MAZARS DATA PROTECTION NEWSLETTER

Issue 4

What is the impact of GDPR? One year in and the jury is still out. There have been only 41 published sanctions from data protection authorities across Europe in the first year: 21 of these were imposed by the UK's ICO and 2 from Ireland's DPC. This is less than most of us anticipated at this point. So we still can't see patterns and have little to reference when deciding on the risks we are accepting. This may have as much to do with the transformation that GDPR has driven in the regulators as mentioned further below.

On the flip side GDPR is not, as some suggested it would be, Y2k. The noise from the regulators have been consistent: they expect organisations to continue to mature and focus on demonstrating accountability. For maturing organisations, compliance now means the ability to make educated risk-based compliance decisions and to demonstrate accountability for these.

Elizabeth Denham the UK's ICO stated in May: The focus for the second year of the GDPR must be beyond baseline compliance - organisations need to shift their focus to accountability with a real evidenced understanding of the risks to individuals in the way they process data and how those risks should be mitigated. Well-supported and resourced DPOs are central to effective accountability.

Update on the Irish DPC's key statistic

Ireland's DPC has provided statistics from the first year of GDPR:

6,624 complaints were received

1,206 Data Protection Officer notifications were received

5,818 valid data security breaches were notified

Staffing numbers increased from 85 at the end of 2017 to 137 in May 2019

Over 48,000 contacts were received through the DPC's Information and Assessment Unit.

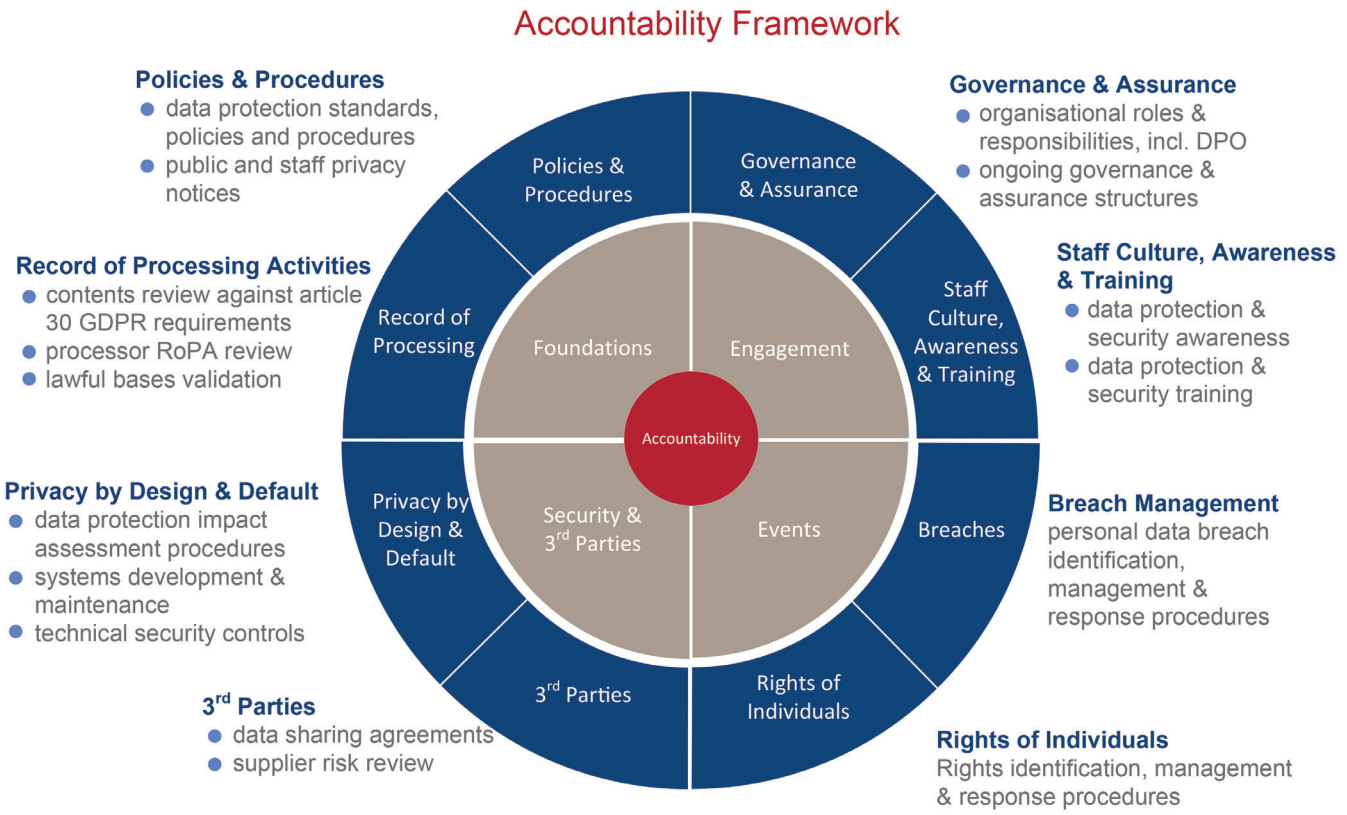
54 investigations were opened
35 of these are non-cross-border investigations and 19 are cross-border investigations into multinational technology companies and their compliance with the GDPR.

