General Data Protection Regulation (GDPR) Frequently Asked Questions (FAQs)

1. What is the GDPR?

The GDPR is European Union (EU) data protection regulation. The GDPR is designed to give patients, service users and staff of the HSE more control over their personal data and ensure that we are taking the appropriate amount of care with personal data.

2. What are the main GDPR principles?

- Personal data must be processed in a transparent manner
- We must have a specific purpose to collect the data
- We must ensure the data is only kept for as long as needed to fulfil the purpose. Our current policy is to retain medical records in line with the HSE Records Retention Policy.
- Where data is held on computers, we must ensure that those computers and networks are safe and secure
- Where data is in paper format, we are obliged to ensure that it is as safe and secure as a computer record

3. How can I become compliant with GDPR?

The HSE is actively working on developing a National Data Protection Office to support and advise you with your data protection responsibilities. Data protection and the GDPR is everyone's responsibility – whatever your position in the HSE you should ask yourself

- Have I identified the personal data that I hold? Any data that can identify a living person is personal data.
- Have I and my organisation identified the lawful basis on which I'm processing this data?

Here are some practical steps that you can take:

1. Make an inventory of all personal data processing that is happening in your area
2. Make an inventory of all of the personal data you are storing
3. Review all Data Privacy Notices in your public and staff areas and on websites

4. Ensure you communicate to individuals in advance of processing relating to: legal basis for processing, retention period, right of complaint, whether data will be subject to automated decision making
5. Review your procedures to ensure compliance
6. Review your procedures for dealing with access requests
7. Examine your legal basis for processing data and document it. This needs to be clearly stated in plain English on your Privacy Notices
8. Examine where you require consent and ensure that there are adequate procedures and processes for this
9. Review the processing of personal data of Children
10. Review your data breach reporting and ensure your staff are aware of them
11. Review your data processing and associated systems to determine whether a DPIA is needed
12. Designate a Data Protection Champion in your area to monitor data processing (not necessarily full time)

4. What allows the HSE to process data?

As it relates to patients and service users and in the daily delivery of health and social care, the HSE gathers and processes personal data, and sometimes sensitive personal data. Health data and other sensitive data can be processed for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of medical care, treatment or social care, for the management of health or social care systems and services, or pursuant to a contract with a health professional. It is expected that the legislation will be more prescriptive in areas like medical research, where specific consent may be required.

5. What information must be given to individuals whose data has been collected?

All service areas and websites must have a ‘data protection & privacy notice’ that will be displayed. It will cover:

- Who is collecting the data
- Why the data is being collected
- The categories of personal data concerned
- Who else might receive it
- Whether it will be transferred outside the EU
- Their right to request a copy of the data
- Their right to lodge a complaint

6. Where to get data protection advice?

The HSE is developing a National data protection office and will appoint an independent Data Protection Officer. Deputy Data Protection Officers (DPO's) within the Consumer Affairs division can provide advice and will determine if escalation to the National data protection office is appropriate.

Deputy Data Protection Officer West, (excluding voluntary agencies) **Consumer Affairs, Merlin Park University Hospital, Galway.** • **CHO 1 – Cavan, Donegal, Leitrim, Monaghan, Sligo** • **Community Healthcare West – Galway, Mayo, Roscommon** • **Mid-West Community Healthcare – Clare, Limerick, North Tipperary.** • **Saolta Hospital Group**	Email: ddpo.west@hse.ie Phone: 091-775 373
Deputy Data Protection Officer Dublin North-East (excluding voluntary hospitals and agencies) **Consumer Affairs, HSE Dublin North East, Bective St., Kells, Co Meath.** • **Midlands, Louth, Meath Community Health Organisation** • **Community Health Organisation Dublin North City & County** • **CHO 6 – Dublin South East, Dublin South & Wicklow** • **RCSI Hospital Group** • **National Children's Hospital**	Email: ddpo.dne@hse.ie Phone: Kells Office: 046-9251265 Cavan Office: 049-4377343
Deputy Data Protection Officer Dublin mid-Leinster (excluding voluntary hospitals and agencies) **Consumer Affairs, HSE, Third Floor Scott Building, Midland Regional Hospital Campus, Arden Road, Tullamore, Co. Offaly.** • **Dublin Midlands Hospital Group** • **Ireland East Hospital Group** • **Community Healthcare Dublin South, Kildare & West Wicklow**	Email: ddpo.dml@hse.ie Phone: Tullamore Office: 057-9357876 Naas Office: 045-920105
Deputy Data Protection Officer South (excluding voluntary hospitals and agencies) **Consumer Affairs, HSE South, Ground Floor East, Model Business Park, Model Farm Road, Cork. Eircode: T12 HT02** • **Cork & Kerry Community Healthcare** • **CHO 5 – Carlow, Kilkenny, South Tipperary, Waterford & Wexford** • **UL Hospital Group** • **South South-West Hospital Group**	Email: ddpo.south@hse.ie Phone: Cork Office: 021 – 4928538 Kilkenny Office: 056 -7785598.

