CHALMIN DATA PRIVACY

Welcome to our February Newsletter 2020.

There were a large number of data breaches reported to the Irish DPC, so here is a reminder for you on how to deal with any incidents that might arise. *Sometimes a breach of personal data may occur, for example, because the personal data is accidentally disclosed to unauthorized persons or lost due to a fire or flood or by accident or stolen as result of a targeted attack or the theft of a computer device or mobile phone.*

*Report A*ll data protection incidents or suspected incidents immediately to your Designated Privacy Compliance Co-ordinator, don't forget each incident should be recorded even it isn't a reportable incident. Don't forget to ascertain if it is reportable. When the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons there may be no requirement to notify. There is a presumption to report to the DPC where a large volume of personal data is concerned or where there is a real risk of individuals suffering some harm. Cases must be considered on their own merits.

There are four main elements to any breach management plan:

- Containment and Recovery
- Risk Assessment
- Notification of Breach
- Evaluation and Response

The DPC's Annual Report

On 20 February, Ireland's data protection supervisory authority, the Data Protection Commission (DPC), published its Annual Report.

The Report reveals 2019 has been an exceptionally busy year for the DPC. It contains a number of interesting statistics, in particular:

- **Complaints:** 7,215 complaints received; 75% increase from 2018; 29% in "access rights" category; 5,496 complaints concluded, and 457 cross-border processing complaints received through the One-Stop Shop mechanism
- **Breaches:** 6,069 valid data breach notifications received; 71% increase from 2018 and 83% related to unauthorised disclosures
- **Inquiries:** 70 inquiries as of 31 December 2019; 21 cross-border inquiries, and 49 domestic inquiries
- **Direct marketing:** 165 new complaints investigated; 77 related to email marketing; 81 related to SMS marketing; seven related to telephone marketing, and prosecutions concluded against four entities
- **General consultation queries:** 1,420 queries received; 44% from the private/financial sector, and 33% from the public sector
- **Data Protection Officers:** 712 new Data Protection Officer notifications, bringing the total number to 1,596 at year end
- **Contacts:** 22,300 emails; 22,200 telephone call, and almost 4,000 items of post.
- **Staff:** increase from 110 at the end of 2018 to 140 at the end of 2019
- **Communications and guidance:** 33 guidance documents, 18 blogs, 8 podcasts, 20,000 social media followers
- **Binding Corporate Rules:** lead reviewer in 19 Binding Corporate Rules applications

There has been a significant increase in the number of complaints received. As in previous years, access request complaints were identified as the highest complaint-type received by the DPC between in 2019 - 2,064 complaints. A high proportion of these related to the failure of organisations to respond to an access request, or failure to release all the appropriate data on foot of an access request.

The DPC is the lead supervisory authority for a broad range of multinationals and the Report sets out that 457 cross-border complaints were transferred to the DPC by other data protection supervisory authorities in 2019.

Some of the trends and issues related to breaches identified in the Report include:

- Late notifications
- Difficulty in assessing risk ratings
- Failure to communicate the breach to individuals
- Repeat breach notifications
- Inadequate reporting

There has been an increase in the number of repeat breaches of a similar nature by a large number of companies, particularly in the financial sector, where the majority of breaches appear to be related to unauthorised disclosures

In 2019, the DPC examined the use of cookies and similar technologies on a selection of websites across a range of sectors, including media and publishing, the retail sector, restaurants and food ordering services, insurance, sport and leisure and the public sector. The Report states that the quality of information provided to users in relation to cookies varied widely and confirms that during 2020, the DPC will produce updated guidance on cookies and other technologies. The Report notes that the DPC will place a strong focus on compliance in this area.

The Report contains various case studies and details of litigation the DPC is involved in. The case studies cover matters including data subject rights data and data breaches.

Facebook Case in Germany, its new App and the action taken by the Irish DPC.

“By clicking Sign Up, you agree to our Terms and that you have read our Privacy Policy, including our Cookie Use" is wrong as confirmed by the Berlin Court of Appeal.

The Berlin Court of Appeal (Kammergericht) has rejected Facebook's appeal against the previous decision which prohibited them from using many misleading clauses for reasons of consumer and data protection.

Under Sec. 309 No. 12 lit. b of the German Civil Code, contractual provisions by which an entrepreneur modifies the burden of proof to the disadvantage of the consumer—in particular by asking the consumer to confirm certain facts—are invalid.

