GDPR Post Apocalypse

(25th May 2018)

James Devoy, CSO

The General Data Protection Regulation (**GDPR**) became enforceable on 25th May 2018 and has been much likened to Y2K in that, both have come and gone, both had major hype, both resulted in lots of consultancy fees, both meant a lot of IT rework and money to spend, both sent fear into all those concerned and both resulted in mass hysteria, panic and nonsensical actions.

The similarity doesn't end there, as at the actual point in time events happened, both resulted in absolutely nothing happening. The world didn't end, time didn't stop and the sky didn't fall in, but there is one difference. Y2K was a point in time January 1st, 2000 @00:00:01, the **GDPR** needs to be considered in the weeks, months and years beyond May 2018.

The 25th of May was a line in the sand, an enforcement date, and save for a barrage of opt-in again emails and many non-EU websites closing their websites to EU countries, nothing else has happened, yet. The effects of the **GDPR** are coming but should we still be worried?

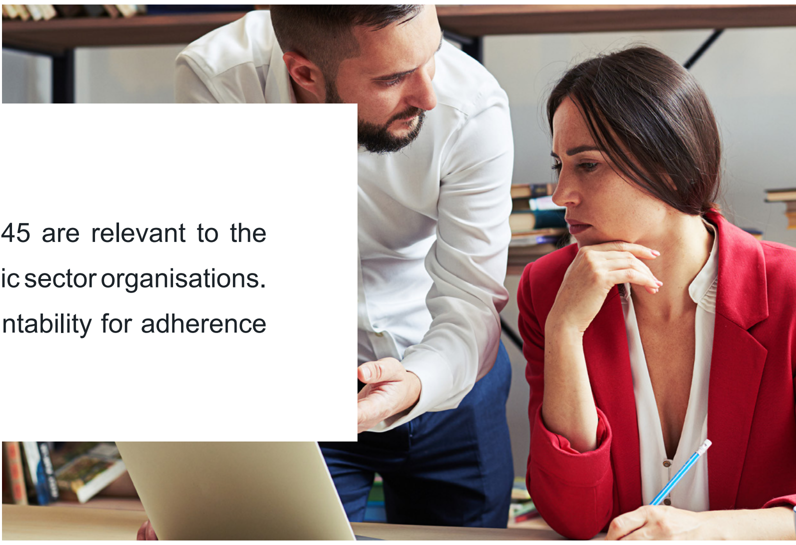
The UK Information Commissioner Elizabeth Denham has dismissed all the predictions and scaremongering of huge fines as 'nonsense' and has advised that the Information Commissioner's Officer (ICO) will use its power "proportionately and judiciously" and fines that are to be levied will always be as a last resort. Last year the ICO investigated 17,300 cases and only 16 of them resulted in fines for the organisations concerned.

Denham goes on to say:

"those who self-report, engage with us to resolve issues and can demonstrate effective accountability arrangement can expect this to be taken into account when we consider any regulatory action".

The hefty fines will be reserved for organisations that persistently, deliberately or negligently flout the law. Worthy of mention here is that the **GDPR** is a pan EU regulation which is now enshrined in UK law as the Data Protection Act 2018 (DPA18) replacing the former DPA98.

Why is it so complex?



Actually, it isn't!

The **GDPR** has 99 articles, however only the first 45 are relevant to the average business, the rest are for Government or public sector organisations. Data Controllers are required to demonstrate accountability for adherence to the six principles of the **GDPR** under Article 5 i.e.

1. Lawfulness, fairness and transparency
2. Purpose limitation – collected for specified, explicit and legitimate purposes
3. Data minimisation – adequate, relevant and limited to the purpose for which they are processed
4. Accuracy – and kept up to date and where inaccurate, rectified or erased without delay
5. Storage limitation – held in a form which permits identification of the data subject for no longer than necessary
6. Integrity and confidentiality (security) – adequately protected against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical measures

One method of demonstrating accountability is to take your processing activities through formal risk management, examining your record of processing activities created from your data discovery exercise:

- Identify where you process personal data and enter this into a risk register with details of the type and quantity of processing activity
- Identify typical threats and vulnerabilities to that data
- Assess the impact that loss, disclosure or damage might cause
- Identify what the risk appetite of your organisation is
- Identify what the probability of threats being realised is
- Identify any current controls and re-evaluate to determine the residual risk
- Identify further risk treatment and set realistic targets for treatment
- Formally document the results of your risk assessment

Following on from your risk assessment, continuously review the assessment and controls and re-evaluate any changes that might affect the impact or probability. Think about adding privacy enhancing controls such as pseudonymisation and encryption.

