Adult Safeguarding Toolkit

Last Updated: July 2025

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Contents

Acknowledgements

The Data Protection Commission (DPC) wishes to thank the following who provided valuable assistance in the course of this project, including through written submissions, consultation meetings and discussions:

- SAGE Advocacy
- Fedvol Data Protection Network
- HIQA
- HSE National Safeguarding Office
- Safeguarding Ireland
- Decision Support Service
- National Rehabilitation Hospital
- Mental Health Commission
- Voluntary Hospital Forum

The DPC also wishes to thank those who are not named but who chose to share personal experiences related to adult safeguarding to inform this guidance document. The DPC remains fully responsible for the content of this guidance document.

Glossary of Abbreviations

The following abbreviations are used throughout this guidance:
AGS – An Garda Síochána
DPC – Data Protection Commission
DPIA – Data Protection Impact Assessment
DPO – Data Protection Officer
EEA – European Economic Area
EU – European Union
GDPR – General Data Protection Regulation
HIQA – Health Information and Quality Authority
HSE – Health Service Executive
LED – Law Enforcement Directive
MHC – Mental Health Commission
NVB – National Vetting Bureau
2018 Act – Data Protection Act 2018

Glossary of Terms

Term	Definition
At-Risk Adult	A person who, by reason of their physical or mental condition or other particular personal characteristics or family or life circumstance (whether permanent or otherwise), is in a vulnerable situation and/or at risk of harm and needs support to protect themselves from harm at a particular time. While not an exhaustive list, this can include individuals suffering from physical or mental conditions (such as cognitive impairment, dementia, acquired brain injury), children with additional needs reaching the age of majority, individuals subject to domestic violence or coercive control, individuals who find themselves homeless, individuals who are subject to financial abuse and individuals who have been trafficked.
Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
Capacity	A person's ability to understand when a decision is being made and the nature and consequences of that decision in the context of the available choices. This is based on the person's ability to make a specific decision about something, at a specific time. (This definition is in line with the definition of capacity as set out at section 3 of the Assisted Decision-Making (Capacity) Act 2015).
Consent	Some types of processing of personal data are done on the basis that the data subject has given their consent. Consent must be freely given, specific, informed and unambiguous.
CORU	The multi-profession health and social care regulator within Ireland. The role of CORU is to protect the public by promoting high standards of professional conduct, education, training and competence through statutory registration of health and social care professionals, including dietitians, occupational therapists, physical therapists, social workers, speech and language therapists and social care workers.

Data Protection Act 2018	The national law which gives further effect to the GDPR, transposes the LED into Irish law and which established the Data Protection Commission.
Data Controller	A person, company, or other body, which decides the purposes and means of processing personal data.
Data Protection Impact Assessment (DPIA)	An assessment carried out by a data controller of the impact of envisaged processing operations on the protection of personal data where those processing operations are likely to result in a high risk to the rights and freedoms of natural persons.
Data Subject	An identifiable natural living person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, an online identifier or to one or more factors specific to their physical, genetic, mental, economic, or social identity.
Data Subject Access Request (DSAR)	A request made by a data subject under Article 15 of the GDPR to obtain from a data controller access to their personal data.
European Economic Area (EEA)	An area of free trade and free movement of peoples comprising the member states of the European Union, in addition to Norway, Iceland and Liechtenstein.
General Data Protection Regulation (GDPR)	Lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. A principled piece of legislation which allows organisations of different sizes, and with different objectives, to decide on and devise their own processes and procedures, to meet their respective objectives, once there is adherence to the basic principles as set out in data protection law.
Health Data	Personal data relating to the physical or mental health of a person, including the provision of health care services.

Lawful Basis	One of six bases set out at Article 6(1) of the GDPR (consent, performance of a contract, legal obligation, vital interests, public interest, and legitimate interests). In short, the lawful reason for processing personal data.
Personal Data	Any information about a living person where that person is either identified or identifiable.
Processing	Doing something with the personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, consulting, using, disclosing by transmission, sharing/ making the data available, aligning or combining, restricting, erasing or destroying personal data.
Processor	A person, company, or other body which processes personal data on behalf of a data controller.
Profiling	Profiling is any kind of automated processing of personal data that involves analysing or predicting a person's behaviour, habits or interests.
Recipient	A person, public authority, agency, service or organisation to which personal data are disclosed.
Safeguarding	Measures put in place to uphold the rights of at-risk adults (including data protection rights), support their health and well-being, protect from harm and reduce risk of harm, and empower at-risk adults to protect themselves and their rights.

Relevant GDPR Articles (see link to full GDPR in "Appendix 4" on page 92)	
Article 4:	Explanation of the key terms in the GDPR
Article 5:	Basic principles relating to the processing of personal data
Article 6:	Legal bases for the processing of personal data
Article 7:	Conditions for consent
Article 9:	Processing of special category data
Article 10:	Processing of personal data relating to criminal convictions and offences
Articles 12-14:	Transparency of processing
Article 15:	Right of access by a data subject to their data
Article 16:	Right to rectification by a data subject of their data
Article 17:	Right to erasure by a data subject of their data ('right to be forgotten')
Article 18:	Right to restriction of processing by a data subject
Article 21:	Right to object to processing by a data subject
Article 23:	Restrictions on the exercise of data subject rights by a data controller

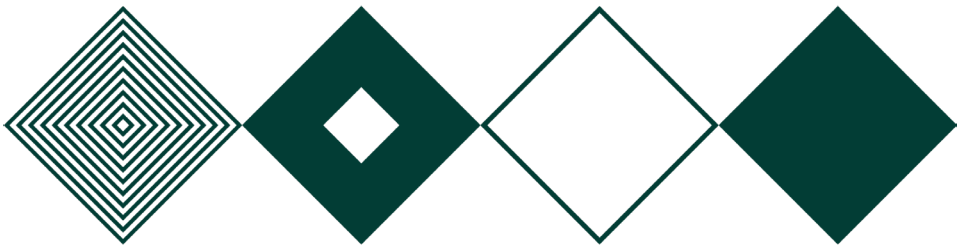
Article 24:	Responsibility of the data controller
Article 28:	Processors
Article 31:	Cooperation with the supervisory authority
Article 32:	Security of processing
Article 33:	Notification of a personal data breach to the supervisory authority
Article 34:	Communication of a personal data breach to the data subject
Article 35:	Data protection impact assessment (DPIA)
Articles 37-39:	Data Protection Officer (DPO)

Foreword

Many organisations engage with adults who are in vulnerable situations or at risk of harm by reason of their physical or mental condition or other particular personal characteristics or family or life circumstance ('at-risk adults'[1]). While not an exhaustive list, this can include individuals suffering from physical or mental conditions (such as cognitive impairment, dementia, acquired brain injury), children with additional needs reaching the age of majority, individuals subject to domestic violence or coercive control, individuals who find themselves homeless, individuals who are subject to financial abuse and individuals who have been trafficked.

Every individual has a fundamental right to protection in relation to the processing of their personal data. However, the right to protection of personal data is not an absolute right and must be balanced against other fundamental rights. In the context of safeguarding at-risk adults, organisations who engage with at-risk adults must ensure that they process the personal data of such individuals in line with data protection law. Processing activities include the sharing or dissemination of personal data to a third party. One of the reasons a data controller may not wish to share personal data is due to concerns arising from compliance with data protection law. However, as set out in this guidance, data protection law does not stand in the way of sharing data within the context of adult safeguarding; what data protection law requires is that the sharing is lawful, relevant, necessary and a proportionate measure for the achievement of the objectives of the data controller, such as the safeguarding of at-risk adults.

The purpose of this guidance document is to assist organisations whether large or small, public or private, or part of the voluntary or charitable sector, in their decision-making processes when processing the personal data of such individuals, given the many challenges they face.



1) The term 'at-risk adult' is used throughout this guidance document to refer to a variety of individuals who are in vulnerable situations or at risk of harm. In using the term 'at-risk adult' the DPC recognises that there are a wide variety of individuals in a variety of situations and circumstances (whether permanent or temporary) who may be at risk of harm at a particular time and require assistance from one or more organisations. The use of a single term to refer to this wide variety of individuals is for ease of the reader and is intended to aid the comprehension and application of the guidance herein.

Background to this Guidance

The Data Protection Commission's Regulatory Strategy 2022 – 2027 prioritises the protection of children and other vulnerable groups. In line with this priority, the DPC aims to ensure that organisations working with, supporting or otherwise engaging with at-risk adults have a better understanding of data protection rights and the legal bases upon which personal data can be shared.

To support this goal, the DPC has engaged with relevant stakeholders (including advocacy groups, service providers across the public, private, voluntary sectors, and other relevant regulatory bodies) in order to identify data protection issues arising in the context of adult safeguarding.

The DPC's overall aim is to foster a consistent approach to data protection across the wider sector, to promote equality, prevent discrimination and ensure that the data protection rights of vulnerable groups are given appropriate consideration.

'data protection law does not stand in the way of sharing data within the context of adult safeguarding; what data protection law requires is that the sharing is lawful, relevant, necessary and a proportionate measure for the achievement of the objectives of the data controller, such as the safeguarding of at-risk adults'

Guidance

Introduction

Individuals at various stages of their lives may find themselves in vulnerable situations, which may place them at risk of harm and in need of assistance from various organisations.[2]

When this happens, it is likely that the organisation will 'process' the individual's personal data for the purposes of providing assistance, advice or support to that person. Under data protection law, 'processing' personal data essentially means doing something with an individual's personal data, such as collecting, storing, sharing or using that data in some way. The entity or organisation is the data controller as they are deciding why and how they are going to process the personal data. Data subjects are individuals whose data is processed by the organisation.

Occasionally, it may be necessary for that original organisation to share that person's information with a third party. For example, this may be because there is an obligation under law to report a matter of concern to An Garda Síochána ('AGS') or it may be a safeguarding or welfare matter. Any sharing of personal data by the original organisation to a third party constitutes processing for the purposes of data protection law. This must be done lawfully.

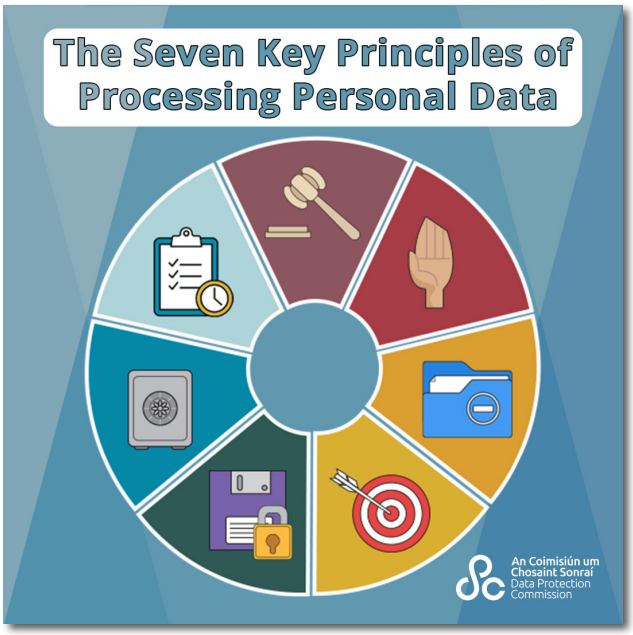
It is mandatory for any organisation or entity which processes personal data to be aware of their duties and obligations under data protection law, and this applies even if the entity is operating in a voluntary or charitable capacity. All data controllers are expected to devise, develop and continually review their data protection policies and practices which should be shared widely with all employees, volunteers and/or contractors engaged by them. This includes the provision of training on data protection law to employees, volunteers and/or contractors which then assists those individuals providing such assistance, advice or support at the 'coal-face' of the organisation in carrying out their roles.

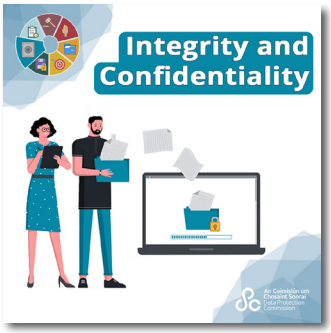
While it is not necessary for every organisation or entity to have a Data Protection Officer (DPO), it is advisable for each organisation, including those in the voluntary and charitable sector, to assign an individual to a data protection role. This person then serves as the first point of contact for both at-risk adults who may have queries in relation to the processing of their own data and it also serves as a point of contact for individuals who work at the 'coal-face' of the organisation who may have a query relating to data protection.

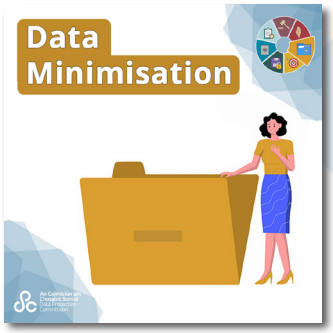
Where a DPO is appointed by an organisation, it is the responsibility of that organisation to ensure that the DPO is provided with the necessary resources to perform their tasks. The organisation should ensure that both at-risk adults and employees, volunteers and contractors are informed of their right to contact the DPO with regard to data protection issues and are provided with the contact details for the DPO. The DPO also acts as the contact point for the DPC on issues relating to the processing of personal data.

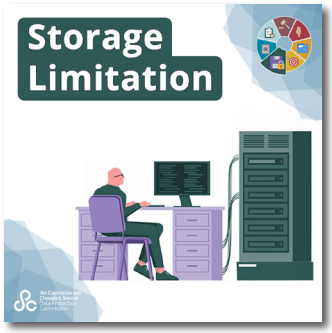
2) While not an exhaustive list, this can include individuals who suffer from a physical or mental health condition such as cognitive impairment, dementia, acquired brain injury or children reaching the age of majority born with additional needs. It can also include those subject to domestic violence, coercive control, any form of abuse including financial abuse, human trafficking or homelessness. The particular circumstances of an individual may be permanent or temporary.

The General Data Protection Regulation ('GDPR') is a principles-based piece of legislation which allows organisations of different sizes, and with different objectives, to decide on and devise their own processes and procedures, to meet their respective objectives, once there is adherence to the basic principles as set out in data protection law. While the practice of safeguarding itself lies outside of the remit of the DPC, the DPC recognises that nuances may arise when processing personal data for safeguarding purposes. Therefore, the primary purpose of this guidance document is to assist organisations who engage with at-risk adults in their decision-making processes (which includes understanding the need and importance in developing policies and procedures which underpin their objectives) regarding their data protection obligations.









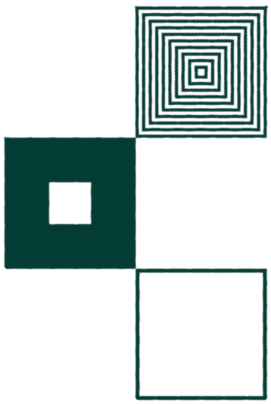
Basic Principles of Data Processing

Article 5 of the General Data Protection Regulation (GDPR) sets out key principles which lie at the heart of the data protection framework. These key principles are set out right at the beginning of the GDPR and they both directly and indirectly influence the other rules and obligations found throughout the legislation. Therefore, compliance with these fundamental principles of data protection is the first step for controllers in ensuring that they fulfil their obligations under the GDPR.

In processing personal data, data controllers must ensure personal data is:

- Processed lawfully, fairly and transparently;
- Processed for specific purposes;
- Limited to what is necessary;
- Kept accurate and up to date;
- Stored for no longer than necessary; and
- Protected against unauthorised or unlawful processing, accidental loss, destruction, or damage.

Controllers must also be able to demonstrate compliance with these principles, and must take responsibility for the processing of personal data.



Lawful Bases

It is important for data controllers to correctly identify their lawful basis for the processing of personal data. Without a lawful basis, there is no justification for its processing and the processing is therefore unlawful and in contravention of data protection law. Article 6 of the GDPR sets out a finite list of six lawful bases for the processing of personal data which are: consent, contract, legal obligation, vital interests, public task, or legitimate interests.

