Just one month until GDPR legislation passes - **is your pharmacy ready?**

By Richard Kelly

One of the biggest issues facing Irish business and indeed business throughout the EU will be the passing into EU statute of the General Data Protection Regulations legislation on May 25th. Whilst the legislation itself was adopted in April 2016, the end of the two-year post adoption grace period is fast approaching and with each day that passes, the chatter surrounding the impending changes gets louder.

Richard Kelly, Director, Profit Pharm

Profile

Richard Kelly, Director at Profit Pharm, is a qualified and experienced business coach who has been running his own business since 2003, having spent 20 years in various sales, marketing and senior management roles.

Working initially within a variety of business sectors, for the last 10 years Richard has focused particularly on the community pharmacy sector, where he had fantastic results.

Profit Pharm is a new business launching this Spring. Its primary mission is "to support the independence of independents" through helping independent pharmacy build long term, sustainable growth and profit into their business.

Richard says "it's not just about money, it's about looking at every area within the business. Working with a preferred partner model, we are all about using proven and innovative strategies and ideas to produce a return on all spend within the pharmacy business, whether this is marketing, sales, staff, compliance, digital or IT.

"We will help each business become the best it can be. Profit Pharm brings all our experience into one place enabling us to deliver real benefit to the bottom line of each business."

Richard can be contacted on 085 1455 425 or email gdpr@profitpharm.ie for a no obligation discussion.

For some, the early adopters, they have embraced the process, are implementing change in their business and are well on their way to being compliant. It would appear that for most businesses however, this is not the case, with many now playing catch up now that the compliance date is looming.

Why the Change?

One of the first questions people ask is "Why change?" In many ways, much of the intrinsic content of the existing Data Protection Legislation remains, however, the fundamental change is to give all EU citizens (each a data subject) full control over the collecting, use and storage of any personal data held by any organisation that relates to them.

The EU constitute personal data as "Any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address."

Another key difference is that GDPR is a legal regulation, fully enforceable from May 25th, rather than an EU directive as was previously the case. Each country took the directive into law within their own jurisdiction whereas now, with GDPR, there is no requirement for the State bring into law, although there is an Irish bill currently on the way. This legal change will harmonise Data Protection Legislation throughout the EU, making the management and control of data much easier.

Key Changes – What's different?

Registration

To date, the only actual relationship with the Data Protection Commissioner for most businesses was a simple registration process and the payment of a fee. In return, a certificate was issued and you were compliant. It is a PSI requirement to hold an in-date certificate.

With GDPR, there will no longer be any requirement to register with the Commissioner. From May 25th, it is expected that those businesses that need to be compliant, will be. Indeed, the Data Protection Commissioner Helen Dixon has warned Irish companies "that there will be no leeway or second chances for non-compliance of the new rules". If an Inspector is standing at your door on May 26th, you are expected to be compliant.

Accountability

As I mentioned earlier, Accountability is the cornerstone of GDPR and under Article 24 it states " The legal requirement for Data Controllers (legal entity who determines how data is

collected, processed and used within an organisation) and Data Processors (person that processes data on behalf of the Data Controller) to demonstrate that all appropriate measures have been put in place to meet GDPR compliance guidelines". What does this mean in reality?

From a compliance standpoint, you will need to review all the personal data you hold (for patients /customers and also your staff).

Frame the review with questions such as:

Why am I storing this information?

How did I obtain it?

Do I require or have the appropriate consent?

How long do I need to keep it?

Is it stored securely?

Who needs access to it or more importantly….who doesn't

Have I completed due diligence on and have written contracts for third party organisations with which I share information. (McLernons / Clanwilliam / Touchstore?)

How often do I audit / review these processes?

To be compliant, you will need to demonstrate, generally through written policies and procedures, that you have measures in place to manage these questions.