There was no effective consent ...

– to transfer personal data to the U.S.

– to promotional use of names and profile pictures.

– to any future data processing in any amended version of the Privacy Policy, not even for tacit use after 30 January 2015

https://www-bloomberg-com.cdn.ampproject.org/c/s/www.bloomberg.com/amp/news/articles/2020-02-13/facebook-fined-in-germany-for-violating-data-protection-rules **Facebook** has also postponed the launch of its new dating app after the Irish DPC s early morning visit to their Dublin Headquarters. We will have to watch this space.

Legal Basis for processing:

The "Guidance Note on the Legal Bases for Processing Personal Data" from the Data Protection Commission Ireland sheds light on the different legal bases available to controllers and processors under the GDPR, namely

- consent.

- contractual performance.

- legal obligation.

- vital interests.

- public interests.

- public tasks; and

- legitimate interests.

From experience, clients are often interested in the scope of the legitimate interests (LI) ground and the DPC reiterates that LIs can exist in the following areas:

(1) processing pursuant to relevant and appropriate relationship between the data subject and the controller (e.g. where the data subject is a client, asking if the data subject could 'reasonably expect' at the time and in that context that processing for that purpose may take place);

(2) processing for the purposes of preventing fraud.

(3) processing for direct marketing to existing clients.

(4) transmitting personal data within the corporate group for internal administrative purposes; and

(5) strictly necessary and proportionate processing to enable a network/information system resist actions that could compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal data.

Italian Fine

€27.8 million fine imposed by the Italian Data Protection Authority on a telecommunications company for alleged infringement of the GDPR. Following hundreds of complaints, they investigated and found the company had allegedly breached the GDPR. The heaviest breaches identified included:

Telemarketing without prior consent (or despite individuals' refusal)

lack of tech/org measures to ensure proper data breach management

lack of control on (and appropriate instructions for) processors

breach of accountability and privacy by design principles

Data retention in breach of storage limitation principle.

They determined the fine considering: the number of data subjects involved (thousands)

the duration of the infringement (more than a year)

the nature and gravity of the infringement (breach of fundamental GDPR's principles)

the intentional character of some infringements (breach of consent requirements)

the negligent character of some infringements (breach of accountability principle)

previous infringements for similar misconducts (promotional calls)

financial benefits gained from infringement (also potential). The fine is equal to 0,2% of the company's turnover.

Here below the decision (Italian version only).

Provvedimento del 15 gennaio 2020 [9256486]

Norwegian Fine

The Norwegian data protection authority has imposed a fine of €120,000 on the municipality of Oslo for the data processing in the Skolemelding app. It was used for communication between school employees, parents and pupils. The municipality did not implement appropriate technical and organisational measures to ensure a level of #security appropriate to the risks. The app contained well known vulnerabilities prior to its launch due to inadequate security testing, which made it possible for unauthorised persons to access and alter the personal data of more than 63,000 pupils.

The authority intended to impose a fine of €200,000, however since the municipality implemented measures to limit the dangers as soon as it was made aware of the security issues and showed willingness to fix them.

https://edpb.europa.eu/news/national-news/2020/norwegian-data-protection-authority-imposes-fine-municipality-oslo-education_en

WhatsApp

The key issue with WhatsApp is the fact it shares the telephone numbers of people in a group with each other and allows uploading of contacts from phones without a clear legal basis. Add to that the audit and control of group membership I have always said avoid and err on the side of caution.

https://www.rte.ie/sport/gaa/2020/0128/1111512-gaa-urges-clubs-to-avoid-whatsapp-due-to-gdpr-concerns/

Tracking and Cookies:

In the last few weeks, I saw a Company realise that when you respect the law (eg have tracking cookies disabled by default and proper consent) then google analytics is useless.

Using 3rd party cookies on your website. You need to ensure that any consent mechanism you put in place allows users to have control over all the cookies your website sets, not just your own.

For example, if you want to set third-party content such as tracking pixels and beacons from social networks, you need to ensure that users are given information about these and appropriate controls to signify whether or not they consent.

Ultimately, you are the one who determines what cookies are set on your website, and in particular the number and type of third-party cookies involved. One of the considerations before incorporating a third-party cookie should therefore be whether your consent mechanism allows the user to control whether the cookie is set or not.

As always read more at www.chalmindataprivacy.ie

Gail Chalmin

gail@chalmindataprivacy.ie