Therefore, one of the first key questions a data controller needs to ask themselves is: 'What is my reason or justification or objective for processing this personal data?' Once that is reflected and decided upon, the data controller must then consider which of the six lawful bases under Article 6(1) of the GDPR applies, if any. Each of the six lawful bases is set out and considered in more detail hereunder.

Concept of necessity

The concept of necessity means, if the data controller is able to fulfil their objective in a less intrusive manner other than by processing personal data, then that is what ought to be done, otherwise it is likely the processing will be considered unlawful.

Some of the key questions data controllers ought to ask themselves in advance of processing any of the data subject's personal data are:

- What is my objective?
- Do I need to process personal data at all to achieve this objective?
- Do I need to process this person's personal data?
- Is it absolutely necessary to process each piece of data I am requesting for the purposes of achieving the objective? Is there any personal data that is being requested that is not actually necessary in order for me to achieve my objective?
- Is there a less intrusive way in which I can achieve my objective without processing lots of personal data?
- What is the minimum data I require to achieve my objective?
- Is it reasonable for me to process this data? For example, if processing sensitive personal data or special category data?
- Is it proportionate for me to process this amount of data considering the objective being pursued?
- How can I ensure that the period for which I process this personal data is limited to a strict minimum considering the objective being pursued?

Article 6(1)(a): Consent

While Article 6 (1)(a) of the GDPR provides for the lawful basis of consent, Article 7 of the GDPR sets out the conditions for valid consent. The consent of the data subject is a choice they are exercising of their own free will. However, the data subject must be made aware of what they are consenting to and if that is unclear, or ambiguous, then the consent is unlikely to be valid consent.

Recital 32 of the GDPR also sets out that such consent must be an

> **'unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement'.**

Consent cannot be 'bundled'. This means that a data controller cannot use one consent agreement of the data subject to cover a host of other data processing activities. The data controller must ensure that it has explained each processing activity to the data subject and has obtained the data subject's consent for each separate processing activity. For example, if the data controller wishes to rely on the consent of the data subject to process their personal data for the provision of a health service and a financial service, then the data controller must ensure that it has obtained separate consent for each processing activity.

Data controllers, if relying on consent as a lawful basis to process personal data, must be able to show that the data subject has consented to the specific processing activity. This responsibility falls on the data controller and not on the data subject. Therefore, it would be appropriate for the data controller to have such consent in writing.

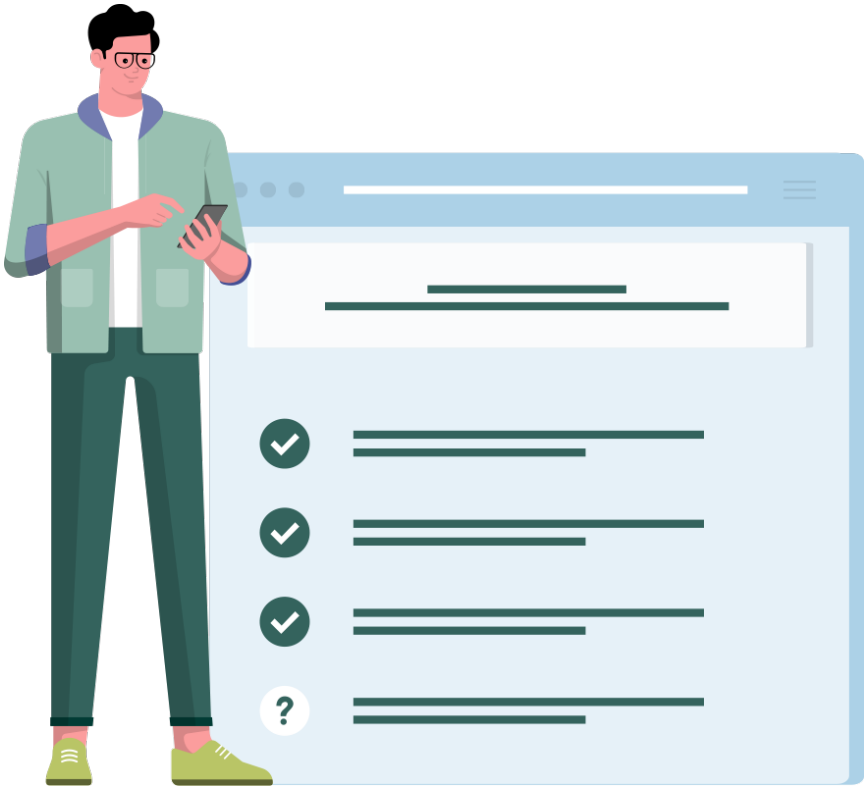
Relying on the consent of an individual who is in a vulnerable situation or at-risk of harm may be difficult. The question is whether they have the ability, at that point in time, to provide the data controller with valid consent, if they are in a vulnerable situation or at risk of harm and feel under pressure? But that is an assessment the data controller has to make and it may vary from case to case as each case is different and each set of facts is different.

Further, one of the difficulties with relying on consent as a lawful basis for the processing of personal data is that, consent can be withdrawn at any time. That does not mean that the processing carried out up to the time of the withdrawal of consent is invalidated, it is not – the processing which occurred up to that point remains lawful under the lawful basis of consent. It simply means that going forward, the data controller cannot rely on consent as its lawful basis.

So, even though it may be possible overall for a data controller to rely on consent as their lawful basis to process the personal data of a data subject, it might be prudent to consider relying on a different lawful basis if possible.

For consent to be valid, at a minimum the following ought to be included in a consent agreement form:

- The name of the data controller;
- What personal data is being processed;
- The processing activity being undertaken by the data controller;
- The purpose of each processing activity;
- The existence of the right to withdraw consent at any time;
- If there is going to be automated decision-making, the information in relation to this;
- If there is a risk that the personal data of the individual is going to be transferred out of the jurisdiction, then relevant information in relation to this; and,
- The consent agreement form should be signed by the data subject.



Article 6(1)(b): Performance of a contract

To rely on this lawful basis there must be an actual contractual relationship between the data subject and the data controller. Also, the processing must be necessary to perform the contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. Both the data controller and the data subject must be the parties to the contract in question. A controller cannot use a contract between themselves and another service provider as the lawful basis for the processing of a data subject's personal data, just because the processing would be necessary to perform that contract – as the data subject is not a party to that contract. Thus, this lawful basis would not apply in the absence of a direct contractual relationship with the data subject concerned.

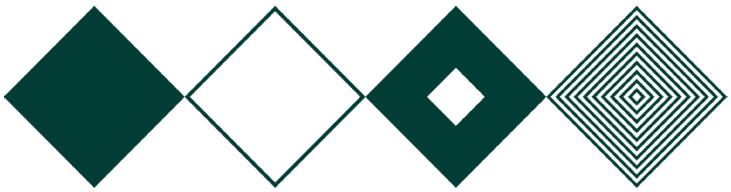
In some cases, written contractual terms may clearly specify that processing of personal data is required as an element of performance of the contract. However, it is not required for the purposes of Article 6(1)(b) that each granular processing operation must be specified in contractual terms. In many cases, processing which is necessary for the performance of a contract will not be expressly stated in contractual terms between the parties, and instead must be considered in the wider context of the agreement entered into, including an assessment of what is reasonably necessary in order to perform the underlying agreement.

This does not remove the controller's obligations regarding the principles of transparency, in particular under Article 13 of the GDPR, to ensure that the data subject is aware of both the types of processing operations and purposes of processing which will be undertaken with their personal data. This includes the express obligation under Article 13(2)(e) to provide information (at the time personal data are obtained from a data subject) on whether the provision of personal data is a contractual requirement.

Example

An individual is preparing to return to the work place after a long period of time, having been out of employment due to various difficulties. This individual contacts a service provider who provides training and workshops for such individuals. Having discussed a plan, both parties enter into a contractual arrangement for the service provider to provide a number of training sessions and a series of workshops tailored to the specific needs of the individual and the individual in return must attend all such sessions and receives a nominal payment.

As part of that contractual agreement, the service provider as data controller will have to process the personal data of the individual to give effect to the agreement in the contract. For example, the service provider is likely to have to process their name, address, minimal information relating to their skills (for the purposes of providing the training and workshops), bank account details and their PPSN. Under those circumstances, the service provider can rely on the lawful basis of contractual necessity.



Article 6(1)(c): Compliance with a legal obligation

It is important for data controllers to understand and have knowledge of the legislative framework within which they function and operate. This is because although organisations or entities as data controllers are subject to data protection law, they may also have other legal obligations under EU or Irish legislation, the common law or they may be subject to a court order. Where data controllers are processing personal data for the purposes of complying with a legal obligation, it is necessary for data controllers to specify which provision/legal obligation they are relying on.

In addition, to rely on the lawful basis of legal obligation a data controller must assess whether processing is actually 'necessary' in order to comply with that obligation. If data controllers can reasonably comply with their legal obligations without processing the personal data, then they cannot lawfully rely on this legal basis.

Example 1

Under the Criminal Justice (Withholding of Information on Offences against Children and Vulnerable Persons) Act 2012, as amended, section 3 provides for an offence of withholding information on certain offences against vulnerable persons. It sets out:

> 3(1): Subject to this section, a person shall be guilty of an offence if –
>
> a. He or she knows or believes that an offence, that is a Schedule 2 offence, has been committed by another person against a vulnerable person, and
>
> b. He or she has information which he or she knows or believes might be of material assistance in securing the apprehension, prosecution or conviction of that other person for that offence,
>
> and fails without reasonable excuse to disclose that information as soon as it is practicable to do so to a member of the Garda Síochána.

Schedule 2 sets out the relevant offences (such as false imprisonment, rape, sexual assault, human trafficking). So, under these provisions, an individual who has such information where an act, specifically provided for under Schedule 2 of that Act, was committed by one person against 'a vulnerable person', or they believe this to be the case, and which information could assist AGS in the 'apprehension, prosecution or conviction' of that person, that person has no option but to disclose that information to AGS. That person is mandated by law to make that disclosure and if they do not do so, they are at serious risk of being found guilty of a criminal offence. Insofar as data protection law applies, if that individual is a data controller, their lawful basis for the disclosure is Article 6(1)(c) of the GDPR as that disclosure is required and mandated by law.

Example 2

In general, compliance with a legal obligation will not be applicable as a legal basis to process personal data where a data controller has discretion as to whether or not to process personal data, or if there is another more reasonable and proportionate means to achieve the objective in question, without the use of personal data.

Occasionally, some statutory provisions may permit data controllers to exercise some level of discretion in relation to the data they process and in these instances, the data controller may be able to rely on Article 6(1)(c) of the GDPR for the lawfulness of such processing if the principles of Article 5 have been adhered to together with ensuring that any data processed is relevant, necessary and proportionate for the purposes of meeting the objective.

For example under S.I. No. 415/2013 – Health Act 2007 (Care and Welfare of Residents in Designated Centres for Older People) Regulations 2013, section 5 provides for the individual assessment and care plan. Section 5(5) provides:

> 'A care plan, or a revised care plan, prepared under this Regulation shall be available to the resident concerned and may, with the consent of that resident or where the person-in-charge considers it appropriate, be made available to his or her family'.

Let's assume that the data subject in this case is not in a position to consent to the sharing of the care plan. This provision offers an alternative to the 'person in charge' and permits them, if they deem it appropriate, to share the care plan with family members. In other words, they are exercising their discretion as to whether they will do so or not. To the extent that the care plan contains the personal data of the data subject, they may wish to consider various factors such as:

- What is the level of personal data contained within the care plan?
- Who is seeking access to this personal data?
- Are there concerns in relation to this family member who is seeking this data?
- What are those concerns?
- What is the detriment to the data subject if this care plan is shared with this family member?
- What is the benefit to the data subject if this care plan is shared with this family member?
- Are there any concerns if this family member had access to this personal data and if so, what are those concerns?

- Has the data controller, where possible, satisfied itself regarding the will and preferences of the data subject justifying the sharing of this personal data with this particular family member?
- Does any part of the personal data contained within the care plan require redaction? If so, why?

Finally, it must be noted that the exercise of the data controller's discretion against sharing care plans with family members must be for bona fide reasons only.

Note that the above is not an exhaustive list. Other factors may be required to be considered which will depend on the data controller and the nature of their engagement with the data subject.

Article 6(1)(d): Vital Interests

The processing of personal data for the purposes of vital interests arises mainly within the context of emergency situations. Data controllers must consider whether the processing is necessary to achieve the goal of protecting the vital interests of the data subject, such as someone's life or in mitigation against a serious threat to an individual, for example, in circumstances where they go missing.

Recital 46 of the GDPR further elaborates on the kinds of situations in which vital interests may apply, namely where it is 'necessary to protect an interest which is essential for the life of the data subject or that of another natural person' (i.e. a living individual). Thus, vital interests can be understood as interests essential for the life of a data subject – mainly covering life-threatening situations, but potentially situations which very seriously threaten the health or life of an individual.

Example 1

An individual in a residential facility collapsed and became unconscious. The staff called an ambulance to bring the data subject to hospital. As there was a serious concern for the life of that individual, the staff member disclosed some health data to the paramedics who recorded this information before leaving the residential facility.

It is likely that the lawful basis for the sharing of health data with paramedics in the circumstances outlined above would have a lawful basis under Article 6(1)(d) of the GDPR once the sharing of the data is necessary to protect the vital interests of the data subject.

Example 2

An individual in a residential unit went missing leading to concerns by the data controller for that person's safety and welfare. The data controller contacted AGS and disclosed some of that person's personal data to them, including the fact that the individual suffered from a mental health issue.

It is likely that the lawful basis for the sharing of health data with AGS in the circumstances outlined above would have a lawful basis under Article 6(1)(d) of the GDPR once the sharing of the data is necessary to protect the vital interests of the data subject.

Article 6(1)(e): Public Interest

This lawful basis is limited to data controllers where it is necessary for them to process personal data to carry out a task in the public interest, or exercise their official authority. This means that this provision will be relied upon mainly by public authorities. Article 6(3) of the GDPR sets out that where the processing is based on this lawful basis, the processing should be based on either EU law or national law. Therefore, a data controller can rely on this lawful basis if it is necessary for them to process the personal data in question, either in the exercise of their official authority (covering public functions and powers as set out in law) or to perform a specific task in the public interest (as set out in law). This lawful basis could potentially be relied upon by any controller which in some way exercises official authority or carries out a task in the public interest. The precise meaning of the term 'public interest' is largely dependent on the provisions of the specific piece of EU law or national law being relied upon as well as the circumstances of the particular case. It is not possible to cite in this guidance every example of legislation that refers to tasks or functions being carried out in the public interest or to provide a strict definition of the term 'public interest'. However, it is generally accepted that tasks carried out in the public interest relate not to a small self-determined group of individuals, but to a large section of the population.

Although the GDPR sets out that the relevant processing of personal data must be based on EU law or national law, this does not mean that there has to be a specific legal power; however, the underlying task, function or power of the data controller must have a clear basis in EU law or Irish law (this includes common law). That law should be clear and precise.

Examples of areas in which a task may be carried out in the public interest are given in Recital 45 of the GDPR, including health purposes such as public health and social protection and the management of health care services.

Example 1

The Health Service Executive ('HSE') is a public body established under the Health Act 2004, as amended ('2004 Act') and whose object and functions are set out under section 7 of that Act. Section 7(1) of the 2004 Act provides:

> '[t]he object of the Executive is to use the resources available to it in the most beneficial, effective and efficient manner to improve, promote and protect the health and welfare of the public'.

So the purpose of the HSE as an organisation is to benefit the public as its functions are to use its resources to improve, promote and protect the health and welfare of the public. This grounds the public interest lawful basis under Article 6(1)(e) of the GDPR.