In addition, with GDPR, liability for breaches of Data Protection now extend to Data Processors as well as Data Controllers, so both Pharmacists, Technicians and Admins have a responsibility to maintain and observe GDPR protocols.

Legal Basis for collection of Data

A description of your legal basis for collection of data should be included in your Privacy Statement. This should detail Lawfulness, Transparency and Fairness aspects of your processing activities. Detail pertaining to Purpose Limitation, Data Minimisation, Storage Limitation should also be included

CCTV information is an area that can give rise to various legal interpretations. You should have a very clear and unambiguous statement as to what your CCTV system is used for.

Consent

With the new legislation, the bar has been raised considerably in regard to obtaining consent to process personal data:-

All requests for consent should be in clear and unambiguous language with the purpose for data processing clearly stated. The Data subject should also be advised that they can withdraw consent at any time. If the consent relates to permission to market electronically, then each mail sent should always include an "opt out" or unsubscribe option. It should be as easy to withdraw consent as it was to give it.

The default position in now "opt in" so, for example where previously a registration form for a loyalty card may have said "tick the box if you do not want to receive etc.", playing on peoples general aversion to ticking boxes meant that no tick meant they were "in"…going forward, the box should only indicate a request to receive info etc. Care should be taken initially to fully determine the amount of information required for each activity, as consent as the only legal basis to proceed is a weak defence should it's need be challenged.

Personal Privacy Rights

The personal privacy rights of the individual are now greatly enhanced with GDPR

Brief overview of each below:-

- **Right of Access**
  - Confirmation that their data is being processed
  - Access to their personal data
  - Other supplementary information – (this should be contained in your privacy statement

Individuals have a right to request a copy of any personal data relating to them whether held electronically or hard copy. Ideally, the request should be made in writing and identity verified before proceeding. The information must be supplied (free of charge) within one month of request (previously 40 days).

There are a number of scenarios in which access to data can be restricted or refused. These are outlined fully in the regulations, however in the main they centre around the protection of health and wellbeing of the individual. Any general conditions that warrant refusal of an access request should be outlined in your Privacy Statement.

Your documented processes should include a section on Managing and Fulfilling Access requests.

- **Right to rectification**
  - The GDPR gives individuals the right to have personal data rectified.
  - Personal data can be rectified if it is inaccurate or incomplete.
- **Right to Erasure (Right to be forgotten)**
  - The right to erasure is also known as 'the right to be forgotten'.
  - The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.
- **Right to restriction of processing**

Individuals have the right to limit the extent to which their data is used. For example, you might get consent regarding marketing on a particular subject or product. Use of data could be restricted to just this and not other generalised marketing.

- **Right to Object**

Individuals have the right to object to:

  - Processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling)
  - Direct marketing (including profiling)
  - Processing for purposes of scientific/historical research and statistics.

With the exception of Direct Marketing, there may be circumstances regarding the two remaining criteria that can refuse to comply with the objection

- **Right to Data portability**

An individual has the right to request that their information is transferred to another pharmacy, there are no grounds for non-compliance with the request. All requests must be expedited within one month.

Data Breach

With such a strong focus on the rights of the individual being paramount, it follows therefore that any data breach should be treated with the same level of importance.

From May 25th, all data breaches must be reported to the Data Protection Commissioner within 72 hours. The report should detail the nature of the breach, the likely scale of impact on those whose information has been compromised. In cases where identity or financial / health details could be compromised, the Data Controller must inform the individuals concerned.

By default, you should have a Data Breach log and a detailed Data Breach response procedure.

Fines and other penalties

Worth pointing out at this stage the actions / sanctions that the Commissioner can take in the event of non-compliance or a data breach

A written warning in the case of a first-time non-intentional non-compliance.

Tier 1 – a fine of up to €10m or 2% of gross annual turnover (whichever is the greater) for the full preceding trading year

Tier 2 – a fine of up to €20m or 4% of gross annual turnover (whichever is the greater) for the full preceding trading year

In addition to financial penalties, the Commissioner has the right to seize equipment, ie computers etc and /or order all data collection activities within a business to cease immediately.

