts apply.
* Photographs of staff/Supporters/stakeholders taken for public use e.g., for promotional purposes. These are likely to be stored electronically and shared with the public and the terms of the Data Protection Acts apply.

In all instances where a photograph is taken, or a video and/or audio recording is made for official use, the explicit and informed consent of the person (and, for minors, their parent/guardian) will be sought for its use or publication in any medium, e.g., website, annual report, newspaper advertisement.

Informed consent is a process whereby participants are informed and asked for agreement prior to their data (including images) being collected and used. The individual will be given any information required to ensure fairness and transparency. Informed consent includes providing the individual with the opportunity to withdraw consent previously given, if desired.

Consent will be obtained for each intended use of the images. Individuals should be informed of the purpose for which their data will be used and the bodies/people to whom the data might be transferred.

If it is intended to share the data with a third party (e.g., giving photo to a local newspaper) specific consent to transfer the image must be obtained in advance of any transfer. Consent can be written or verbal but must be recorded on The Care Trust’s systems.

Where photographs are stored by The Care Trust, they may be held on a computer system in line with the appropriate retention schedules per The Care Trust’s Data Retention Policy, after which they are deleted from the system.

**Stock Image**

The Care Trust may, from time to time, use stock images from authorised sources. In such instances, The Care Trust will abide by the terms of the licensing agreements in place.

**Contact Details**

Should there be any questions about data protection please contact: thecaretrust@give.ie. Our registered address is The Care Trust DAC, College House, 71-73, Rock Road, Blackrock Co. Dublin, A94 F9X9.

The Care Trust Charity Registration details are: The Care Trust Registered Charity Number: 20043285 CHY Number: 13691.

**Appendix 1: Definition of Terms**

| **Issue** | **The Directive** | **The GDPR** | **Impact** |
| --- | --- | --- | --- |
| **Personal data**EU data protection law only applies to personal data. Information that does not fall within the definition of “personal data” is not subject to EU data protection law. | **Art.2(a)**“Personal data” means any information relating to an identified or identifiable natural person (“data subject”); an **identifiable person is one who can be identified, directly or indirectly**, **in particular by reference to an identification number** or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. | **Art.4(1)**“Personal data” means any information relating to an identified or identifiable natural person (“data subject”); an **identifiable 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, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. | The definition of personal data is, for the most part, unchanged under GDPR.For some organisations, the explicit inclusion of location data, online identifiers and genetic data within the definition of "personal data" may result in additional compliance obligations (e.g., for online advertising businesses, many types of cookies become personal data under the GDPR, because those cookies constitute "online identifiers"). |
| **Sensitive Personal Data** Sensitive Personal Data are **special categories of personal data that are** | **Art.8(1)**“Sensitive Personal Data” are personal data revealing racial/ ethnic origin; political opinions; religious/philosophical beliefs; | **Rec.10, 34, 35, 51; Art.9(1)**“Sensitive Personal Data” are personal data, revealing racial/ ethnic origin; political opinions; religious/philosophical beliefs; | For most organisations, the concept of “Sensitive Personal Data” remains unchanged.For organisations that process genetic or biometric data, |

|  |  |  |  |
| --- | --- | --- | --- |
| **Issue** | **The Directive** | **The GDPR** | **Impact** |
| **subject to additional protections**.In general, organisations require stronger grounds to process Sensitive Personal Data than they require to process “regular” personal data. | trade-union membership; data concerning health or sex life. | trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data. Data relating to criminal offences and convictions are addressed separately. | those data are now expressly categorised as “Sensitive Personal Data”, and will therefore be subject to additional protections and restrictions. |
| **Anonymous data**Some sets of data can be **amended in such a way that no individuals can be identified from those data (whether directly or indirectly)** by any means. | **Rec.26**The Directive does not apply to data that are rendered anonymous in such a way that individuals cannot be identified from the data. | **Rec.26**The GDPR does not apply to data that are rendered anonymous in such a way that individuals cannot be identified from data. | Data that are fully anonymised (i.e., data from which no individuals can be identified) are outside the scope of both the Directive and the GDPR. |
| **Pseudonymous data** Some sets of data can be amended in such a way that no individuals can be identified from those data (whether directly or indirectly) without a “key” that allows the data to be re-identified. A | **N/A**The Directive does not explicitly address the issue of pseudonymous data. Pseudonymous data are treated as personal data. | **Rec.26, 28-29, 75, 78, 156; Art.4(5), 6(4)(e), 25(1), 32(1)(a), 40(2)(d), 89(1)**Pseudonymous data are **still treated as personal data because they enable the identification of individuals (albeit via a key).** However, provided that the “key” that enables re-identification of | Pseudonymisation of data provides advantages. It can allow organisations to satisfy their obligations of “privacy by design” and “privacy by default” and it may be used to justify processing that would otherwise be deemed "incompatible" with the |

|  |  |  |  |
| --- | --- | --- | --- |
| **Issue** | **The Directive** | **The GDPR** | **Impact** |
| good example of pseudonymous data is coded data sets used in clinical trials. |  | individuals is kept separate and secure, the risks associated with pseudonymous data are likely to be lower, and so the levels of protection required for those data are likely to be lower. | purposes for which the data were originally collected. In addition, the GDPR explicitly encourages organisations to consider pseudonymisation as a security measure. |
| **Processing**The term “processing” is very broad. It essentially means **anything that is done to, or with, personal data (including simply collecting, storing or deleting those data)**.This definition is significant as it clarifies that EU data protection law applies wherever an organisation does anything that involves or affects personal data. | **Art.2(b)**“Processing” means any operation or set of operations performed upon personal data, whether or not by automatic means**,** such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. | **Art.4(2)**“Processing” means **any operation or set of operations performed upon personal data or 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. | The GDPR introduces minor amendments to the wording of the definition of “processing”. These amendments are unlikely to make any practical difference to most organisations. |
| **Controller**Under the Directive, “Controller” has | **Art.2(d)**“Controller” means the natural or legal person, public authority, | **Art.4(7)**“Controller” means the natural or legal person, public authority, | The concept of a “controller” is essentially unchanged under the GDPR. Any entity that is a |