Example 2

The Health and Social Care Professionals Act 2005 ('2005 Act') established CORU, which is made up of the Health and Social Care Professionals Council and Registration Boards for certain designated health and social care professions (for example, occupational therapists, social care workers, social workers). The 2005 Act provides for the registration of those 'designated professionals' and the determination of complaints relating to their fitness to practice.

Section 8(1) of the 2005 Act provides:

> 'The [Health and Social Care Professionals] Council shall do all things necessary and reasonable to further its object and shall exercise its powers and perform its functions **in the public interest**.' [emphasis added]

Sections 27 (1) and (2) of the 2005 Act provide:

> 'The object of the registration board of a designated profession is to protect the public by fostering high standards of professional conduct and professional education, training and competence among registrants of that profession.'
>
> 'A registration board shall do all things necessary and reasonable to further its object and shall exercise its powers and perform its functions **in the public interest**.' [emphasis added]

So the purpose of the Health and Social Care Professionals Council and the Registration Boards (e.g. the Social Care Workers Registration Board) is to benefit the public as their functions include, for example, enforcing standards of practice for registrants of the designated professions, including codes of professional conduct and ethics (section 8(2)(d)) and giving guidance to registrants concerning ethical conduct (section 27(3)(c)) and it is clearly stated in the 2005 Act that these functions are carried out in the public interest. This grounds the public interest lawful basis under Article 6(1)(e) of the GDPR.

However, controllers relying upon this lawful basis need to ensure that the processing of the personal data of the data subject must actually be necessary in order to carry out the task in the public interest or in the exercise of official authority. As is the case of other lawful bases which involve the concept of necessity, what precisely is 'necessary' to carry out the task in the public interest or in the exercise of official authority will ultimately depend on the circumstances of each case.

As public authorities have access to potentially very large amounts of personal data, it is imperative that they ensure both the type and amount of personal data processed are adequate, relevant and limited to what is necessary to achieve their objective.

Article 6(1)(f): Legitimate Interests

This lawful basis sets out that 'processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child'. This lawful basis carries increased obligations on controllers to balance the legitimate interests they are seeking to pursue with the rights and interests of the data subject.

There are three main elements to this lawful basis, all of which must be considered by the data controller.

a. Controllers must identify a legitimate interest which they or a third party wish to pursue;

b. Controllers must demonstrate that the intended processing of the data subject's personal data is necessary to achieve the legitimate interest; and

c. Controllers must balance their legitimate interest against the data subject's interests, rights, and freedoms.

Where a controller is considering processing personal data based on its legitimate interests, they should ensure that they have undertaken the balancing exercise between their interests and the rights/freedoms of the data subjects whose data they intend to process. They must be confident that the data subjects' interests do not override those legitimate interests and that the personal data are used in ways the data subject would reasonably expect – unless there is a very strong reason overriding these concerns.

Example 1

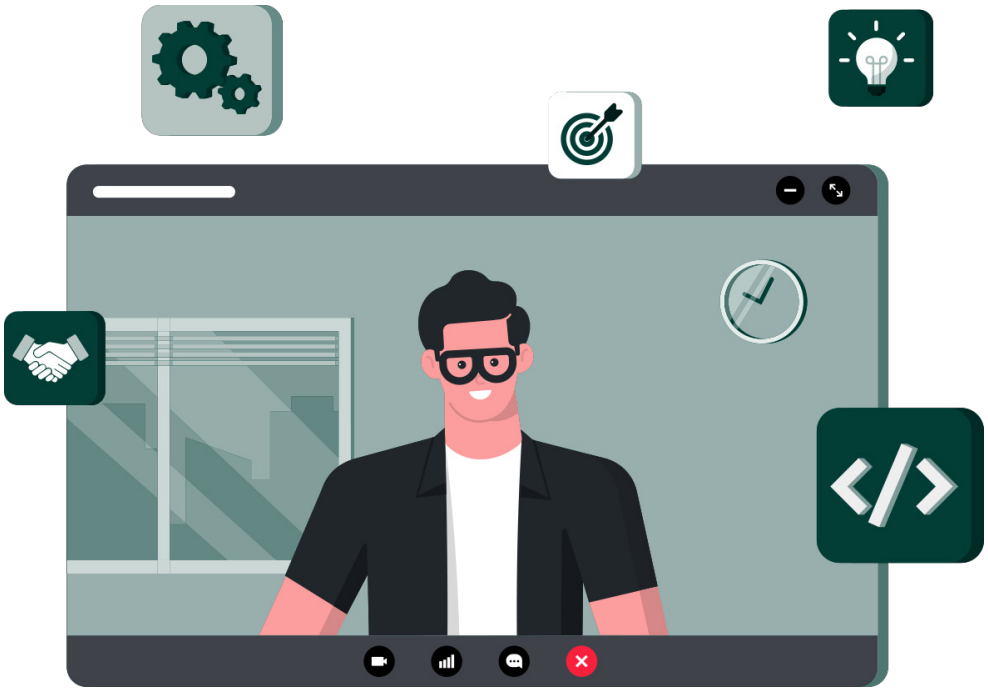
A private nursing home is considering installing CCTV cameras to protect the health and safety of residents and staff. Part of this consideration involves balancing the interests of the nursing home in maintaining a safe living environment and workplace, with the fair expectations of privacy of both residents and staff.

This assessment should address the areas that will be covered by CCTV, and ensure that cameras are not recording in areas where both residents and staff have reasonable expectations of privacy e.g. bedrooms, bathrooms, changing areas etc.

The purpose of this assessment is to establish whether the organisation can process personal data to achieve its legitimate goals without having a disproportionate impact on people.

In line with the principle of accountability under data protection law, controllers should keep a record of the assessment/balancing exercise they undertook to determine whether the legitimate interests were overridden by the interests, rights, or freedoms of the data subject. There is no set way in which controllers are required to do this, but it is important that they record their reasoning in some way, to show that an appropriate decision-making process was utilised to justify processing, and that data subject rights and freedoms were sufficiently taken into account. This is further considered in "Appendix 1" on page 68 of this guidance document.

Finally, it must be noted that public authorities cannot rely on the lawful basis of 'legitimate interests' to justify the processing of personal data, which is carried out in the performance of their tasks. Therefore, public authorities need to understand what personal data they are processing and for what purpose. If the data is being processed on the basis of a task in the public interest or the exercise of official authority, then they cannot rely on the lawful basis of legitimate interests. If the processing of personal data is not on the basis of a task in the public interest or in the exercise of official authority, then they may be able to rely on the lawful basis of legitimate interests.



Article 9

Article 9 of the GDPR prohibits the processing of special categories of personal data unless it falls into one of the exceptions permitted under Article 9(2). Special category data is personal data:

> **'revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation'.**

This is a finite list. For example, individuals often refer to their finances or taxes as being sensitive data. While it may very well constitute 'sensitive data' in the normal sense of the word, financial data is not special category data as defined under Article 9 of the GDPR.

Therefore, data controllers and individuals working with at-risk adults need to be aware as to what constitutes special category data; the reason being, the starting position is that this data is prohibited from processing, unless one of the exceptions under Article 9(2) applies. It is likely that organisations or entities who engage with at-risk adults will, at some stage during the course of their engagement with those at-risk adults, need to process their health data or perhaps other special category data. This arises as a result of the nature of the individual's needs and safeguarding requirements and the organisation's function and role in the provision of services or care to that individual.

For the processing of special category data to be lawful, data controllers must have a lawful basis under Article 6 of the GDPR in the first instance and they must also be able to demonstrate reliance on one of the permitted exceptions under Article 9(2) of the GDPR.

Article 9(2)(c) of the GDPR provides that processing is lawful where the:

> **'processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent'.**

Similar to the example above (see 'vital interests'), an individual in a specialised mental health residential facility collapsed and became unconscious. The staff called an ambulance to bring the data subject to hospital. As there was a serious concern for the life of that individual, the staff member disclosed some health data to the paramedics who recorded this information before leaving the residential facility.

It is likely that the lawful basis for the sharing of health data with paramedics in this scenario would have a lawful basis under Article 6(1)(d) of the GDPR once the sharing of the data is necessary to protect the vital interests of the data subject. However, as this is special category data under Article 9 of the GDPR, the data controller must also fall into one of the exceptions provided for under Article 9(2) of the GDPR. It is likely that Article 9(2)(c) of the GDPR could be lawfully relied upon in these circumstances, because the individual is not capable of providing consent due to being unconscious, or incapacitated.

Other exceptions that are sometimes relied upon by public bodies are Articles 9(2)(f), (g) and (h) of the GDPR.

Article 9(2)(f) of the GDPR provides that the processing of special category data is lawful where the:

> **'processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity'.**

For example, if a data controller is being sued, it is entitled to defend that legal claim. Under those circumstances, Article 9(2)(f) provides that data controller with a lawful basis for the processing of special category data for the purposes of those court or judicial proceedings.

Article 9(2)(g) of the GDPR provides that the processing of special category data is lawful where the

> **'processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject'.**

It is important to note the phrase '**substantial** public interest' which must be set out in EU or national laws. This means that the public interest itself must be substantial.

Recital 46 of the GDPR refers to certain data processing examples on the basis of public interests as:

> **'processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters.'**

In practical terms what does this mean for data controllers? This would indicate that the threshold is high for data controllers seeking to rely on this lawful basis and that they would need to demonstrate that there is not just a public interest, but that it is one that is 'substantial' and set out in law.

Article 9(2)(h) of the GDPR provides that the processing of special category data is lawful where:

> **'processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3'.**

This exception is for medical and social care purposes only.

Medical: This provision permits data controllers to process personal data for the purposes of health care, including diagnosis, treatment and prevention. However, the processing must be carried out by a professional who is bound by 'professional secrecy' under law (or certain rules) (by Article 9(3)).

This provides professionals within the health care sector such as (but not limited to) doctors, consultants, dentists or psychologists to process the health data of their clients, where they are under a duty of confidentiality.

Social Care: This covers assistance granted by social security authorities. For example, it may be necessary to process the personal data of an individual for the provision of emergency accommodation. Let's say an individual has specific medical needs and requires wheelchair access or needs to have various electrical outlets to support a dialysis machine or a breathing apparatus, it is likely that whichever data controller is processing that person's application for housing or some sort of accommodation would need to know this information to ensure that the individual is housed appropriately.

Article 10 and the processing of personal data relating to criminal convictions and offences

Organisations working with at-risk adults may, on occasion, have cause to be concerned regarding criminal convictions and offences or allegations of same. Such information is personal data and if the organisation or entity is going to use that information in some way, they must do so lawfully and in compliance with data protection law.

Article 10 of the GDPR provides for the processing of personal data relating to criminal convictions and offences; however, such processing can only be carried out in the following circumstances:

- ✓ **Where such processing is under the control of official authority or**
- ✓ **When the processing is specifically authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. and**
- ✓ **Any comprehensive register of criminal convictions shall only be kept under the control of official authority.**

Essentially, Article 10 of the GDPR provides for the processing of personal data by 'official authorities', which are public authorities. This includes bodies such as AGS (where the Law Enforcement Directive does not apply). Private entities or companies are not 'official authorities' and therefore cannot process this data, unless there are provisions for them to do so under either EU or national law.

Section 55 of the Data Protection Act 2018 gives further effect to Article 10 of the GDPR in Irish law and it also extends the scope of Article 10 of the GDPR in two ways in particular:

First, section 55(9) of the Data Protection Act 2018 provides that 'Article 10 data' includes 'personal data relating to the alleged commission of an offence and any proceedings in relation to such an offence'. Therefore, this broadens the base for 'Article 10 data' to include allegations of offences as opposed to just the offences themselves. This is an important distinction, as it requires data controllers to afford the same consideration to information and personal data about allegations of criminal convictions and offences, as to information about actual convictions and offences.

Second, section 55(1) of the Data Protection Act 2018 provides that 'Article 10 data' may be processed

a. 'under the control of official authority or

b. where –

(iv) processing is necessary to prevent injury or other damage to the data subject or another person or loss in respect of, or damage to, property or otherwise to protect the vital interests of the data subject or another person.'

So this means that organisations other than 'official authorities' can process such personal data, including relating to the alleged commission of an offence, for the purposes set out under section 55(1)(b)(iv) of the Data Protection Act 2018.

Section 55 of the Data Protection Act 2018 does not set out that an allegation must be reported to an official authority, such as AGS, in order for the data to be processed by an organisation which came to be informed themselves of an allegation. However, any processing of personal data of this nature must be processed with extreme care by the entity or organisation, in particular where the matter is an allegation. Aside from the general data protection compliance principles, in terms of processing such data, there are three main requirements which must be adhered to by data controllers: they relate to lawful bases, safeguards and the principle of necessity.

1. **Lawful Basis:** This means that data controllers must have a lawful basis under Article 6(1) of the GDPR for the processing of this data (section 55 does not provide a standalone legal basis for processing personal data by itself):

Example

While each data controller will have to determine their own lawful basis in line with the relevant set of facts and their objectives:

Care providers in the public sector are likely to rely on Article 6(1)(e) as part of their tasks carried out in the public interest, however a specific legislative provision should be identified which assigns the controller with the task or function concerned.

Private care providers should consider whether Article 6(1)(f) may be applicable, where processing is necessary for a specific legitimate interest i.e. the care and treatment of other residents.

Article 6(1)(d) may provide a lawful basis, where processing is necessary for the protection of the vital interests of the data subject or another person. However, It should be noted that Article 6(1)(d) refers only to those situations where immediate risk to a person's vital interests is present - a life or death situation - and outside of these rare, limited circumstances does not present a suitable lawful basis in most cases of safeguarding concerns.

2. **Safeguards:** The implementation of suitable and specific measures to safeguard the fundamental rights and freedoms of the data subject: this means that it will be necessary to put in place safeguards when processing Article 10 data to protect the person in question, recognising the sensitivity of the data and the possible consequences of inappropriate processing.

Section 36(1) of the Data Protection Act 2018 provides a non-exhaustive list of such safeguards, which should be considered in this context. Of particular relevance would be:

- Limitations on access to the personal data undergoing processing within a workplace in order to prevent unauthorised consultation, alteration, disclosure or erasure of personal data;
- Specific targeted training for those involved in processing operations;
- Logging mechanisms to permit verification of whether and by whom the personal data have been consulted, altered, disclosed or erased;
- Encryption of the personal data.

3. **Necessity:** necessary to prevent injury or other damage to the data subject or another person or loss in respect of, or damage to, property or otherwise to protect the vital interests of the data subject or another person: this element contains the crucial determination that the processing of Article 10 data is strictly necessary in order to prevent harm to a person.

This determination should be based on an evidential and fact-based assessment of the risk presented to an identified person or persons by the data subject in question.

Section 55(1)(b)(iv) should only be applied on a limited and case-by-case basis. That said, it should be noted that the harms set out under this section are broad in scope.

Going through these elements, or steps, in a decision-making process should enable a data controller to determine whether the processing of personal data relating to criminal convictions, offences, or alleged offences will be permissible in a particular context. For accountability purposes, all steps in this decision-making process should be clearly documented by the organisation.

Section 41 of the Data Protection Act 2018

Section 41 of the Data Protection Act 2018 (the '2018 Act') provides for 'the processing of personal data for a purpose other than the purpose for which the data has been collected'. Section 41 of the 2018 Act states that a purpose other than the purpose for which the data has been collected shall be lawful to the extent that such processing is necessary and proportionate for the purposes—

> **'(a) of preventing a threat to national security, defence or public security,**
>
> **(b) of preventing, detecting, investigating or prosecuting criminal offences, or**
>
> **(c) set out in paragraph (a) or (b) of section 47'.**

Section 47 of the 2018 Act provides for 'Processing of special categories of personal data for purpose of legal advice and legal proceedings'.

