MASON HAYES & CURRAN

GDPR: One Year Older But Are We Any The Wiser?

We have survived the first year of living with the GDPR. What has happened in the last 12 months and what can be learnt?

Security breach notifications a plenty

What has happened?

Over 89,000 notifications had been filed since May 2018. With a regime where over-notification suffers no penalty, but failure to notify could incur a fine, one could not blame businesses for taking this approach.

This approach, however, is not without risks. Once a breach is notified, a controller opens itself up to further questions and scrutiny from their regulator on how the risk has been categorised. As regulators further settle into their roles and increase their capacity to investigate breaches, we may see a more cautious approach to notifications emerge with businesses wanting to stay below the radar.

Key takeaway

Businesses should consider stress testing their security breach response policies and procedures. The reality is that many shiny documents prepared to comply with GDPR look great but offer little operational guidance on who needs to do what when a breach hits.

Controllers need to familiarise themselves with the online breach notification forms. The Data Protection Commission's form requests a lot of information about the controller and its business in addition to information on the breach. Ensure you are not looking at the form for the first time while the 72 hour clock ticks down.

Even more complaints

What has happened?

Over 144,000 complaints had been received by regulators since May 2018. The overwhelming reason for these complaints was the failure of controllers to appropriately respond to data subject requests.

Key takeaway

Make sure everyone in your organisation knows what a request looks like and which team needs to know about them as soon as they are received, whether that's legal, compliance or HR. Deal with a request as soon as it is received and make a note of the statutory deadline (one month is not a long time). Ensure you engage with the data subject to acknowledge receipt, update them if you intend to extend the timeframe to respond or to refuse a request. Meaningful engagement reduces risks of complaints or negative regulatory reactions.

Extensive investigations but little high profile enforcement (yet)

What has happened?

With the obvious exception of the CNIL's massive €50m fine of Google, none of the regulators have concluded any very high profile enforcement action to date. It has also been reported that Google intends to appeal the CNIL's fine, which is good news for those concerned by the CNIL's approach (as explained in our Tech Blog post). There is significant investigative work going on however (particularly into the practices of big tech organisations and those in the ad tech industry) and we expect to see a steady increase in enforcement action in the coming months as those investigations conclude.

Key takeaway

Make sure to monitor regulatory activity closely over the next 6-12 months, including the guidance that businesses continue to be inundated with. The unspoken 'grace period' has ended. This first wave of significant GDPR enforcement will provide valuable insight into regulators' priorities for the coming years and their expectation of businesses, what level of fines can be expected going forward, and the mistakes others have made which can be learnt from. Signing up to the MHC Tech Blog is a great way to stay up to date with important developments.

GDPR has had an impact on cookies... while we wait for the ePrivacy Regulation

What has happened?

The much discussed and debated ePrivacy Regulation has still not been agreed. There are major obstacles to overcome to get agreement and it's not clear when this will happen. In the meantime, the existing rules on cookies and tracking technologies have to be interpreted in light of the new higher standard for consent set by the GDPR which creates significant challenges for business.

Key takeaway

Businesses need to look very closely at their use of cookies and technologies and how they obtain consent. Our recent Tech Blog post on a recent opinion of the CJEU Advocate General provides some helpful guidance on what to avoid (namely, relying on pre-ticked boxes or inaction on the part of the user as consent) and what needs to be included in a cookie policy. This makes for essential reading for any website operator.

Living with GDPR

What has happened?

Businesses have come to terms with the fact that 25 May 2018 was not an end point and when it comes to GDPR there will always be more work to do. The GDPR's concept of accountability and the need to 'demonstrate compliance' represents the new regulatory norm. While this creates significant challenges for businesses that does not mean they need to stop being innovative. Carefully considered policies and procedures can enable ongoing compliance without stifling business.

Top 3 tips for the future

Businesses should keep the following in mind when looking at internal compliance over the coming months and years:

- **Get the basics right.** Put in place a transparent privacy notice, ensure you know your legal bases for processing, adopt an appropriate global data transfer program and have tried and tested policies in place to respond to security breaches and data subject rights.
- **Don't be afraid to make changes.** Many businesses implemented compliance solutions in a rush before the 25 May 2018 deadline. If these don't work, they should be replaced or changed. This is not a reflection on your business's compliance. Regulators expect policies and procedures to be reviewed and revised over time.
- **Focus on key risks.** No one is fully compliant across all areas of their business. Resources should be focused on key compliance risks areas and be informed by key regulatory developments.

Key Contact

Brian Johnston
Partner, Privacy & Data Security
+353 1 614 7746
bjohnston@mhc.ie