7. What is a Subject Access Request (SAR)?

A SAR is a request made by an individual for their personal information. If an individual makes a SAR and their personal information is being processed, they are entitled to receive the following information:

- the reasons why their data is being processed;
- the description of the personal data concerning them;
- anyone who has received or will receive their personal data; and
- details of the origin of their data, if it was not collected directly from them.

Please note that the HSE does not hold records for Private or Voluntary hospitals and that requesters should apply directly to those hospitals to obtain their records.

The information must be provided free of charge unless the request is 'manifestly unfounded or excessive'.

8. What is a personal data breach?

A personal data breach is a 'breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'. All data protection incidents and suspected data protection breaches must be documented and must be reported to a deputy DPO immediately. If there is or is likely to be a significant detrimental impact on individuals, the individuals must be notified. All suspected IT Security breaches must be reported to the OoCIO and deputy DPOs as per HSE policy.

Deputy Data Protection Officer West, (excluding voluntary agencies) **Consumer Affairs, Merlin Park University Hospital, Galway.** • **CHO 1 – Cavan, Donegal, Leitrim, Monaghan, Sligo** • **Community Healthcare West – Galway, Mayo, Roscommon** • **Mid-West Community Healthcare – Clare, Limerick, North Tipperary.** • **Saolta Hospital Group**	Email: ddpo.west@hse.ie Phone: 091-775 373
Deputy Data Protection Officer Dublin North-East (excluding voluntary hospitals and agencies) **Consumer Affairs, HSE Dublin North East, Bective St., Kells, Co Meath.**	Email: ddpo.dne@hse.ie Phone: Kells Office: 046-9251265 Cavan Office: 049-4377343

• **Midlands, Louth, Meath Community Health Organisation** • **Community Health Organisation Dublin North City & County** • **CHO 6 – Dublin South East, Dublin South & Wicklow** • **RCSI Hospital Group** • **National Children's Hospital**	
Deputy Data Protection Officer Dublin mid-Leinster (excluding voluntary hospitals and agencies) **Consumer Affairs, HSE, Third Floor Scott Building, Midland Regional Hospital Campus, Arden Road, Tullamore, Co. Offaly.** • **Dublin Midlands Hospital Group** • **Ireland East Hospital Group** • **Community Healthcare Dublin South, Kildare & West Wicklow**	Email: ddpo.dml@hse.ie Phone: Tullamore Office: 057-9357876 Naas Office: 045-920105
Deputy Data Protection Officer South (excluding voluntary hospitals and agencies) **Consumer Affairs, HSE South, Ground Floor East, Model Business Park, Model Farm Road, Cork. Eircode: T12 HT02** • **Cork & Kerry Community Healthcare** • **CHO 5 – Carlow, Kilkenny, South Tipperary, Waterford & Wexford** • **UL Hospital Group** • **South South-West Hospital Group**	Email: ddpo.south@hse.ie Phone: Cork Office: 021 – 4928538 Kilkenny Office: 056 -7785598.
Office of the Chief Information Officer (OoCIO)	Email: chris.meehan@hse.ie

9. What is a data controller?

Data controllers are senior managers who decide how the service is delivered and therefore decide how personal data will be processed. A controller could be a person, group of people, or an organisation.

10. What is a data processor?

Data processors are those that processes personal data on behalf of the controller. This does not include an employee of the controller who processes data during the course of

their employment. A data processor can be held liable if they are responsible for a data protection breach.

11. What is data processing?

Processing in relation to personal data is an operation or set of operations performed on personal data including – collecting, recording, organising, structuring, erasing, destroying, altering, combining or disclosing the data.

12. What is profiling?

Profiling means any form of automated processing of personal data consisting of the use of the data to evaluate certain personal aspects relating to an individual, including to analyse or predict aspects concerning the individual's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movement. Data subjects have the right to object to an automated decision made without human intervention.

13. How do we deal with requests to have personal data rectified?

Individuals have the right to have personal data rectified if it is incorrect or incomplete. If the data has been disclosed to a third party then they must also be notified. This doesn't extend to a medical opinion where the data was recorded accurately with the opinion in question.

14. How long can data be retained?

The length of time data can be retained depends on the type of data. Full details of how long each type of data can be retained can be found in the HSE Record Retention Policy.

15. What is a Data Protection Impact Assessment (DPIA)?

A DPIA is a mechanism for identifying, quantifying and mitigating the risks associated with the processing of data. A DPIA is undertaken to ensure appropriate controls are in place when a new process, system, or way of working involving high risk processing, for example the processing of sensitive health related data.

More information regarding GDPR can be found on the European Commission website: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

Index