DPC Department of Health Inquiry 2023

In June 2023, the DPC issued its Decision on its Inquiry concerning the Department of Health (the 'Department'). The DPC's inquiry was commenced following public allegations in 2021 that the Department had unlawfully collected and processed personal data about plaintiffs and their families in special educational needs litigation. **More information regarding the Decision of the Inquiry can be found on our website.**

What is important to note here is the application of Section 41(b) of the 2018 Act and the EU law principles of necessity and proportionality. The DPC found that the Department did not infringe data protection law by seeking information about the services that were being provided to plaintiffs in relation to cases where there was open litigation. However, the DPC found the Department did infringe data protection law by asking broad questions that resulted in the provision of sensitive information about the private lives of plaintiffs and their families. This information included details about plaintiffs' jobs and living circumstances, information about their parents' marital difficulties and in one case, information received directly from a doctor about the services that were being provided to the plaintiff.

The DPC found that the processing of information obtained in response to broad scoping questions sent to the HSE for the purposes of seeking to settle a case was excessive and disproportionate to the aims pursued by the Department and that the processing for this reason was not necessary for the purposes of litigation. Therefore the DPC found that there was no lawful basis for this processing in the files examined, and that the Department had infringed the principle of data minimisation by processing this personal data.

While the DPC noted in its decision that Section 41 of the 2018 Act allows for the re-purposing of personal data where it is 'necessary and proportionate' for the purposes of legal advice, claims and proceedings, Article 6(4) of the GDPR takes supremacy over Irish law, and the compatibility test must apply equally when controllers seek to rely on section 41. The analysis of necessity and proportionality applies equally to the application of section 41 of the 2018 Act.

Data Subject Rights

Introduction

Individuals are data subjects for the purposes of data protection law and all data subjects have rights under Articles 12-22 and Article 34 of the GDPR. However, no right is absolute, which means that, while an individual can exercise their rights, restrictions may also be applied to their rights by data controllers. Recital 4 of the GDPR states that,

> **'[t]he right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.'**

In the context of adult safeguarding, the fundamental rights of all individuals, including their rights to life, protection from harm, dignity, and personal/bodily integrity, should be balanced appropriately with competing considerations around the right to the protection of personal data.

The circumstances of an individual, does not alter their entitlement to their data protection rights. Regardless of their living situation, their knowledge of their own rights, their ability to exercise these rights, or the restrictions that can be lawfully imposed on their rights, at-risk adults remain at all times entitled to have their rights upheld.

Exercise of Rights

Data protection rights are personal to and, in most circumstances, exercised by individuals themselves. In the normal course of events, if an individual wishes to exercise their data protection rights, they must contact the relevant data controller, setting out which data protection right they wish to exercise, or simply setting out their data protection concern.

While such requests/queries will often be directed to the DPO (or designated person for data protection queries) of the organisation, sometimes data subjects may send the request to the individual they happen to be dealing with, or they may send their request/query to a customer service representative. In those circumstances, those individuals who receive those requests are expected to be trained sufficiently in data protection law by their organisation to recognise that this is a request/query that ought to be sent immediately to the DPO/designated individual for data protection queries of the organisation so that they can respond within the designated time frame set out under Article 12 of the GDPR and deal with the matter expeditiously.

Data controllers providing services to or engaging with at-risk adults should be cognisant that those individuals may not necessarily be aware of the exact data protection right they wish to exercise or necessarily raise their concern in a way that immediately identifies a data protection issue. As such, it is important that organisations prioritise staff data protection training and data protection awareness

throughout the organisation. Furthermore, the DPC recognises that not all organisations engaging with at-risk adults have sufficient staff numbers or capacity to appoint a DPO or designated person for data protection, and, again, this emphasises the need for all staff in the organisation (however small) to be trained sufficiently in data protection by their organisation so that any requests or concerns raised can be recognised and responded to expeditiously by the organisation.

Data controllers must respond to those seeking to exercise their Right of Access, without undue delay and within one month from the date of receipt of the request. Even if a data subject has a data protection query, not necessarily related to the exercise of a right, the data controller should also respond as soon as is reasonably possible. It is also advisable that the data controller responds in writing and it is expected by the DPC that an appropriately detailed response is provided by the data controller to the data subject.

In the first instance, a data subject must exercise their own rights with the data controller prior to engaging the assistance of the DPC. If a data subject believes that their request has not been adequately dealt with, they can make a complaint to the DPC, setting out the basis of their complaint, and providing the DPC with copies of the correspondence exchanged between the data subject and the data controller and the DPC will assess the matter.

Assisted Decision-Making (Capacity) Act 2015

Issues can sometimes arise regarding the exercise of one's data protection rights where that individual lacks capacity in some way and is therefore unable to exercise their own data protection rights. The Assisted Decision-Making (Capacity) Act 2015 ('2015 Act'), as amended, provides some mechanisms which may assist data subjects in the exercise of their rights, including the exercise of their data protection rights.

The 2015 Act, which came into effect on 26 April 2023, provides a legal mechanism for supported decision-making. It adopts a tiered approach to capacity and provides for the will and preferences of the individual as opposed to what is in their best interests. Aside from providing for a functional test for the assessment of capacity, some of the main provisions relate to:

- Decision-making assistance agreements;
- Co-decision-making agreements;
- Decision-making representative orders.

Should any such arrangement be in place for a data subject, it would be expected that those assisting an individual must ensure that the arrangement in place provides them with the authorisation to assist the individual with their data protection concerns. In the absence of same, the data controller can then carry out a risk-based assessment and this is discussed further below.

Articles 12-14: Transparency of Processing

There is an obligation on data controllers to be transparent when processing personal data. What this means is that individuals are entitled to know, amongst other things, who is processing their data, how their data is being processed, with whom their data is being shared and the lawful basis for each of these processing activities. Data controllers tend to fulfil their transparency obligations by way of publication of a Privacy Policy or Privacy Statement/Notice or Data Protection Statement on their website. These Policies/Statements ought to clearly set out the contact details of the DPO (or the individual to whom data protection queries can be directed). This applies to all organisations including those in the voluntary or charity sector. (Further information on preparing a Privacy Policy can be found in "Appendix 2" on page 72.)

Article 12(3) of the GDPR provides that any request made to the data controller regarding the exercise of one's data protection rights (under Articles 15 to 22) must be responded to within one month of receipt of the request. In very limited circumstances, the data controller can extend the time within which to respond by up to two further months but must inform the data subject before the expiry of the one month time frame that an extension of time is required, setting out the reasons why.

Article 15: Right of Access by the Data Subject

Article 15 of the GDPR provides data subjects with the right of access to specific information about the processing of their personal data and it also provides data subjects with the right to obtain a copy of their personal data. Where an individual requests access to their personal data, any sensitive information, including Article 9 and 10 data, should be considered within the scope of the request.

It should also be noted that information about safeguarding may constitute either health data or social work data of the data subject. In this case, the organisation should make an assessment as to whether granting access to the data would be likely to cause serious harm to the physical or mental health of the data subject, or their emotional condition. Access to this type of data is governed by the Data Protection Act 2018 (Access Modification) (Health) Regulations 2022 (S.I. No. 121/2022) and the Data Protection (Access Modification) (Social Work) Regulations, 1989 (S.I. No. 83/1989). Safeguarding organisations should familiarise themselves with these regulations to ensure that personal data access requests are handled appropriately.

For more information please see the DPC's guidance, Subject Access Requests: A Data Controller's Guide.

Article 16: Right to Rectification

This Article provides for the correction of inaccurate data that is being processed by the data controller. For the purposes of the GDPR, personal data is inaccurate if it is incorrect as to a matter of fact. This ties in with the Article 5(1)(d) principle of 'accuracy' whereby data must be kept accurate and up to date.

Article 16 of the GDPR essentially provides for two things:

1. That the data subject shall have the right to obtain from the data controller without undue delay the rectification of inaccurate personal data. For example, if the data subject's name, address or date of birth is incorrect, then it ought to be corrected;

2. Taking into account the purposes of processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement. If for example, a service user is dissatisfied with a medical opinion and wishes to have that rectified, that is unlikely to happen, the reason being, a medical opinion is a clinical opinion and the circumstances under which this can be rectified will be very limited, if at all; however, if an individual disagrees with the medical opinion on their file, that disagreement can be noted by way of supplementary statement on their file. Further guidance on the rectification (and erasure) of medical records can be found on our website.

Article 17: Right to Erasure ('right to be forgotten')

This Article provides for the right of the data subject to obtain from the data controller the erasure of their personal data in certain circumstances. Article 17(1) of the GDPR sets out the bases upon which data can be erased if one of the following grounds apply:

1. Where your personal data are no longer necessary in relation to the purposes for which they were collected or processed.

2. Where you withdraw your consent to the processing and there is no other lawful basis for processing the data.

3. Where you object to the processing and there is no overriding legitimate grounds for continuing the processing (see exceptions under Article 17(3), set out below).

4. Where you object to the processing and your personal data are being processed for direct marketing purposes.

5. Where your personal data have been unlawfully processed.

6. Where your personal data have to be erased in order to comply with a legal obligation under EU or national law.

7. Where your personal data have been collected in relation to the offer of information society services (e.g. social media) to a child.

There are certain circumstances under which the right to be forgotten will not apply and they are set out under Article 17(3) of the GDPR:

- Exercising the right of freedom of expression and information.

- Compliance with a legal obligation required under EU or national law or the performance of a task carried out in the public interest or in the exercise of official authority.

- Reasons of public interest in the area of public health (See Article 9(2)(h) & (i) and Article 9(3), GDPR).

- Archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

- Establishment, exercise or defence of legal claims.

Restrictions on rights

The right to data protection is not an absolute right. It must always be balanced against other values, fundamental rights, human rights, or public and private interests and there may be circumstances under which an organisation may have grounds to refuse to grant an individual's request to exercise their data protection rights.

There are certain limitations contained within the data protection rights set out under the GDPR. For example, your right to access your data should not adversely affect the rights and freedoms of others under Article 15(4) of the GDPR. Certain data protection rights only apply in certain circumstances. The right to erasure ('right to be forgotten'), for instance, only applies under certain conditions, such as the personal data no longer being required for the purpose it was collected. In certain very limited cases the GDPR allows organisations to charge a reasonable fee for responding to a request, or even to refuse to act on a request, if the request is manifestly unfounded or excessive.

The GDPR allows for **further restrictions** on data protection rights in national law, but these restrictions must adhere to an exhaustive list of requirements, respect the essence of the fundamental rights and freedoms of individuals, and be necessary and proportionate to safeguard certain objectives of societal or general public interest. Some of the restrictions contained in the Data Protection Act 2018 relate to processing carried out for the exercise or defence of legal claims, and personal data relating to an opinion given in confidence.

For example, under Article 15 of the GDPR, a data subject has a right to obtain from a data controller access to personal data concerning him or her, which are being processed. The data controller must respond to a data subject access request without undue delay and in any event within one month of receipt of the request. However, section 60(3)(b) of the Data Protection Act 2018 provides that the right of access to personal data does not extend to data which consist of the expression of opinion about the data subject by another person given in confidence, or on the understanding that it would be treated as confidential to a person who has a legitimate interest in receiving the information.

- This exemption does not extend to information that is factual in nature, it just extends to the part of the information that is an expression of an opinion;
- A data controller must ensure they have a solid basis for such an assertion to rely on this exemption;
- The fact that an opinion given in confidence might attract this exemption does not mean that the other personal data contained in that same document is similarly exempt from the right of access;
- The data controller can only redact the part of the data to which the exemption validly applies;

- Information that is simply confidential is not exempt from an access request and the data controller cannot rely on this exemption which is for an opinion given in confidence;

- An opinion given in confidence on the understanding that it will be kept confidential must satisfy a high threshold of confidentiality;

- Simply placing the word 'confidential' at the top of a page, will not automatically render the document confidential.

In any case, an organisation must always respond to a data protection request within one month, even if they believe they have grounds to refuse it. Where an organisation refuses or partly refuses a request, their response must set out clearly which limitation or restriction they are relying on to refuse to act on the request, their reasons for not taking action, and must inform the individual of their right to lodge a complaint with the DPC or seek a judicial remedy.

Sharing of Data

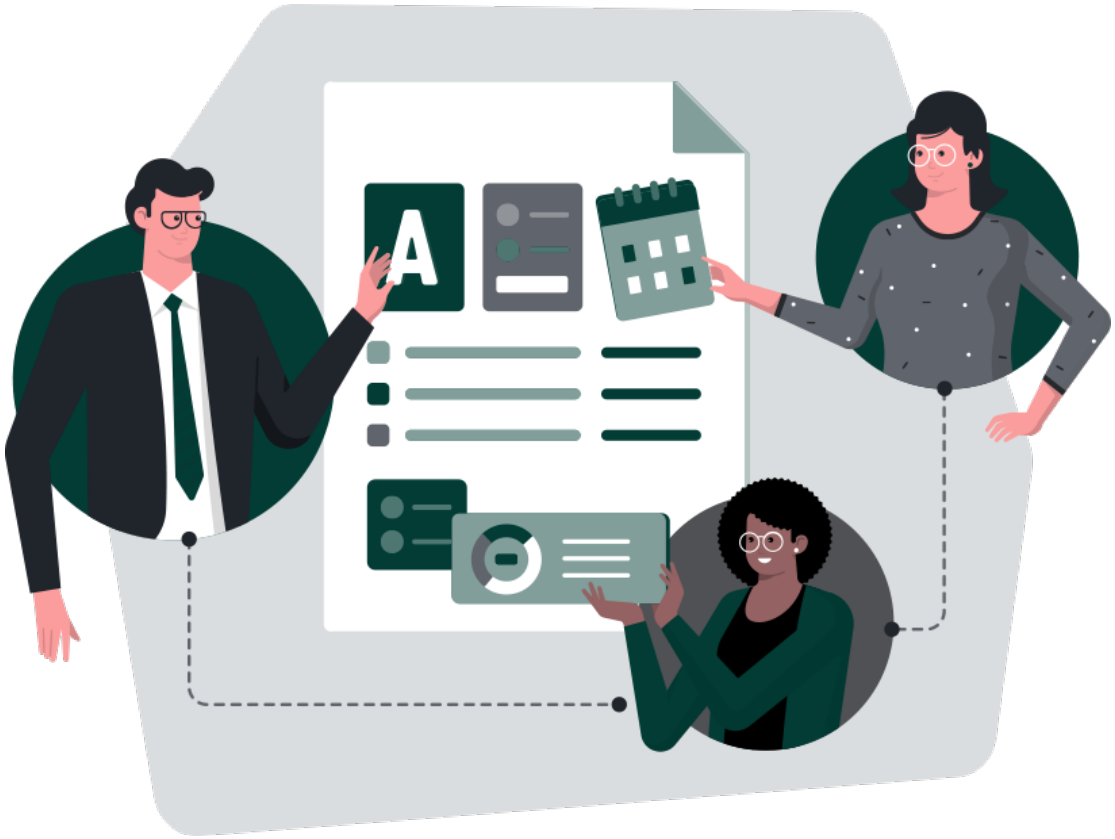
Introduction

It is important to note that the context within which adult safeguarding issues arise is extensive and there is no finite list of scenarios that will address all those circumstances; therefore there is 'no one size fits all' answer as to how and when personal data may be shared between organisations. What this means is that any sharing of data with a third party constitutes processing for the purposes of data protection law and such processing must be in line with established principles under the GDPR. Therefore, before any sharing of personal data takes place, it is incumbent on data controllers to consider the basic and first principles of the GDPR which will inform their decision-making processes.