Above all else

Train staff to ensure that they are aware of their responsibilities for information security and especially for data breaches so that they know how to recognise and report a breach. Create an Incident Management plan, including breach response, include how and to whom a breach should be reported. Designate an individual or individuals to be responsible and create processes for reporting notifiable breaches to the supervisory authority and the data subjects. Test that the data breach incident procedure works for you and that you can manage a breach properly. Give staff regular refresher training and check for adherence to a code of conduct.

> **Update your Privacy Policy on your website, ensure that it is honest.**
> **Consider your lawful bases for processing.**
> **Think about Data Protection Impact Assessments (DPIAs).**
>
> These only actually need to be done for **high-risk** processing.

The definition of high-risk being:

SYSTEMATIC and **EXTENSIVE** automated processing, including profiling that results in decisions

Processing on a **LARGE SCALE** of special categories (basically discrimination), or criminal convictions

Systematic monitoring of **publicly accessible areas** (public CCTV for example)

In most cases, a DPIA will not be required but in cases where it is not clear whether you need a DPIA or not, the Working Party 29 recommends that a DPIA is carried out nonetheless.

Carrying out a DPIA is a useful exercise where there may be any element of risk and helps toward demonstrating accountability. In thinking about DPIAs, think about what projects are coming in your organisation that might need them?

Exercise data protection by design and by default. Create a process which specifies the factors to look for such as type and volume of data, special categories of data or those relating to children.

Address the findings of DPIAs and action any follow up items and for those where the risk cannot satisfactorily be mitigated, detail the actions taken including referral to the supervisory authority and their decision.

Ensure that you have robust processes in place to deal with **Data Subject Access Requests** (DSARs or SARs).

Data subjects can ask about any of the following:

- What their data is used for
- Who it is shared with and to stop sharing (restrict processing)
- How long it is stored for and why
- Where it came from
- If it has been transferred outside of the European Union and if so what security measures were used to protect it
- Whether the data is used for profiling or automated decision making
- They can challenge the accuracy of the data or ask for it to be deleted or object to its use
- They can ask for a copy of it and it must be provided in an electronically readable format
- They can ask for the data to be ported to another data controller

The process to respond to these requests should be documented and made available to all those who may be asked to handle a SAR.

The process may involve designing a form which includes the contact details of the organisation, the person who will handle the request, a reference number (to keep a log of all the SARs for evidence) and a section to steer their end customer to be specific about their request i.e. what specifically do they want i.e. copies of orders made between January and June. Embed any processes created into job functions so that they are at the forefront of the minds of those concerned with them.

The GDPR provides a great opportunity for good data protection practice to pervade your organisation and with support from the top down, you can demonstrate that you have appropriate controls and thinking in place to show your customers, service partners and the regulator that you take the security and usage of personal data seriously.

Consider leveraging your **GDPR** alignment activities by consolidating them into broader information governance programs such as **ISO27001**.
Finally, remember what the Information Commissioner said:

Self-report, engage with us, demonstrate accountability. Don’t be persistent, deliberate or negligent.

sysnet® | Cyber Risk

About Sysnet Cyber Risk

Headquartered in Dublin, with offices in London, Atlanta, Dallas, Poznan, Hyderabad and Cape Town, Sysnet is a **global market leader in Cyber Security, Risk and Assessment services**. Specialising in designing robust business focussed control frameworks.

Sysnet has been a provider of these services **since 1989** and as such has one of the longest pedigrees in the information and cyber security world. Sysnet has an envied global list of clients spread over **60 countries**.

UK +44 (0) 207 868 1630	**Poland** +48 61 631 1230
Ireland +353 (0)1 495 1300	**India** +91 (0)4 06 713 5336
US +1 404 991 3110	**South Africa** +27 (0) 83 629 7514

CyberRisk.Sales@sysynetgs.com

cyber-risk.sysnetgs.com