The number of DPOs registered looks to be very small in the context of the number of businesses in Ireland that you would expect to need a DPO. Coming back to the accountability principle, having a DPO is key. Where organisations have a DPO and haven't yet registered the individual, they should recognise this is a key part of being accountable. It is easy to register a DPO on the DPC website

Risk-based accountability -what does good look like?

Many organisations across the EEA are challenged to achieve 100% compliance with the GDPR. Question is what is realistic and expected is to be accountable? This includes actively identifying, managing and mitigating GDPR risks as an operational process (a risk log is a must!); having clear roles and responsibilities; demonstrating that you put effort into being complaint and document your discussions and conclusions where you make risk-based decisions.

We use the accountability framework below as the basis for GDPR compliance and, when working as DPO, actively engage members of the management team to understand the requirements and resolve issues.



Difficult data subject? Challenge them on the right they are invoking?

While working as DPO's over the last year we have witnessed letters, emails and phone calls from data subjects wanting to invoke a right under GDPR. Most of these are clear and concise, i.e. the data subject states the right they are invoking. However, some of the communications received are people venting their frustrations, anger and outrage with the organisations and generally attempting to weaponize the GDPR.

The person receiving the communication naturally feels a bit stressed by the manner of the communication and this can lead to the recipient trying to be as helpful as possible. It's not uncommon for the data subject to challenge whether the organization is compliant with GDPR and the temptation for some is to provide evidence that you are. You are not obliged to do this. Go back to the data subject and ask, what right under the GDPR do you want to invoke. Let them tell you, then use your standard approach to process these requests.