Aside from full compliance with the principles as set out in Article 5 of the GDPR considered above, all processing activities must have a lawful basis under Article 6 of the GDPR. If there is processing of special category data, such processing must also fall into one of the permitted exceptions under Article 9(2) of the GDPR to be lawful. Sometimes, within the safeguarding context, a situation might arise necessitating further processing of data, which was not foreseeable when the lawful basis for the initial processing of personal data was decided. For example, a data controller may come into possession of some information about a vulnerable adult that affects their relationship and engagement with that person, and they may need to share data with a third party. This may involve the sharing of personal data, special category data or data that might be considered 'high-risk' information, such as a criminal conviction or an allegation of a criminal nature. If this arises, data controllers need to examine their lawful basis for this new processing act, the sharing of data with a third party. The data controller will need to consider whether the sharing of the data, as an act of processing, is compatible with the current lawful basis and if not, they may require a separate lawful basis for the sharing of that data. Note that Article 5(1)(b) states that personal data shall be:

> **'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes'**

Data controllers may be concerned that they do not have the consent of the data subject to share their data with a third party. However, as set out above, consent is only one lawful basis and data controllers may be in a position to rely on one of the other lawful bases negating the need to rely on consent in the first instance. Data controllers may be able to rely on the lawful basis of public interest or legitimate interest; however, in doing so, data controllers must ensure that they are validly relying on this basis and must also be in a position to demonstrate how and why that lawful basis applies.



Considerations for data controllers before sharing data:

Data controllers should consider the following points each time they are contemplating sharing personal data with a third party as each situation is likely to be different. Note that this is not an exhaustive list of considerations:

Do I have a lawful basis under Article 6 for the sharing of this data?

Do I have a lawful basis under Article 9 for the sharing of this data (if required)?

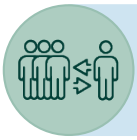
Is the data I wish to share Article 10 data?

Is it necessary to share this information?

Is the data I am proposing to share relevant to the concern?

Is the amount of data that I am proposing to share proportionate to the aim/objective I am seeking to achieve?

With whom am I sharing this information?



Will the third party share this information with anyone?

I must ensure the data is secure: by what mechanism is it being transmitted?

Can I share the information on an anonymised basis and still achieve the stated objective?

Have I carried out and documented a risk-based assessment?

Considerations for a risk-based assessment:

Considerations for a risk-based assessment should include the following (this is not an exhaustive list):


What was the purpose for collecting the data in the first place?


What lawful bases might apply to the proposed further processing of this data?


To whom is the data being disclosed?


Are there any statutory provisions governing the intended processing by the data controller?


Who will be affected by the decision to share, or not to share, the information?


What risks arise and to whom, by the decision to share, or not to share, the information?


What is the nature of the risks that may arise?


What are the benefits to those persons affected by the sharing of the data?


What is the detriment to those persons affected by the sharing of the data?


Can your purpose be achieved without sharing personal data?


Can you reduce the amount of personal data to be shared?


Who may need to be informed about the sharing of data?

Based on the above, it will be necessary for data controllers to balance the rights of individuals regarding the processing of their personal data against any identified safeguarding concerns of third parties. Under those circumstances, it is incumbent on data controllers to centre the necessity, proportionality and relevance of any form of processing in terms of the rights of all data subjects.

Documenting Concerns Prior to Sharing Data with Third Parties

In the course of their work with at-risk adults, data controllers may come into possession of sensitive information, including Article 10 data that relates to criminal or alleged criminal activity. This information will often be in the form of so-called 'soft information', where concerns or allegations are made regarding a person, without any factual evidence being present. For example, a family member of an adult in a residential facility might report that another resident has been accused of sexual offences or has a reputation in the community as an alleged offender. If this so-called 'soft-information' is written down or recorded by the organisation, it will constitute personal data for the purposes of data protection law, and must be processed accordingly.

It is important to note the following:

- In line with Article 5(1)(b) of the GDPR, personal data should only be collected for specified, explicit and legitimate purposes. Therefore, this type of information should only be collected where there is a genuine need to do so. The information provided about a person in the context described above gives rise to a safeguarding concern that may require action by the organisation, but if there is no identified purpose for using this information it should not be retained or recorded.

- Article 5(1)(d) of the GDPR provides that organisations are obliged to process data accurately. Therefore, it is important to categorise information properly. In this context, an allegation or hearsay about a person's behaviour ought to be documented as such, rather than as a statement of fact. The organisation cannot reasonably ignore the information if it is considered to give rise to a genuine safeguarding concern, but it should not create an inaccurate record pertaining to the person concerned, in particular where Article 10 data is concerned.

Data controllers will also be required to put safeguards in place to ensure that sensitive information of the type in question above is handled appropriately. These safeguards may take the form of both technical and organisational measures (note that this is not an exhaustive list):

In terms of **technical measures**, the following examples may be applicable:

- Access to the digital records should be limited to certain individuals to ensure that only authorised staff have permission to view or amend records that deal with particularly sensitive information, including Article 10 data;

- Logging mechanisms ought to be in place which records who accessed the data, when it was accessed, why it was accessed and what amendments were made, if any;

- Encryption of personal data that relates to sensitive information in this context;

- Enhanced device security for ICT equipment that may be used to gain access to sensitive information;

- Pseudonymisation of the personal data, to limit the identification of the individuals in question.

In terms of **organisational measures**, the following may be relevant in this context:

- Specific staff training around handling highly sensitive and Article 10 data;

- Limitation of access to physical records containing highly sensitive and Article 10 data to those staff members who strictly need it.

In the context of adult safeguarding, it may be necessary for the data controller to take actions based upon the highly sensitive/Article 10 data which has been brought to their attention. That is a matter for the data controller to decide within the context of adult safeguarding and those actions are not data protection matters. The data protection aspect of this concern is limited to how the data is processed. Therefore, from a data protection perspective, if it is not strictly necessary for the staff involved in implementing these actions to be aware of this new data then they should not have access to it. Staff members, other residents, and visitors may be able to infer certain sensitive information about a resident based on the safeguarding actions that have been implemented, i.e. control of their physical location or the care staff assigned to them. What matters for the purposes of data protection law, is that those who are not entitled to access this information should not be able to gain access to it even though the actions being implemented may be based on that data.

Sharing Sensitive Data, including Article 10 Data

From time to time safeguarding organisations, as data controllers, may wish to share sensitive information, including Article 10 data, with other organisations, or seek such information from another organisation.

Examples in this context could include:

- Circumstances where a resident is moving to a new setting and has been assessed as posing a threat to the safety of fellow residents due to information that their current safeguarding organisation is aware of.

- A data controller wishes to clarify information about a resident with another body or AGS in order to fully assess safeguarding actions.

As set out above, the data controller must be satisfied it has a legal basis, under Article 6(1) of the GDPR to process the information that is being sought. This means that the information in question must be strictly necessary to perform a specific and legitimate function of the organisation. Where this is the case, Section 55(1)(b)(iv) of the 2018 Act may permit the processing of data to take place, subject to suitable and specific measures being put in place to protect the confidentiality of the data and to ensure compliance with the principles of data protection. In addition, the data controller will need to identify their lawful basis under Article 6(1) of the GDPR.

When considering data sharing in this context, **only so much of the data as is strictly necessary to meet the specific and legitimate purpose that has been identified should be shared between the organisations.** For example, it may suffice for one organisation to confirm to another that particular safeguarding actions were taken with regard to an individual without revealing particular details, or for one organisation to confirm that they hold similar information.

It should be noted however that Section 55(1)(b)(iv) does not provide any obligation for one organisation to share personal data with another. It permits the processing of personal data for the purposes outlined but any data sharing is discretionary on the part of the organisation concerned.

One of the reasons a data controller may not wish to share the data is due to concerns arising from compliance with data protection law. However, as set out, data protection law does not stand in the way of sharing data within the context of adult safeguarding; what data protection law requires is that the sharing is lawful, relevant, necessary and a proportionate measure for the achievement of the objectives of data controller, such as the safeguarding of at-risk adults.

The DPC blog on **'Failure to share information with a nursing home about a resident's criminal convictions'** provides an example of how Section 55(1)(b)(iv) can be applied in practice.

Conclusion

The data protection legislative frameworks are principles-based, and it is the responsibility of data controllers to implement these principles by way of a risk-based approach that takes into consideration the nature, scope, context and purposes of processing. The safeguarding concerns addressed in this guidance note arise from the consideration of risk in balancing the occasionally competing interests of at-risk adults. Data protection legislation requires data controllers, regardless of the sector, whether public, private, voluntary or charitable, to implement measures to ensure and to be able to demonstrate compliance (the principle of accountability) with data protection law. To this end it is imperative that decisions made on the basis of risk assessments are clearly documented each time personal data relating to the behaviour of individuals, and in particular where data relating to criminal convictions or offences (or allegations of such) are processed.

FAQs

Frequently Asked Questions

General Data Sharing Concerns

1. **I work in a health care facility as a social worker. I am unsure whether I can share information with a third party and if I can do that, I am not sure how much information I might be able to share. Who should I ask about this?**

You should contact your organisation's Data Protection Officer (DPO) (or the individual assigned to address data protection issues if there is no DPO) if you are unsure whether you should disclose information. Your DPO is your first point of contact for any data protection queries and they can advise you how or when to share information.

2. **In assessing the risk associated with sharing a client's personal data with a third party what should we consider?**

Note that the below is not an exhaustive list and other factors may be required to be considered and each situation is likely to be fact and case specific.

The data controller should conduct and document a risk based assessment and in doing so, ought to consider the following, at a minimum:

- ✓ What was the purpose for collecting the data in the first place?
- ✓ What lawful bases might apply to the proposed further processing of this data?
- ✓ To whom is the data being disclosed?
- ✓ Are there any statutory provisions governing the intended processing/sharing of personal data by the data controller?
- ✓ Who will be affected by the decision to share, or not to share, the information?
- ✓ What risks arise and to whom, by the decision to share, or not to share, the information?
- ✓ What is the nature of the risks that may arise?
- ✓ What are the benefits to those persons affected by the sharing of the data?
- ✓ What is the detriment to those persons affected by the sharing of the data?
- ✓ Can your purpose be achieved by not sharing personal data?

- ✓ Can you reduce the amount of personal data to be shared?
- ✓ Who may need to be informed about the sharing of data?

A data controller must remember that while it is necessary to assess the risk involved with sharing the data, it is also important to assess the risk involved with not sharing the data.

Example

A parent acting on behalf of their adult son who attends regular appointments with a mental health care provider has requested a copy of their appointment schedule in order to help them to attend their appointments. The vulnerable adult has a history of missing their appointments, and the health care provider is familiar with the parent and knows that they are involved in assisting their adult child.

In the first instance, the health care provider should consider the will and preference of the vulnerable adult who is their patient, and whether they have capacity to agree to the sharing of this information with their parent.

The health care provider may also wish to consider the risk of sharing and the risk of not sharing this data with the patient's parent. The health care provider should consider the provision of health care and the welfare of the patient when making this decision and can therefore conduct a risk-based assessment, having regard to the factors as set out above, when determining whether to release the information to the parent. Such an assessment should be recorded in writing, and the vulnerable adult should be informed at all stages of the process.

3. Should I keep a record of my decision to share or not to share information?

Yes, you should always document your decision to share or not to share information/ personal data and your reasons for whatever course of action you took.

You should also document the information/personal data that was shared, highlighting with whom the information/personal data was shared in line with the organisation's policies and procedures.

An individual has the right to submit a complaint to the Data Protection Commission (DPC) if they believe their data protection rights have been infringed. In reviewing such complaints, the DPC may request sight of a copy of your risk assessment. Therefore, it is essential to maintain clear records that justify the rationale for sharing personal information.

4. How much information should be shared in an adult safeguarding situation?

This must be assessed on a case by case basis. In essence, the data controller must ensure that they have a lawful basis for sharing the data, are compliant with Article 5 principles, have appropriate safeguards in place and have a documented risk-assessment.

When deciding what information to share, data controllers should ask themselves the following questions (not an exhaustive list and will be fact/case specific):

- ✓ Have I carried out and documented a risk assessment to assist in the analysis of the potential risks of sharing any personal data of the data subject?
- ✓ What is the purpose of sharing this information?
- ✓ Is it necessary that information is shared at all?
- ✓ How much information needs to be shared for the purposes of the aim to be achieved?
- ✓ What is the minimum amount of data that needs to be shared?
- ✓ Is the sharing of the data proportionate to the objective to be achieved?
- ✓ Do I have a secure way to share this information with this specific person?

5. Should individuals be informed of the sharing of their personal data?

Yes, a data controller needs to comply with the principle of transparency in line with Articles 12-14 of the GDPR and this includes informing individuals as to how their personal data will be used and for what purpose, who has access to it, and how the sharing of that information will impact them. This can be achieved via privacy policies, information leaflets etc.*

***There may be some limited exemptions applicable under Article 14(5) of the GDPR, such as:**

- **Where the individual already has the information;**
- **Where the provision of the information is impossible or would involve a disproportionate effort;**
- **Where you have obtained the information under a legal obligation; and**
- **Where the personal data must remain confidential due to an obligation of professional secrecy regulated by law.**

6. Should the data controller inform the individual that their information was disclosed in circumstances where the individual objected to the sharing of their information in the first place?

In certain circumstances a data controller may need to disclose information to a third party, such as AGS, without informing the individual. This disclosure might be contrary to the will and preference of the data subject; however the data controller might form the view that notwithstanding this, the disclosure of the data should nonetheless take place.

This might arise where there is a risk to the safety of an at-risk adult and that safety risk might be heightened by its non-disclosure. Under those circumstances, a data controller should carry out a risk-based assessment.

If the data controller decides to inform the data subject that their data was shared in the absence of their consent, it would be prudent for the data controller to document its rationale for the disclosure. If the data controller decides not to inform the data subject that their data was shared in the absence of their consent, it would be prudent for the data controller to document this also. Under both sets of scenarios, the data controller ought to document the legal basis under Article 6(1) of the GDPR for the sharing of the personal data and it also must ensure compliance with the principles set out in Article 5 of the GDPR alongside ensuring appropriate safeguards are in place.

Example

A private nursing home is concerned that one of its residents is a victim of financial abuse and that a family member is the perpetrator. A social worker has carried out an assessment and believes there are reasonable grounds for concern. The social worker has spoken to the resident about this who has expressed their will and preference on this matter which is to not disclose this matter to AGS.

In such circumstances the data controller must remember that from a data protection perspective there is nothing to prevent the processing of such information, the issue is how this processing occurs. It is a matter for the data controller to make an informed decision as to how to address this overall; however, from a data protection perspective, the data controller must:

(a) consider the veracity of the information they are acting upon and

(b) conduct a risk-based assessment.

Having completed that, the data controller must then decide next steps, which is to disclose or not disclose the personal data of the resident to AGS. If the data controller decides to share the personal data with AGS, they must then consider whether they are going to tell the resident that they have done so in the absence of their consent, in line with the transparency of processing principles.

So, even though the resident has not provided their consent to the disclosure of their personal data that does not mean the data cannot be shared. However, it is contingent on the data controller carrying out its due diligence on the data protection issues arising, meaning that there must be adherence to the Article 5 data protection principles, there must be a lawful basis for the sharing of the information under Article 6 of the GDPR and there must be appropriate safeguards in place. The data controller must also be in a position to marry the will and preferences of the resident with the ultimate act of sharing of the data subject's personal data. It is advisable for the data controller to document the various steps, assessments and rationale because in the event of a complaint to the DPC, this information will be requested from the data controller.

Lawful Basis under the GDPR for processing (sharing/ disclosing) information

7. Do you need to have a lawful basis for sharing/disclosing information?

Yes. The sharing or disclosure of personal data constitutes processing for the purposes of data protection law. Any processing of personal data will require a lawful basis under Article 6 of the GDPR. In the absence of a lawful basis under Article 6 of the GDPR, the processing will be deemed unlawful.

For more information please see our guidance note on Legal Bases on our website.

8. Is consent always required when sharing information in an adult safeguarding context?

Consent is only one of the six lawful bases outlined in Article 6(1) of the GDPR. When processing special category data under Article 9(2)(a) of the GDPR, that consent must be explicit consent. For consent to be valid, it must be freely given, clear, informed and unambiguous.