Data Protection Officer

There are a number of public and private sector areas where the appointment of a Data Protection Officer is mandatory.

GDPR

Ireland's Data Protection Commissioner Helen Dixon

The jury is out however as to at what level you don't need one. Given the scope of the changes involved and the potential to fall foul of the regulations especially in the early stages, it might be worth considering appointing a staff member as a Data Protection or Privacy lead in your business, or using an external provider on a retained basis. It is important now that GDPR will be law to ensure that Data Protection is at the core of what you do. The Data Controller cannot be this person as there is an obvious conflict of interest. The role is an advisory and compliance ready one: informing and advising on legal obligations relation to data processing; monitor continued compliance with legislation through audit and review; build awareness through training and also as a liaison and conduit of information with the Supervisory Authority.

Privacy Statement

Your pharmacy should produce a Privacy Statement which outlines the following as a minimum:-

Identity of Data Controller and Processors

Category of Data that is collected

Purpose for collection

Collected from where?

Is the data shared and if so, who with

How long is it kept for?

List the Individuals rights as outlined above

Once completed this should be made available on request and/ or displayed within the pharmacy

Online and Web

If you operate a website and especially an online shop, participate in Social Media marketing, ie Facebook, Instagram, Snapchat etc, you need to review all of the above in the context of the information you gather through the site. You need to produce a separate online privacy statement that covers collection methods, cookies etc. This need to be published on your website with access via a visible tab or button called Data Protection

Yes, I get it, but where do I start?

As the old saying goes... "Start with the end in mind". By the 25th May, you need to be able to demonstrate you are compliant, so it makes sense to work out exactly where you are today?

As there is no certification process, in reality, it's a bit like an NCT for your car, at that time, on that day, your car was deemed roadworthy.

Complying with GDPR is a continuous process, with 25th May being more of a beginning than an end. That said however, a great way to show intent is to audit all the areas discussed in this article…if you've ever carried out a risk analysis for HACCP or Health and Safety, adopt a similar approach.

Establish in each area where you are today against what's required, this give you your initial gaps. Prioritise which tasks need doing first, who will do them, by when etc. Once each one is completed, you can move to the next and so on. The benefit of this approach is that will be able to demonstrate measurable progress to a fully compliant position. All the processes and corrective action you take should be documented and form part of your Data Protection operational folder.

In terms of your mindset, use the same methodology and processes that currently exist in your pharmacy. I imagine you adopt an "inspection ready" state as your pharmacy default. You never know when a PSI Inspector will arrive going forward, this is the mindset you should adopt for Data Protection

Urgent, but not too late – just get started

Hopefully this article has given you a flavour and some insight into what is required from you to make your pharmacy business compliant with the new GDPR legislation.

Here are some useful resources

www.profitpharm.ie
www.gdprandyou.ie
www.eugdpr.org

Is your pharmacy business compliant with GDPR legislation? **Grab a pen**

Score your business (1 "not compliant" to 5 "fully compliant") across the following areas to help start your gap analysis

1. I have documented what personal data I hold, where it came from, who I share it with and what I do with it.
2. I have identified my lawful bases for processing and documented them
3. I reviewed how we ask for and record consent
4. I have systems to record and manage ongoing consent
5. I have provided privacy notices to individuals
6. I have a process to recognise and respond to individuals' requests to access their personal data
7. I have processes to ensure that the personal data I hold remains accurate and up to date.
8. I have an appropriate data protection policy
9. I provide data protection awareness training for all staff
10. I have a written contract with any data processors I use
11. I have an information security policy supported by appropriate security measures.
12. I have effective processes to identify, report, manage and resolve any personal data breaches.

Obviously the closer to 60 you are the better…… however, what important is to get started, use your lowest scoring areas to help prioritise your corrective action plan.