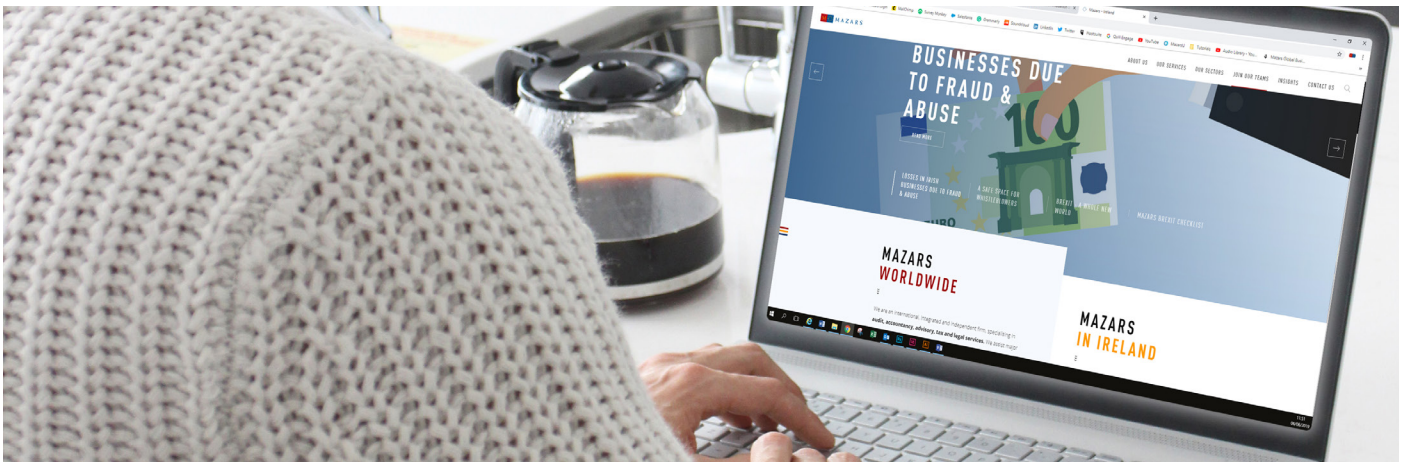
Invisible cookie banners

One visible change from GDPR is the now invisible cookie banners that we all click through in milliseconds without ever reading, and who could blame us, as they generally don't achieve the objective of transparency and choice. We need the ePrivacy directive to come in and hopefully move the situation forward. However, it is not clear when it will be introduced and has already been delayed on several occasions.

Our current understanding of the ePrivacy directive is that it will aim to simplify the rules regarding cookies and streamline cookie consent in a more user-friendly way. This will include;

- Freely provided consent and unambiguous action, the current banner simply informing of the use of cookies or prompting to "accept cookies" will no longer be enough.
- The information on the cookies and consent must be provided in an understandable language, without jargon.
- Propose that consent is no longer required for non-privacy intrusive cookies which improve internet experiencee.g. to remember shopping cart history.
- Users will choose their settings on browsers.

The ICO in the UK has published a very prescriptive draft code of practice for online service providers on age appropriate design. It assumes that, unless you can prove otherwise organisations should assume all service users are children and act accordingly.



Security is where it's at

One area of GDPR that the regulator and consumers clearly care about is the security of personal data. An aspect of security which has received considerable media attention over the last 12 months is cyber-attacks.

But cyber-attacks are just a concern for Facebook, WhatsApp, and big corporations such as Tesco, right? Wrong. With more than 60% of companies reporting at least one attack in 2018, cybersecurity is grasping the attention of both the wider public and businesses of all sizes. Despite large businesses usually receiving the unwelcome media attention, almost half of cybercrime attacks are committed against small businesses (global research firm Cybersecurity Ventures).

So, what exactly is a cyber-attack? It is an attack launched from one or more computers against another computer to gain illegal access for the purpose of causing damage or harm. This includes, but not limited to; phishing, password attack, third party service vulnerabilities and hacking.

From our experience over the last year, we have seen both phishing and hacking where illegal access has been both attempted and gained in medium sized businesses. In some instances, it has initiated an investigation from the DPC with significant financial investment to mitigate the risk quickly.

A recent report by the insurance company, Hiscox, found that nearly 74% of businesses were considered unprepared for a cyber-attack, after failing a cyber readiness test. In our experience, through both our GDPR and IT Security Audit work we are not surprised by this statistic.

How can you protect your business from the threat of cybersecurity?

Change attitudes towards Information Security

Human error is the root cause of a significant number of data breaches. Challenge is, millions of people are often unaware of how their personal data or the information of their organisation could be a target of cyber-attack.

Don't cringe at the word, but, "culture", and staff's attitudes towards security considerations such as not clicking on links/attachments in phishing emails, use of strong passwords, not sharing passwords (certainly not writing them down!), locking computers whilst unattended and clearing desks at the end of the day can make a real difference. We are seeing organisations shift focus from GDPR compliance ticking efforts (e.g. annual training) to influencing ongoing behavior and culture change toward data protection and security. A progression which has been deemed necessary from the GDPR findings over the last year.

Cyber Insurance

It is ultimately for a business to decide whether they feel the cost of cyber insurance outweighs the potential risks such as financial and reputational damage. If the business has an appetite for the risk of no insurance, then they must be prepared for the financial repercussions in the event of an attack. It is worth noting that Cricket Ireland was hit by a 'six-figure' cyber fraud which pushed the organisation into a financial crisis.

Data Protection Impact Assessments

Ensure that all Data Protection Impact Assessments (DPIAs) have been completed to demonstrate that vulnerabilities have been identified and these risks have been mitigated. Where a project or technology has been considered for a DPIA, but deemed not applicable, this must be recorded to demonstrate accountability.

Contacts

If you would like more information please contact:

Liam McKenna, Partner
T: +353 (01) 449 6454
E: lmckenna@mazars.ie

Sarah Hipkin, Director
T: +353 (01) 449 4419
E: shipkin@mazars.ie