It is important for data controllers to note that if relying on consent for any processing activity, including sharing information in adult safeguarding contexts, that consent must not be 'bundled consent'. 'Bundled consent' is where a data controller seeks to rely on one consent agreement for a host of processing activities. For consent to be valid, consent must be sought for each processing activity. Where a data controller has another lawful basis under Article 6 of the GDPR consent will not be required for the processing activity.

Our blog on the **'Failure to share information with a nursing home about a resident's criminal convictions'** provides a clear example where consent is not required to share information.

Further, the sharing of personal information may occur without consent when there is a legal obligation, as demonstrated in two key pieces of legislation:

- Section 19 of the National Vetting Bureau (Children and Vulnerable Persons) Act 2012 requires specific organisations like HIQA, MHC, CORU, and the HSE to share specified information with the National Vetting Bureau regarding persons working with vulnerable persons.
- Additionally, Section 3(1) of the Criminal Justice (Withholding of Information on Offences Against Children and Vulnerable Persons) Act 2012 makes it an offence to withhold information about Schedule 2 offences against vulnerable persons from AGS. However, this Act's scope in adult safeguarding only provides a lawful basis for sharing information with AGS, not other bodies, and only applies to specific offences listed in Schedule 2.

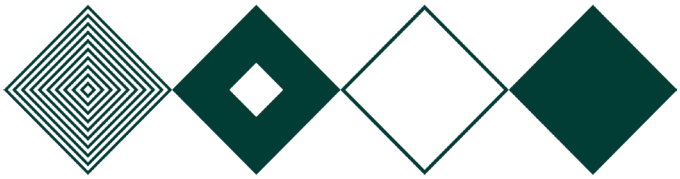
Processing Information relating to Alleged Criminal Offences

9. I work in a private nursing home and a resident may have recently committed an alleged offence against other residents. The matter is currently being investigated by the Gardaí. The patient in question is now due to move to another private nursing home. Can I share the information relating to the incident with the new nursing home even though it might not fall under the care and treatment of the resident?

When considering whether to share this information the data controller must consider the circumstances and nature of the allegation.

As set out previously, the decision to share information needs to be carefully considered by a data controller on a case by case basis. The data controller ought to adopt a risk based approach having regard to the gravity of the offence.

As also set out in previous FAQs, the data controller should also document the risk assessment carried out prior to any potential sharing of information/personal data. This may include setting out the nature of information/personal data which is the subject of the risk assessment, the person/body with whom the information/personal data may be shared in line with the organisation's policies and procedures and the purpose of potentially sharing this information/personal data.



10. In a private nursing home setting there has been an alleged sexual assault on a resident. The resident has significant cognitive impairment and is unable to recall details of the incident. The family of the resident now want to know information on the alleged perpetrator. Should this information be shared with the family?

It is a matter for the data controller to carry out a risk-assessment to determine whether they should share the information relating to the alleged perpetrator with the family member who made the request. This will require a consideration of the facts, including the gravity of the allegation and potential impact upon the rights and freedoms of all parties (victim and alleged perpetrator) as a consequence of the disclosure of the relevant information versus non-disclosure of the information.

11. How do we respond to Gardaí requesting information from us? Are we allowed to share information in these circumstances?

If personal data is requested from a law enforcement body such as AGS for the purposes of preventing, detecting, investigating or prosecuting criminal offences, then Section 41 of the Data Protection Act 2018 applies.

The 2018 Act permits the processing of personal data other than for the purpose for which it was collected where such processing is necessary and proportionate for preventing, detecting, investigating or prosecuting criminal offences; however the individual's right to privacy must be balanced against the need to investigate offences.

On receipt of a Section 41 request for the disclosure of data from AGS, the data controller is entitled to ask for the request to be in writing and the data controller is also entitled to ask AGS for the purposes of the request. This assists the data controller in determining their legal basis for the sharing of the data and it also assists the data controller in determining the minimum amount of data to be shared. Data controllers maintain their obligation for compliance with the principles of Article 5, even though the request is from AGS.

You can find the official text for Section 41 of the Data Protection Act 2018 (Ireland), on the Irish Statute Book website.

12. As a Healthcare facility providing care to adults in vulnerable situations, can we process information relating to a criminal offence? And how do we deal with information relating to alleged criminal offences?

As explained in the DPC guidance document, Article 10 of the GDPR provides for the processing of personal data relating to criminal convictions and offences. Furthermore, under section 55(9) of the Data Protection Act 2018, Article 10 data was extended to include personal data relating to the alleged commission of an offence and any proceedings in relation to such an offence. In addition, section 55(1)(b)(iv) of the 2018 Act provides for data controllers (who are not an 'official authority') to process personal data in certain circumstances, such as that where 'processing is necessary to prevent injury or other damage to the data subject or another person or loss in respect of, or damage to, property or otherwise to protect the vital interests of the data subject or another person'.

In this regard, data controllers may process personal data in respect of an alleged offence, for the purposes outlined, but must have consideration for the data protection principles under Article 5, namely accuracy, purpose limitation and data minimisation, when it comes to sharing personal data relating to an alleged offence. The data controller must also have a lawful basis under Article 6 of the GDPR for the processing of this data with appropriate safeguards in place.

As outlined above it is best practice for a data controller to conduct a risk based assessment prior to sharing the information and to document the decision.

13. What should we do if an alleged perpetrator does not consent to the sharing of their personal information by a hospital to a nursing home?

Matters such as these ought to be considered on a case by case basis. The data controller needs to conduct a risk-based assessment. This will assess the circumstances and nature of the allegation and the impact on the rights and freedoms of all concerned.

This assessment should be documented and the assessment ought to include the rationale to share or not to share the information with the nursing home.

If the hospital decides to share the personal data with the nursing home and if a complaint is subsequently lodged by this individual/data subject with the DPC regarding the sharing of the data, the DPC would request sight of the risk assessment giving rise to the sharing of the data.

14. Can personal information collected by a body be shared with another organisation?

Under the GDPR the sharing of information is not prohibited. However, careful consideration must be taken before sharing any information. Any disclosure of personal data to a third party is regarded as 'processing', and it is the legal responsibility of each data controller to ensure that all processing of personal data is underpinned by a valid lawful basis and carried out in compliance with the provisions of the GDPR and the Data Protection Act 2018.

The body in question must ensure that it has a lawful basis under Article 6 of the GDPR for sharing this personal information and in instances where special category data is involved, a lawful basis under Article 9 of the GDPR is also required. In the absence of consent of the at-risk adult the body must look to Articles 6(1)(b)-(f) and Articles 9(2)(b)-(j) of the GDPR. In relation to those provisions under Article 6 of the GDPR the concept of 'necessity' applies. Service providers must consider what personal data is necessary to process for the relevant lawful basis they are relying upon to achieve their objective.

15. Can you share information from a private nursing home to a public body institution?

Yes, information sharing is possible once there is a lawful basis under Article 6 of the GDPR for sharing the information. Responsibility rests with each controller to ensure that a specific legal basis is in place before any disclosure takes place and that any disclosure is strictly relevant, necessary and proportionate to the objective. Each request for disclosure should be assessed on a case-by-case basis.

When sharing information the service provider must consider the data protection principles under Article 5 of the GDPR, such as data minimisation, accuracy and integrity and confidentiality of the personal data in question.

For example if a private nursing home is concerned about a resident being sent to Accident and Emergency (A&E) in a public hospital due to an allegation of a sexual nature against another resident, and the concerns stem from this resident being in a crowded A&E and subsequently being admitted to a public ward, the private nursing home can carry out their risk assessment and, in doing so, set out for the hospital what their safeguarding plans for that resident are (for example they are not left unattended around certain persons etc.). This would be in line with the Article 5 principle of data minimisation.

However, this will be fact specific and it may be the case that having carried out a risk assessment, the private nursing home is of the view that either less or more information is required. This concerns the safety not just of the at-risk resident but also concerns the safety of others who may come into contact with the resident, having regard to the nature of the allegations.

16. As a Healthcare facility we deal with quite a large number of referrals and follow up queries from various elected representatives, is it lawful to process such data?

Please read our guidance document, **'Guidelines on the processing of personal data by Elected Representatives under Section 40 of the Data Protection Act 2018'**, which sets out the obligations placed on elected representatives in relation to the making of such representations on behalf of the data subject and their responsibilities in relation to personal information that comes into their possession and control. This guidance highlights the obligations placed upon organisations (public and private data controllers) that process representations made on behalf of individuals by elected representatives.

17. We have received a Subject Access Request (SAR) from a family member of one of our patients, should we respond to same/are we in trouble if we do not respond?

The GDPR does not prohibit an individual allowing a third party (e.g. a relative, friend or solicitor) to make a SAR on their behalf and in the case of an at-risk adult it can be quite common for a third party to do so. However, as a data controller, you need to be satisfied that the third party making the request is entitled to act on behalf of the individual.

It is the third party's responsibility to provide you with documentation in relation to their legal authority to act on behalf of the individual in question. For example, this can be achieved by providing a written authority, signed by the individual, stating that they give the third party permission to make a SAR on their behalf.

It may also be the case that a third party holds an enduring power of attorney (which may cover the issue), or the at-risk individual is under the wardship jurisdiction of the court (in which case the Committee of the Person may be able to engage with the data controller). Also, the Assisted Decision-Making (Capacity) Act, 2015, as amended, sets out various arrangements to support certain individuals in their decision-making but it will be necessary to ascertain if this includes matters such as data protection.

Data controllers have one month to respond to such a request and even if the request is being denied, they must still respond, setting out the reasons for same. It is then open to that person to lodge a complaint with the DPC, should they wish to do so.

Data controllers should also be conscious of ensuring that the personal data of any third parties who are mentioned in documentation that forms part of a resident's subject access request are redacted, as appropriate. Examples of such persons may be employees such as nursing staff or family members/visitors of the resident.

18. One of our patients died recently and the family members have made a subject access request to access the deceased patient's safeguarding care plan. Should I comply with this request?

Recital 27 of the GDPR specifies that the GDPR does not apply to the personal data of deceased persons. However, there is no reason why a data controller could not comply with the request for information/personal data of the deceased.

If the data controller does release the data of the deceased individual to a family member, they ought to ensure they redact all third party personal data.

19. We have received a rectification request/erasure request from a family member of one of our patients, should we respond to same and if so, how do we respond?

As with the exercise of any data protection right, the GDPR does not prohibit an individual allowing a third party (e.g. a relative, friend or solicitor) to also make a rectification and/or erasure request on their behalf.

As a data controller, you need to be satisfied that the third party making the request is entitled to act on behalf of the individual i.e. that they have the legal authority to do so.

Data Protection and Potential Risks to At-Risk Adults relating to the Conduct of Employees

20. Following a complaint against an employee in our Healthcare Facility we have recently conducted an investigation into that employee's conduct and have concerns that they pose a further risk to the other at-risk adults. Who should we report this information too?

Section 19 of the National Vetting Bureau (Children and Vulnerable Persons) Act 2012 (the '2012 Act') places a legal obligation on certain service providers to notify specified information to the National Vetting Bureau of AGS regarding persons engaged in work or activities relating to at-risk adults. However, a data controller must be aware that the information that can be shared under Section 19 of the 2012 Act is limited.

As set out in the main Guidance document, data controllers must have a lawful basis under Article 6(1) of the GDPR to process personal data. If any other statutory provisions mandate the disclosure of certain data by the data controller with another body, the GDPR provides for this disclosure under the lawful basis of Article 6(1)(c) of the GDPR, which is that processing is lawful if it is in compliance with a legal obligation.

Section 19 of the 2012 Act states that following an investigation, inquiry or regulatory process in respect of a person, the notifying organisation has a bona fide concern that the person who is the subject of that investigation, inquiry or regulatory process, may—

a. harm any child or vulnerable person,

b. cause any child or vulnerable person to be harmed,

c. put any child or vulnerable person at risk of harm,

d. attempt to harm any child or vulnerable person, or

e. incite another person to harm any child or vulnerable person,

That organisation shall provide specified information to the Bureau and notify the Bureau in writing of that concern and shall state the reasons for it as soon as possible.

Resources

Appendix 1

Conducting a Balancing Exercise (Article 6(1)(f) GDPR)

When providing services to and working with at-risk adults, data controllers may encounter situations requiring the processing and/or sharing of an individual's personal data with another person or organisation. This may be necessary to safeguard and protect the interests, and rights, of an individual at risk of harm or in a vulnerable situation.

When this arises, and prior to the sharing of any personal data, the data controller should carry out a balancing exercise; the balancing exercise aims to balance the legitimate interests of the data controller/third party (e.g. to safeguard and protect the data subject in some way) against the rights of the individual whose data is going to be disclosed to a third party by the data controller. In addition, the data controller ought to consider whether the sharing of the data is both necessary and proportionate to achieve the identified legitimate interest, or whether there is a less intrusive way in which this can be achieved.

Article 6(1)(f) of the GDPR encompasses three elements which data controllers need to consider. Data controllers should:

- ✓ Identify the **legitimate interest**;
- ✓ Demonstrate that the intended processing of an individual's personal data is **necessary to achieve** the legitimate interest and;
- ✓ **Balance** the legitimate interest against the **individual's interests, rights and freedoms**.

Further general guidance about the three elements needed for the Article 6 (1)(f) GDPR legitimate interests legal basis can be found on our website.

Example

A private nursing home is concerned that one of its residents is a victim of financial abuse and that a family member is the perpetrator. A social worker has carried out an assessment and believes there are reasonable grounds for concern. The social worker has spoken to the resident about this who has expressed their will and preference on this matter which is to not disclose this matter to An Garda Síochána (AGS).

It is a matter for the data controller to make an informed decision as to how to address this overall, however, from a data protection perspective, the data controller must (a) consider the veracity of the information they are acting upon and (b) conduct a risk-based assessment.

Having completed a) and b), the data controller must then decide next steps, which is whether to disclose or not disclose the personal data of the resident to AGS.

Considerations for a Balancing Exercise:

The three elements of Article 6(1)(f) GDPR must be considered by the data controller:

✓ Is there an identifiable **legitimate interest**?

The identifiable legitimate interest in the example above could be the protection of the resident from potential financial abuse and fraud. Additionally, a secondary identifiable legitimate interest could be the broader societal benefit of preventing financial abuse and fraud against at-risk persons, however this secondary legitimate interest is identified in tandem with, rather than in isolation from, the first identifiable legitimate interest of protecting the resident from potential financial abuse.

✓ Can the nursing home demonstrate that the intended processing (sharing) of the resident's personal data is **necessary to achieve** the identified legitimate interest?

Necessity test: Is the potential sharing of the resident's personal data with AGS regarding alleged financial abuse a **reasonable** and a **proportionate** way to achieve the legitimate interest e.g. the prevention of potential further financial abuse of a resident?

- **Reasonable:**
  - Has the nursing home given due consideration to the veracity of the information which they may act upon i.e. reporting the allegation on the basis of a reasonable concern?
  - What evidence supports the social worker's assessment of reasonable grounds for concern?
  - Is there an immediate risk to the resident's financial wellbeing?
  - What are the possible repercussions for the resident by not sharing this information?
  - What are the possible repercussions for the resident by sharing this information?
- **Proportionate:**
  - Is there a less intrusive way to achieve the intended result?
  - What is the minimum amount of information needed to share with AGS if disclosure is deemed necessary?
  - If a decision is made to report the concern to AGS, is the nursing home only providing the necessary, limited information in line with the GDPR principle of data minimisation e.g. refraining from including any information that is not relevant to the concern such as providing details about the resident's medical information, other family members etc.?
  - Can the concern be reported to AGS in a manner which ensures that the information is provided in a secure and confidential manner?

and;

- ✓ **Has the nursing home balanced the legitimate interest against the data subject's interests, rights and freedoms?**
  - What data subject rights are potentially affected?
  - To what extent are the data subject rights affected?
  - Does the identified legitimate interest outweigh or align with the affected data subject's interests and rights?
  - Do the data subject's rights outweigh the identified legitimate interest?
  - How are the will and preferences of the data subject considered within this assessment? Particularly where the resident has expressed their will and preference is for this information not to be shared with AGS.