|  |  |  |  |
| --- | --- | --- | --- |
| **Issue** | **The Directive** | **The GDPR** | **Impact** |
| particular importance because compliance obligations under EU law are primarily imposed on controllers. Under GDPR, controllers still **bear the primary responsibility for compliance,** although processors also have compliance obligations. | agency or any 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 processing are determined by EU or Member State laws, the controller may be designated by those laws. | agency or any 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 processing are determined by EU or Member State laws, the controller (or the criteria for nominating the controller) may be designated by those laws. | controller under the Directive likely continues to be a controller under the GDPR. |
| **Processor**The term “processor” refers to any entity that processes personal data under the controller's instructions (e.g., many service providers are processors). | **Art.2(e)**“Processor” means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller. | **Art.4(8)**“Processor” means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller. | The concept of a “processor” does not change under the GDPR. Any entity that is a processor under the Directive likely continues to be a processor under the GDPR. |
| **Consent**The concept of “consent” is foundational to EU data protection law. In general, the validly obtained consent of the data subject will permit | **Art.2(h)**“The data subject's consent” means any freely given, specific and informed indication of his wishes by which the data subject signifies his agreement to personal | **Rec.25; Art.4(11)**“The consent of the data subject” means any **freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative** | The GDPR makes it considerably harder for organisations to obtain valid consent from data subjects. For organisations that rely on consent for their business activities, the processes by |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Issue** |  | **The Directive** |  |  | **The GDPR** |  | **Impact** |
| almost any | type of | data relating to | him being | **action,** | signifies agreement | to | which they obtain consent will |
| processing | activity, | processed. | personal data relating to them | need to | be | reviewed | and |
| including Cross-Border |  | being processed. | revised | to | meet | the |
| Data Transfers. |  |  | requirements of the GDPR. |
| **Data breaches** | **Art.17(1)** | **Art.4(12)** | Although the GDPR introduces |
| The term “data breach” is | “Data breach” is not specifically | “Data breach” means a breach of | a formal definition that is not |
| commonly used to refer | defined in the Directive; but Art. | security leading to the accidental or | provided in the Directive, the |
| to **the scenario in which a** | 17(1) obliges controllers to protect | unlawful | destruction, | loss, | concept of a data breach does |
| **third party** | **gains** | personal data | against | alteration, unauthorised disclosure | not materially change. |
| **unauthorised access to** | accidental/unlawful destruction, | of, or access to, personal data |  |
| **data,** including personal | loss, alteration, | unauthorised | transmitted, stored or otherwise |  |
| data. | disclosure/access, and all other | processed. |  |
|  | unlawful forms of processing. |  |  |
| **Relevant filing system** is any set of information that, while notcomputerised, is structured by reference to individuals, or by reference to criteria relating to individuals, so that specific information is accessible. |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Issue** | **The Directive** | **The GDPR** | **Impact** |
| **Redaction** is the separation of disclosable from non-disclosable information by blocking out individual words, sentences or paragraphs or the removal of whole pages or sections prior to the release of the document. |  |  |  |

**Appendix 2: The Care Trust Data Breach Plan**

A data breach is 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.

1. **Identify and classify the data breach**

Essential details will be recorded in writing:

* + - Date / Time breach occurred – can be approximate
		- Date / Time breach detected
		- The person reporting the breach and to whom it was reported
		- Description of the breach – as detailed as possible
		- Any IT systems involved

All data breaches should be immediately notified to a member of the SMT. Members of the SMT will ensure the Chief Executive (CEO) is notified immediately.

1. **Contain and recover the data breach**
	* CEO will appoint an Investigation Leader from SMT, depending on type of breach. E.g., hacking incident led by the Head of IT; loss of manual files by Dir of Finance & Admin.
	* Immediate action will be taken to minimise/recover losses, as advised by Investigation Leader.
	* The Investigation Leader will assign tasks to staff, with deadlines, and be responsible for ensuring actions and results are recorded.
2. **Assess the risks from the data breach**

From their investigative work, the SMT will assess and quantify the risks. This will include consideration of the type / nature of data breached and the security measures in place as well as the potential number of Supporters / individuals affected.

1. **Notify the relevant parties**

Using the decision tree provided and the time limits set out, notify relevant parties. If the Data Protection Commissioner (DPC) needs to be notified, use the webform at dataprotection.ie or the following details:

**E-Mail** - dpcbreaches@dataprotection.ie **Phone -** 1800 437737; 01 765 0100

Initial contact should only communicate the circumstances surrounding the incident. Do not include personal data in this initial communication.

If the DPC requires a detailed written report of the incident, they will specify a timeframe for this and may request the following information:

1. a chronology of the events leading up to the loss of control of the personal data;
2. amount and nature of the personal data that has been compromised
3. action being taken to secure and / or recover the compromised personal data;
4. action being taken to inform those affected or reasons for the decision not to do so;
5. the action being taken to limit damage or distress to those affected by the incident;
6. the measures being taken to prevent repetition of the incident.



