Data protection newsletter

Issue 12

At the beginning of 2022, the full impact of GDPR is becoming more apparent. The implications of regulatory decisions indicate the bar is rising when it comes to assessing what compliance means. In that context, it is probably not surprising that our 6th annual GDPR survey suggests that respondents' attitudes to GDPR have moved negatively in the last year.

Mazars & McCann Fitzgerald GDPR survey

In December 2021, Mazars and McCann Fitzgerald conducted our 6th annual General Data Protection Regulation ("GDPR") survey, which indicated a negative shift in attitudes to GDPR, including an increase in the perception that the GDPR is seen as an administrative burden on organisations. The report outlines the topics in which organisations had the most concern about, notably the top five are;

1) **Personal data breach notification;** breaches are becoming more common, increasing an organisation's risk of being subject to a phishing attack. Organisations need to ensure their breach management is robust and relevant notification is made where necessary.

2) **Record of processing activities**; stated by the Duty Data Protection Commissioner during the survey results webinar, this will be a focal point for the Data Protection Commission ("DPC") in 2022. The DPC will conduct a review of several organisations' RoPAs, leading to the DPC releasing guidance on the records of processing activities.
3) **Security obligations**; linked to the increasing number of phishing attacks, organisations need to ensure all technical and organisational security measures are reviewed and tested. Weaknesses should be acted upon, and additional measures to facilitate working from home should be considered.
4) **Documenting and evidencing compliance**; organisations are concerned with demonstrating the principle of accountability. Concerns around non-compliance are rising, as is the risk of civil and regulatory fines. Organisations need to ensure robust data governance in place to demonstrate accountability.
5) **Data subject requests**; awareness amongst individuals of their data subject rights has increased. Organisations need to ensure they can facilitate these data subject rights adequately and effectively to reduce the risk of complaints and civil fines.

The report details several other interesting topics and survey results. To read the survey or watch the Mazars and McCann Fitzgerald webinar click here.

Key action: download survey and watch the webinar for some more valuable insight.

Cookie compliance, consent and international transfer

In the last number of months, cookie banners have been a topic of discussion. The requirement of providing a "reject all" button on cookie banners has been received with resistance. Many organisations rely on cookies to improve how they operate and function online. With the introduction of a "reject all" option, organisations believe this will put them at a disadvantage. Data Protection Authorities across Europe have imposed fines on big tech companies for non-compliant cookie banners. They have stated that website users must be able to refuse cookies with the same degree of simplicity as to accept them. The DPC guidance informs us that we do not require a reject all but must have a way to reject all, such as a "manage preferences" selection. However, given the findings from other regulators, this guidance may need updating

The French Data Protection Authority have fined Facebook (renamed Meta) €60 million for inadequately facilitating the refusal of cookies. Similarly, they have also fined Google €150 million under the same grounds.

The recent decisions against IAB Europe by the Belgian Authority and Google Analytics by the Austrian and French Authorities will have far-reaching impacts on the digital space.

The Belgian Authority has ruled that the Transparency and Consent Framework (TCF) relied upon by approximately 80% of websites in Europe is invalid and does not capture proper consent. This means that

the consent you have for all of your cookies may no longer be valid! IAB Europe has been given six months to bring the TCF into compliance.

In recent weeks the use of Google Analytics has been deemed non-compliant with the GDPR. The Austrian and French Authorities have found that the transfer of data to the US as part of the Google Analytics process is non-compliant. The supplementary measures in place are insufficient to mitigate the risks involved with processing data in the US. It is doubtful that a company subject to the Foreign Intelligence Surveillance Act ("FISA") will be able to comply with the requirements.

These findings are a sign of the tough stance regulators are taking on the digital space. For more information, please see our article here.

Key actions: Review your own transparency statements and delete any data that was captured on the basis of assumed consent or legitimate interest.

Consider using a different analytics provider other than Google Analytics, but also take another look at your international transfers and kick off Data Transfer Impact Assessments for all Standard Contractual Clauses.

Recent DPC action

Facebook (Meta)

The DPC issued a draft decision on the investigation into Meta on Monday the 21st February, the full details of this are yet to come out at time of writing, however it is evident that the same stance taken y the French and Austrians on Google is taken here. Transfers to the US will likely be banned

Teaching Council

The teaching Council was issued with a €60,000 fine in relation to the mismanagement of a phishing breach. This phishing incident resulted in an auto-forward rule being set up on two staff email accounts, subsequently 323 emails were forwarded to an unknown third party. Compounding the issue is the fact that the IT team received a notification from Office 365 notifying them that an auto forward rule had been set up, however, the Council did not take appropriate action to investigate this resulting in the breach being ongoing for an extended period of time.

The DPC found deficiencies in the technical and organisational measures that were in place to investigate potential breaches.

Key Action: Review your breach identification and management procedures.

Limerick City and County Council

LCCC were fined €110,000 for violations in relation to the use of community CCTV with the core finding being that the Council did not have a lawful basis to process data on a wide number of CCTV cameras. Further to this it was found that:

- There was no data protection policy in place;
- Unauthorised access to the data was possible as there were no access logs
- Retention was not in place
- Subject access requests were not properly managed
- The DPO was not involved in a timely manner

Along with the fine the Council were ordered to stop processing the personal data until it had updated its data protection practices and brought the processing into line with requirements.

Key actions: We believe that if the DPO was consulted in a timely manner that these issues would not have arose, make sure to inform your DPO of new projects or initiatives before you start processing!

DPC annual report

On the 4th of February the DPC published its annual report for 2021 at a time when it is coming under intense fire for lack of enforcement. Some of the key figures from the report:

- Handled 39187 contacts
- 10888 queries and complaints received
- 10645 queries and complaints were concluded
- 6549 breaches (6274 concluded)
- 81 statutory enquiries including 30 cross boarder ones
- Unauthorised disclosure is still the biggest breach category with 4728
- Phishing and ransomware resulted in 138 breaches

Interesting to note is Helen Dixon's quoting of relevant legislation that is to be seen in combination with the GDPR in an attempt to give a more holistic view of data governance.

Right to access guidance document

The European Data Protection Board ("EDPB") recently released guidance for public consultation on the management of Data Subject Access Requests ("DSARs"), much of the guidance confirms what is already in practice in a lot of organisations. However, there are some good examples of specific situations. The key takeaways are:

- Ensure your staff can recognise a valid request and which process to follow if they receive one
- It is challenging to limit the scope of a request
- Make sure any restriction or exemption being applied is accompanied with clearly documented decision making
- Take care when verifying the ID of the data subject to not process additional data.
- If possible, use a portal or other such system to allow data subjects access to their data
- When balancing the right of access and adverse effects on third parties, make sure you examine all of the rights of those third parties, not just data protection ones.

Finally, it is important to make sure that you have an accurate and up to date Records of Processing Activities (“RoPA”) to allow you to identify all of the relevant personal data you process, also ensure that you have proper redaction processes in place.

Key action: Update policy and procedure as necessary, ensure RoPA is accurate and up to date.

Contacts

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

David O’Sullivan, Manager
T: +353 (01) 449 6444
DOSullivan@mazars.ie