If the data controller decides to share the personal data of the data subject with AGS, in the absence of their consent, they must then consider whether they are going to tell the resident that they have done so in line with the transparency principle. In line with the principle of transparency, the nursing home may also decide to explain to the resident in clear and plain language the basis for their legitimate interest in sharing the information and the necessity for sharing the information as well as the safeguards being put in place, i.e. that the minimum amount of personal data will be shared and that the sharing will be done in a secure and confidential manner. The resident should also be made aware of their right to raise a complaint with the Data Protection Commission if they are not satisfied with the decision made by the nursing home.

This example demonstrates that even though the resident has not provided their consent to the disclosure of their personal data, this does not mean the data cannot be shared. However, it is contingent on the data controller carrying out its due diligence on the data protection issues arising, meaning that in addition to carrying out a balancing exercise, there must be adherence to the principles as set out in Article 5 of the GDPR, together with a lawful basis for the sharing of the information under Article 6 of the GDPR with appropriate safeguards.

It is advisable for the data controller to document the various steps, assessments and rationale because in the event of a complaint to the DPC, this information will be requested from the data controller.

Appendix 2

How to write a Data Protection Policy ('Privacy Policy')

Privacy Policy

What is a Privacy Policy?

A data protection notice (also known as a **'Privacy Policy'** or **'Privacy Notice/ Statement'**) is an accountability tool that helps a data controller demonstrate that it is compliant with data protection law, in particular in respect of its obligations under the transparency principle (Articles 12 to 14 of the GDPR), and to fulfil the right of data subjects to receive certain information in relation to a data controller's processing operations.

Privacy policies should reflect a detailed examination of an organisation's processing of personal data and the application of data protection law to these practices. The privacy policy should be a dynamic document, regularly reviewed and updated to reflect changes in the way the organisation processes personal data.

Making a Privacy Policy Easy to Understand

Privacy policies should be written in **clear, plain language** that is easy for the reader to understand. The **use of simple language** helps to ensure that a privacy policy is as clear and easy to understand as possible. The use of clear, plain language is of particular importance when providing information to at-risk adults.

Privacy policies should be **easily accessible**, and should be published on the organisation's website, where possible.

Key questions to consider before writing a Privacy Policy

Firstly, in accordance with a functional approach, a data controller should carefully assess its business and the activities in which it deals with personal data, making sure that the data protection notice will **reflect what its processing operations really are**. Once a data controller has singled out each data processing operation, it will have to gather all the information about the operations that data protection law requires it to provide to data subjects, including the purpose of processing, the recipients of the personal data, the retention period, and so on.

Thereafter, a data controller should **consider the categories of data subjects** it must provide the information to, in order to draft, in **appropriate language**, the data protection notice. Before making a data protection notice available, data controllers should remember to check whether certain information should be omitted in accordance with applicable exemptions or derogations to data protection rights.

Some key questions to consider:

- What kind of personal data do you process?
- What are the reasons for the processing of personal data? Remember that Article 6 (and Article 9 where applicable) of the GDPR requires data controllers to have a lawful basis for processing personal data.
- How do you collect personal data - did you get the personal data directly from the data subject or somewhere else?
- Who will the personal data be shared with?
- How long are you going to keep the personal data for?
- Does your organisation have a Data Protection Officer? How can they be contacted?
- If your organisation does not have a Data Protection Officer, who is the designated person to deal with data protection queries? How can they be contacted?
- Will personal data be transferred outside the European Economic Area (EEA)?

What information must be included in a Privacy Policy?

The kind of information that must be communicated in your privacy policy is set out below (see 'Information Checklist'). Please note that the **level of detail necessary may vary between organisations** and additional information may need to be provided to data subjects depending on the individual circumstances of the organisation and the respective processing activities engaged in. Privacy policies should cover information about **all** data processing activities by the organisation.

Information Checklist

☑ Who is the data controller?

You must provide information about who the data controller is and their contact details. Any organisation which engages with at-risk adults, whether large or small, public or private, or part of the voluntary or charitable sector, and which processes personal data is a data controller, and, where possible, should designate a point of contact for data protection queries.

While it is recognised that not all organisations have a Data Protection Officer (DPO), you must also provide contact information for your organisation's DPO, if you have one.

☑ What kind of personal data are you processing?

You must provide information on the types of personal data that you are processing, e.g. personal data about health information, welfare information, financial information, emergency contact information, etc. Be clear about all types of information you are collecting, particularly if it is information that people wouldn't necessarily expect you to be collecting.

Also, if you did not get the personal data directly from the data subject themselves, you need to tell them where the data came from.

☑ Why are you processing data?

You need to explain the reasons why you are processing personal data, and the lawful basis you are relying on under Article 6 (and Article 9 where applicable) of the GDPR. You may be relying on more than one basis, so make sure to include them all.

If your organisation is relying on legitimate interest, you need to explain what exactly this legitimate interest is.

If your organisation is relying on consent as a lawful basis for any processing activity, you must make it clear to the data subject that they can withdraw this consent at any time, and you must tell them how they can do this. Consent should be as easy to withdraw as it was to give in the first place, so organisations must ensure they have a mechanism in place for handling these requests.

If your organisation is relying on the performance of a contract as a lawful basis for any processing activity, the organisation must be satisfied that there is a valid underlying contract and that any clause(s) the performance of which necessitate the processing of personal data are valid and enforceable.

☑ Who will this data be shared with?

You must provide individuals with information about the recipients of any personal data you collect.

In other words, you have to clearly state if you will be disclosing this personal data to anyone, and if so, to whom? For example, another public authority, agency or other body.

☑ How long will data be kept for?

You must inform individuals **how long** you are going to keep their data for, and importantly, **why**. Sometimes the reasons for this might be set out under other laws to which the organisation is subject. It is important to be really clear about this and why you are keeping data for a specified period of time.

This information can be further explained in your organisation's Retention Schedule that should outline the different time periods for retaining different types of data.

☑ Will this personal data be transferred outside the EEA?

You must inform individuals if their personal data is going to be transferred outside the EEA, either by your organisation or by any third party service providers your organisation might use.

You also must provide details on the safeguards being applied to protect this personal data.

☑ What rights do data subjects have?

You must inform individuals of their data protection rights, e.g. their right of access, their right to rectification, their right to erasure, etc.

You must also explain how they can go about exercising these rights. For example, you can provide them with a contact name and email address where they can submit data protection requests. You could also provide a link to your organisation's Subject Access Request Policy, where applicable.

☑ Are you profiling or making automated decisions?

You need to tell individuals if your organisation will be processing their personal data to profile them or make any automated decisions about them, and what impact this may have on them.

Processing is 'automated' where it is carried out without human intervention and where it produces legal effects or significantly affects an individual.

Individuals have the right to not be subject to a decision based solely on automated processing.

☑ Making a complaint to the Data Protection Commission

You must inform individuals that they have a right to lodge a complaint with the Data Protection Commission if they have any concerns about how you are processing their personal data.

So consider adding the DPC's phone number and a link to our website in your privacy policy to make things easier for individuals.

Appendix 3

Data Protection Impact Assessment (DPIA)

Data Protection Impact Assessment

What is a Data Protection Impact Assessment?

A Data Protection Impact Assessment (DPIA) describes a process designed to identify risks arising out of the processing of personal data and to minimise these risks as far and as early as possible. If required, a DPIA must be completed **before** the relevant data processing has commenced. Article 35 of the GDPR states that a DPIA **must** be carried out by a controller where a type of data processing, in particular using new technologies, is likely to result in a **high risk** to the rights and freedoms of individuals. The GDPR also sets out a number of specific instances in which controllers must conduct a DPIA (see Article 35(3) in particular).

DPIAs are important tools for negating risk, and for demonstrating compliance with the GDPR. As a controller, your organisation needs to make sure that a DPIA is carried out where this is appropriate. An initial assessment of the risk arising from data processing, using the checklist on the following pages, can indicate whether a DPIA is likely to be necessary before introducing a new technological solution or method of working. When making this assessment, organisations should take into consideration that adults in vulnerable situations or at risk of harm often results in a higher level of risk arising from the processing of their personal data.

Data Protection Impact Assessment – Template

The DPC has included on the following pages a sample template of the kind of information that a DPIA should include and how to record it. This template should be read alongside our dedicated DPIA guidance on our website, as well as the criteria for an acceptable DPIA set out in European guidelines on DPIAs.

You should start to fill out the template at the **beginning** of any major project involving the use of personal data, or if you are making a significant change to an existing process.

PLEASE NOTE, THIS TEMPLATE HAS BEEN PROVIDED BY THE DPC FOR ILLUSTRATIVE PURPOSES ONLY. THIS TEMPLATE DPIA IS NOT TAILORED FOR EVERY INSTANCE IN WHICH A DPIA MAY BE REQUIRED. ORGANISATIONS ARE ULTIMATELY RESPONSIBLE FOR ENSURING THAT ALL APPROPRIATE, RELEVANT INFORMATION IS INCLUDED IN ANY DPIA THEY CARRY OUT.

Organisation Information

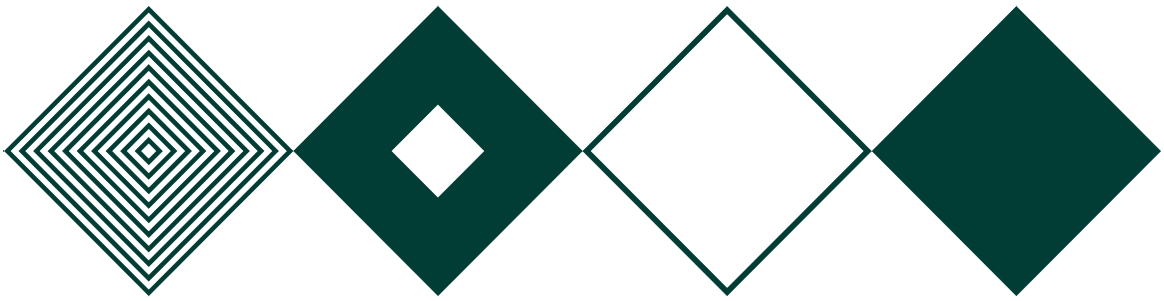
Name of organisation	
Title of DPIA	E.g. DPIA for data sharing between social care services and health care providers to safeguard adults in vulnerable situations experiencing abuse or neglect. DPIA for the use of new software for tracking accidents on organisation's premises.
Name of Data Protection Officer (if applicable) or contact for data protection issues	John Smith
Contact details **Phone** **Email**	 08X – XXX XXXX dataprotection@xxxxxxx.ie
Third parties involved/associated with the project (e.g. agencies, departments, service providers, etc.)	
This DPIA will be kept under review by:	

Is a DPIA required? Initial assessment of the project.

Does your project involve any of the following[3]: The DPC has highlighted below in green the scenarios most likely to trigger the need for a DPIA in the context of adult safeguarding, but this does not mean that the other criteria do not apply. It is for organisations to make that assessment.	Yes	No
Evaluation or scoring of personal data (including profiling and predicting)		
Processing that aims at making automated decisions about data subjects producing 'legal effects concerning the natural person' or which 'similarly significantly affects the natural person' (Article 35(3)(a))		
Systematic monitoring, including of a publicly accessible area		
Sensitive data or data of a highly personal nature (including special categories of data {Art. 9(1)} and criminal data {Art 10})		
Data processed on a large scale (criteria to take into account could include the no. of data subjects, volume of data, duration of processing, geographical extent)		
Datasets that have been matched or combined		
Data concerning at-risk adults (including persons with a mental health condition, asylum seekers, older persons, patients)		
Innovative use or applying new technological or organisational solutions		
Processing that prevents data subjects from exercising a right or using a service or contract		
Use of personal data on a large-scale for a purpose(s) other than that for which it was initially collected pursuant to Article 6(4) GDPR		
Profiling at-risk adults to target marketing or online services at such persons		
Use of profiling or algorithmic means or special category data as an element to determine access to services or that results in legal or similarly significant effects		

3) This checklist is based on criteria provided by the European Data Protection Board in its guidelines on Data Protection Impact Assessments, as well as criteria set down by the Data Protection Commission in its List of Data Processing Operations which require a DPIA.

Systematically monitoring, tracking or observing individuals' location or behaviour		
Profiling at-risk adults on a large-scale		
Processing biometric data to uniquely identify an at-risk adult(s) or enable or allow the identification or authentication of an at-risk adult(s) in combination with any of the other criteria set out in WP29 DPIA Guidelines		
Processing genetic data in combination with any of the other criteria set out in WP29 DPIA Guidelines		
Indirectly sourcing personal data where GDPR transparency requirements are not being met, including when relying on exemptions based on impossibility or disproportionate effort		
Combining, linking or cross-referencing separate datasets where such linking significantly contributes to or is used for profiling or behavioural analysis of at-risk adults where the data sets are combined from different sources where processing was/is carried out for different purposes or by different controllers		
Large scale processing of personal data where the Data Protection Act 2018 requires 'suitable and specific measures' to be taken in order to safeguard the fundamental rights and freedoms of at-risk adults		
If you have answered 'Yes' to any of the above questions, you must conduct a DPIA.		



Step 1: Give an overview of the purpose of this project

Is your organisation a sole data controller or a joint controller?	
Provide a clear description of what you are aiming to achieve with this project. What are the benefits of the data processing?	
What type of processing is involved?	
Who is affected?	
The categories of recipients to whom the data will be disclosed. Who will have access to this information (both inside and outside of the organisation)?	
Why have you identified the need for a DPIA? (See checklist above). E.g. are you processing special category data? Is there a high risk involved? To whom? Why? Is processing being carried out on a large-scale?	
Links to supporting documentation (if any) (e.g. project proposals, reports, pieces of legislation that require this high-risk processing, etc.)	

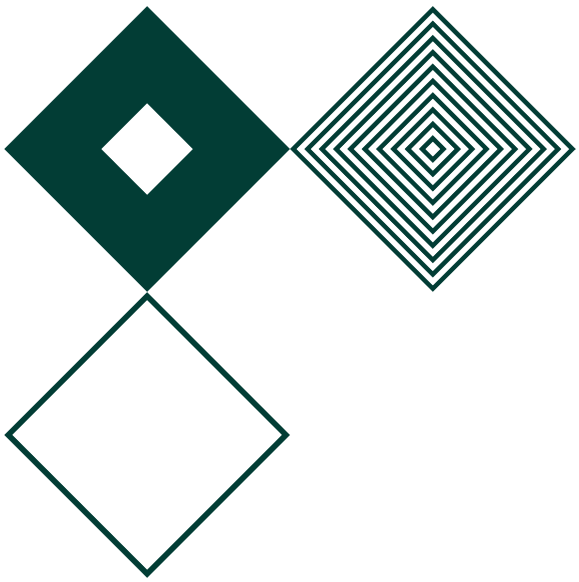
Step 2: Describe the processing activity (nature, scope, context, purpose)

Nature of the processing	
How will your organisation collect, store, use, and delete personal data as part of the project? Please provide details.	
Where has the data been sourced from/ collected from? E.g. directly from at-risk adults or members of their family, from a State Agency, from another database?	
Will your organisation be sharing this data with anyone else? E.g. government departments, agencies, third party providers, etc. If so, who and for what purpose?	
What types of processing identified as likely to be high risk are involved?	
Scope of the processing	
What categories/types of personal data will be collected? E.g. special category data (e.g. health records), financial details etc.	
What type of data subjects are involved? E.g. at-risk persons, family members of at-risk persons, employees, the general public, etc.	
Does the project involve the processing of any special category data (Article 9 GDPR) or data relating to criminal convictions or offences under Article 10 of the GDPR? E.g. medical information about at-risk persons, personal data revealing religious beliefs of individuals, results of Garda vetting, etc.	

How much data will you be collecting and how often will you be collecting it?	
How long will you keep the data for? And why? (E.g. if you have to keep information for a specific number of years because a piece of legislation requires this, please explain this and reference the section of the legislation).	
How many individuals are affected by this processing?	
What geographical area does the project cover? (E.g. are you using any third-party providers who store personal data outside the EEA?)	
What kind of technology will be involved with processing the data? Is it novel in any way?	
Context of the processing	
What is the nature of the organisation's relationship with the data subjects whose data is being processed? E.g. are the data subjects service users or staff of the organisation?	
How much control will these individuals have over their data? E.g. will there be any restrictions on their ability to exercise their data protection rights?	
Would they expect the organisation to use their data in this way?	
Do the data subjects include vulnerable groups?	
What technical measures will be in place to secure the data? (E.g. laptops/ desktops encrypted and password-protected, restricted access to databases/systems, hard copy files/ handwritten notes securely stored away in locked filing cabinets at the end of each day).	

What organisational measures will be in place to secure the data? (E.g. GDPR training for all staff, data breach protocols in place, ICT usage policy, access management policy).	
Are there any prior concerns over this type of processing (E.g. in terms of security) or issues of public concern that your organisation needs to factor in?	
Purposes of the processing	
What does your organisation want to achieve by processing this personal data?	
What impact/effect will this processing have on individuals?	
What are the benefits of the processing? Both to your organisation and to data subjects more generally?	
What is your lawful basis for processing this personal data? E.g. which of the 6 lawful bases under Article 6 GDPR (and Article 9 if you are processing special category personal data) are applicable in this case? If you are processing data to comply with a legal obligation, please specify the specific provisions/sections of the primary legislation.	
Does processing this personal data help you to achieve your intended purpose? Please explain how you have come to this decision.	
Is there any other way you could achieve this purpose that does not involve processing this personal data? Please explain.	
How will you ensure that this personal data is not used for any other purpose than the one for which it was originally processed?	

How will you ensure that the data remains accurate and up to date?	
How will you ensure that you only collect the minimum amount of data required for the purposes of the project?	
What information will you give individuals about the processing of their data and their data protection rights (e.g. in the context of a Privacy Policy)? If the data subjects are at-risk adults, organisations should note that those persons have a right to this information and it should be provided to them, where feasible taking into account their capacity, in clear, concise language that they can easily understand.	
What measures do you take to ensure processors (e.g. third-party software providers) comply with their obligations?	

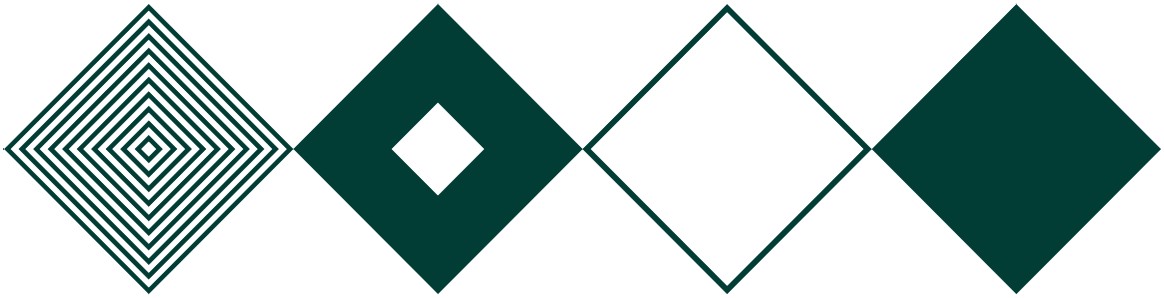


Step 3: Consult with Stakeholders

You should consult with internal stakeholders with a view to identifying the technical aspects of information collection, storage and processing, and how the different elements of the project will fit together in operation. You may also want to consult with external partners, who may be engaged by your organisation as a data processor, or to whom information might be disclosed as part of a project.

It is also advisable to consult with at-risk adults and their family members as appropriate. Seeking their views at the DPIA stage can give individuals an opportunity to voice their concerns about a particular project before it goes live and gives the organisation the opportunity to mitigate any risks that might be highlighted by them. It can also greatly assist the organisation with its transparency obligations.

How and when will you consult with individuals (data subjects) to obtain their views?	
Is there anyone else internally within the organisation that needs to be consulted?	
Are there any external stakeholders that should be consulted? (E.g. service providers engaged by the organisation as a data processor, or other organisations to whom information might be disclosed as part of the project?)	



Step 4: Identify the risks posed and the mitigating measures to be applied

This section identifies the potential risks posed to individuals (or more broadly) as a result of your organisation's proposed processing activities. Article 35 GDPR requires data controllers **to identify and assess** any potential risks to the rights and freedoms of data subjects and to **identify the measures** envisaged to **address these risks** (e.g. safeguards and security measures and mechanisms). The DPC has provided an example below for assessing risk, which organisations can feel free to adjust as they see fit (e.g. add more categories, adjust the weighting, etc.). However, please be advised, **this is just an example**.

Likelihood of risk occurring	
	Highly unlikely – 1
	Unlikely – 2
	Possible – 3
	Likely – 4
	Highly likely – 5
Severity of risk	
	Negligible – 1
	Minor – 2
	Moderate – 3
	Major – 4
	Critical – 5
Overall risk score	
	Very low – 1-5
	Low – 6-10
	Medium – 11-15
	High – 16-20
	Very High – 21-25

Risk assessment template

FOR ILLUSTRATIVE PURPOSES ONLY, the DPC has provided an example of two risks that may occur in the specific context where an organisation is considering the deployment of a 24/7 CCTV system in the recreation room of a day centre for adults with intellectual disabilities for the purposes of ensuring health and safety.

There are a number of additional risks that organisations would need to consider, document, assess and for which they would need to implement mitigation measures.

THIS EXAMPLE IS PROVIDED FOR ILLUSTRATIVE PURPOSES ONLY AND DOES NOT PURPORT TO BE COMPLETE, NOR DOES IT IMPLY THAT THE DPC ENDORSES THE DEPLOYMENT OF CCTV IN DAY SERVICE CENTRES.

Risk No.	Description of risk and the potential impact on individuals	Inherent risk (e.g. without any controls in place) (Likelihood of risk occurring x severity of risk, e.g. 3 x 4 = 12 = Medium risk)	Proposed mitigations	Residual risk (e.g., after mitigating measures have been implemented) (Likelihood of risk occurring x severity of risk)
1	There is a risk that the collection of personal data may extend beyond the confines of the recreation rooms to areas where service users may have a stronger expectation of privacy (e.g. bathrooms, changing rooms).	Likelihood (3) x Severity (4) = 12 - **Medium risk**	The organisation will ensure that cameras are only installed in parts of the recreation rooms where bathrooms or changing areas cannot be captured by CCTV. Cameras in the recreation room will only be turned on during specific periods of the day where there has been a documented track record of health and safety incidents. Cameras will only be turned on when service users are not under the direct care or supervision of staff.	Likelihood (2) x Severity (3) = 6 - **Low risk**
2	The deployment of a 24/7 CCTV system could amount to a level of personal data processing that is excessive, disproportionate and unnecessary.	Likelihood (5) x Severity (5) = 25 - **Very high risk**	Instead of a 24/7 recording system, cameras in the recreation room will only be turned on during specific periods of the day where there has been a documented track record of health and safety incidences. Cameras will only be turned on at times when service users are not under the direct care and supervision of staff.	Likelihood (2) x Severity (5) = 10 - **Low risk**

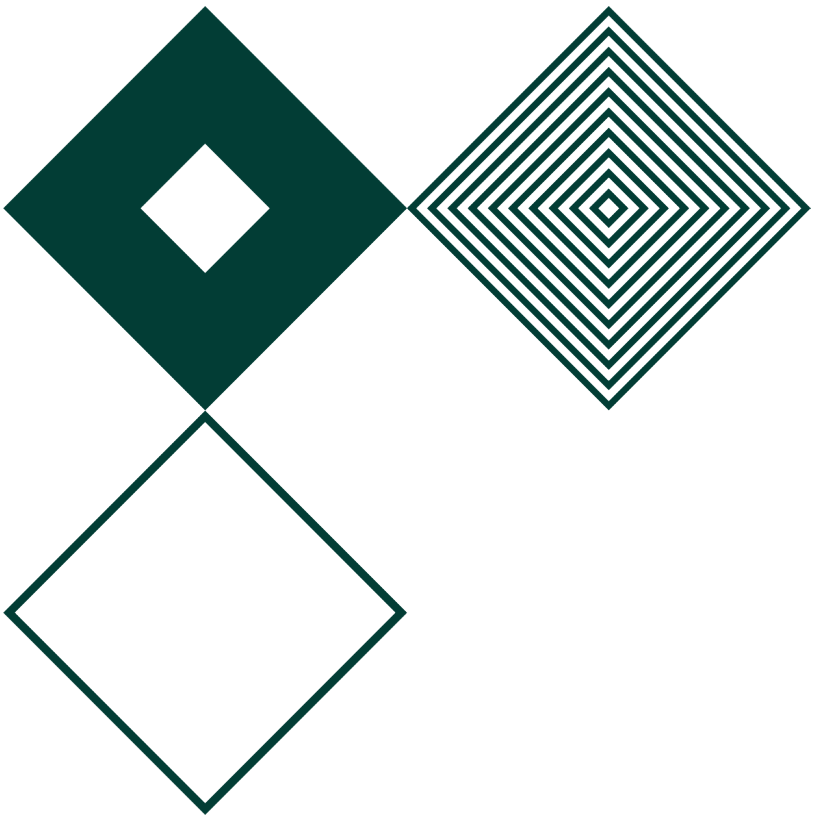
Step 5: Document outcomes and recommendations from DPIA

Item	Name/Title/Date	Comments
Measures to mitigate risks approved by:		Timelines for implementation, parties involved, etc.
Residual risks approved by:		N.B: If your organisation is accepting and undertaking residual high activities (e.g. mitigating measure haven't sufficiently reduced the risk), it must **consult with the DPC** before starting the project.

DPO Advice (where applicable)
[Provide a summary of the advice given by the DPO on the project and whether this advice will be implemented. Where the advice is not going to be followed, an explanation justifying the decision should be provided.]

Step 6: DPIA approval

Approval decision:	Approved or Not Approved or Consult with the Data Protection Commission
Approval by:	[Name and title]



Appendix 4
Further Reading and Useful Links[4]

EU LAW AND NATIONAL LAW	
GENERAL DATA PROTECTION REGULATION **(GDPR)** (Regulation (EU) 2016/679)	GDPR
DATA PROTECTION ACT 2018	Data Protection Act 2018
LAW ENFORCEMENT DIRECTIVE **(LED)** (Directive (EU) 2016/680)	LED
DATA SHARING AND GOVERNANCE ACT 2019	Data Sharing and Governance Act 2019
DATA PROTECTION ACT 2018 **(ACCESS MODIFICATION) (HEALTH) REGULATIONS 2022** (S.I. No. 121/2022)	(Access Modification) (Health) Regulations
DATA PROTECTION **(ACCESS MODIFICATION) (SOCIAL WORK) REGULATIONS, 1989** (S.I. No. 83/1989)	(Access Modification) (Social Work) Regulations
ASSISTED DECISION-MAKING (CAPACITY) ACT 2015	ADMCA
CRIMINAL JUSTICE **(WITHHOLDING OF INFORMATION ON OFFENCES AGAINST CHILDREN AND VULNERABLE PERSONS)** ACT 2012	Criminal Justice (Withholding of Information on Offences Against Children and Vulnerable Persons) Act
HEALTH ACT 2007 **(CARE AND WELFARE OF RESIDENTS IN DESIGNATED CENTRES FOR OLDER PEOPLE)** REGULATIONS 2013 (S.I. No. 415/2013)	(Care and Welfare of Residents in Designated Centres for Older People) Regulations
HEALTH ACT 2004	Health Act 2004
HEALTH AND SOCIAL CARE PROFESSIONALS ACT 2005	Health and Social Care Professionals Act 2005
NATIONAL VETTING BUREAU **(CHILDREN AND VULNERABLE PERSONS) ACT 2012**	National Vetting Bureau (Children and Vulnerable Persons) Act 2012

4) Please note that all hyperlinks in this guidance were checked for accuracy at the time of final draft.

DPC GUIDANCE[5]	
DATA PROTECTION **BASICS**	Data Protection Basics
SUBJECT ACCESS REQUESTS: A DATA CONTROLLER'S GUIDE	Subject Access Requests: A Data Controller's Guide
GUIDANCE ON THE **PRINCIPLES** OF DATA PROTECTION	Guidance on the Principles of Data Protection
REDACTING DOCUMENTS AND RECORDS	Redacting Documents and Records
FUNDAMENTALS FOR A **CHILD-ORIENTED APPROACH** TO DATA PROCESSING	Fundamentals for a Child-Oriented approach to Data Processing
GARDA VETTING – SOME DATA PROTECTION CONSIDERATIONS	Garda Vetting – some data protection considerations
QUICK GUIDE TO GDPR **BREACH NOTIFICATIONS**	Quick Guide to GDPR Breach Notifications
GUIDE TO **DATA PROTECTION IMPACT ASSESSMENTS** (DPIAS)	Guide to Data Protection Impact Assessments (DPIAs)
GUIDANCE ON **ANONYMISATION AND PSEUDONYMISATION**	Guidance on Anonymisation and Pseudonymisation
GUIDANCE ON **APPROPRIATE QUALIFICATIONS** FOR A **DATA PROTECTION OFFICER** (DPO)	Guidance on Appropriate Qualifications for a Data Protection Officer (DPO)
GUIDANCE FOR CONTROLLERS ON **DATA SECURITY**	Guidance for Controllers on Data Security
GUIDANCE ON **LEGAL BASES** FOR PROCESSING PERSONAL DATA	Guidance on Legal Bases for Processing Personal Data
GUIDANCE FOR DATA CONTROLLERS ON THE USE OF **CCTV**	Guidance for Data Controllers on the use of CCTV
DATA PROTECTION TOOLKIT FOR SCHOOLS	Data Protection for Schools
DPC CASE STUDIES MAY 2018 – MAY 2023	Case Studies
INFOGRAPHICS FOR ORGANISATIONS	Infographics for Organisations
GDPR READINESS SELF-ASSESSMENT CHECKLIST FOR DATA CONTROLLERS	Self-Assessment Checklist

5) To access the full list of DPC guidance documents please visit our website: https://www.dataprotection.ie/en/dpc-guidance

KNOW YOUR **OBLIGATIONS**	Know your Obligations
FAQs (Frequently Asked Questions)	FAQs
FAQ – Can I use the GDPR to have my medical records amended or erased?	Medical Records
FAQ – How do I make a privacy policy?	Privacy Policy
FAQ – What do I do if there is a security breach?	Security Breach
FAQ – What security measures should I have in place to protect personal data from unauthorised processing?	Security Measures
FAQ – How long should personal data be held to meet the obligations imposed by the GDPR?	Retention Periods
FAQ – What should be contained in a contract between a data controller and a data processor?	Contract between Data Controller and Data Processor
EDPB GUIDANCE	
GUIDELINES, RECOMMENDATIONS, BEST PRACTICES FOR ALL MATTERS RELATING TO GDPR	EDPB Guidance

Notes

www.dataprotection.ie

6 Pembroke Row
Dublin 2
D02 X963
Ireland

01 7650100 or 1800 437 737

An Coimisiún um
Chosaint Sonraí
Data Protection
Commission