Observing 2021–22 data breach decisions of the Irish Data Protection Commission

Received: 19th October, 2022

Marie C. Daly
Special Counsel, Covington & Burling, Ireland

Marie Daly has a background as a litigator, employment and data protection lawyer and lobbyist. She latterly served as the general counsel of Ibec, the largest Irish lobby and business representative group, for over 16 years before joining Covington and Burling LLP. This included responsibility for ensuring competition compliance for 38 trade associations and the development of a data protection compliance regime in recent years. Marie has significant corporate governance experience in the private and public sector having also served as a long-standing board member of two Irish regulators. Marie was, until recently, a member of the Irish Company Law Review Group, appointed by the Minister of Business Enterprise and Innovation, and was deeply involved in the drafting of the comprehensive new Companies Act 2014.

Covington & Burling LLP, 13 Merrion Square, Dublin 2, Ireland
Tel: +353 1 9609409/+44 20 7067 2082; E-mail: mdaly@cov.com

Abstract The Irish Data Protection Commission (DPC) regulates many of the top global technology companies and as such its decisions have a significant impact on the companies and on the many users of their platforms. This article examines a number of recent data breach decisions of the DPC and finds them forensic, focused, reasoned and formulaic in approach. The decisions deal with key General Data Protection Regulation (GDPR) provisions, notably on requirements for data breach notification and communication with data subjects. In a change of strategy earlier this year, the DPC no longer offers guidance to controllers dealing with a breach, as was its previous practice. Decisions such as these are likely to help fill that vacuum.

KEYWORDS: data breach, breach notification, DPC, data subjects

INTRODUCTION

Data breaches — no-one wants them, except perhaps for the data protection authorities to whom they are reported. Despite a 2 per cent fall in the number of reported breaches in 2021, they are still a rich vein of investigative activity for the Irish Data Protection Commission (DPC).[1]

New DPC strategy

The level of engagement on individual breaches changed last January in a shift in strategy by the DPC. Instead of engaging with every notified data breach, as it had done, the authority will now engage on only selected breaches. In addition, it will no longer offer guidance to a data controller dealing with a breach and will now focus on enforcement cases instead.[2]

Clear and detailed decisions

Several decisions announced in late 2021 and early 2022 have given clear and detailed interpretation of the law and standards regulating breach identification and notification. These leaned on the 2018 European Data Protection Board (EDPB) Breach Notification Guidelines[3] and indicate

how the DPC, as a key European regulator, interprets data breach requirements.

As such, the decisions offer an opportunity to take stock of what is expected of an organisation navigating a data breach where the DPC is the relevant data protection authority.

BACKGROUND

Data breaches represent a significant work stream for the DPC with 6,549 valid notifications in 2021. Most of the 2021 breaches (71 per cent) related to unauthorised disclosures, 'mostly due to poor operational practices and human error, such as inserting the wrong document in an envelope addressed to an unrelated third party or sending email correspondence to multiple recipients using the "To" or "Cc" fields instead of the Bcc field'.[4]

It is not the breach itself that most occupies the DPC — most organisations will suffer one — but rather the way the breach is handled. The damage to data subjects, the integrity of the remedial work and the willingness to work with the regulator will each inform the reaction of the regulator.

However not all breaches require notification and not all of those that are notified require informing the data subject. These issues are of particular focus in the identified decisions.

The regulator — the DPC

The DPC is the Irish data protection authority.[5] It is currently a one member led commission — a situation that is due to change later this year with the recruitment of two additional commissioners.[6] The DPC has grown significantly in recent years given its role as lead supervisory authority under the General Data Protection Regulation (GDPR)[7] for several large technology companies including Meta, Microsoft, Google, Apple, Twitter and TikTok each of which have their European operations based in Ireland.[8]

The DPC deals with a significant number of breach notification cases. While a large chunk are domestic, it also has a number of ongoing complex cross border cases (Figure 1).[9]

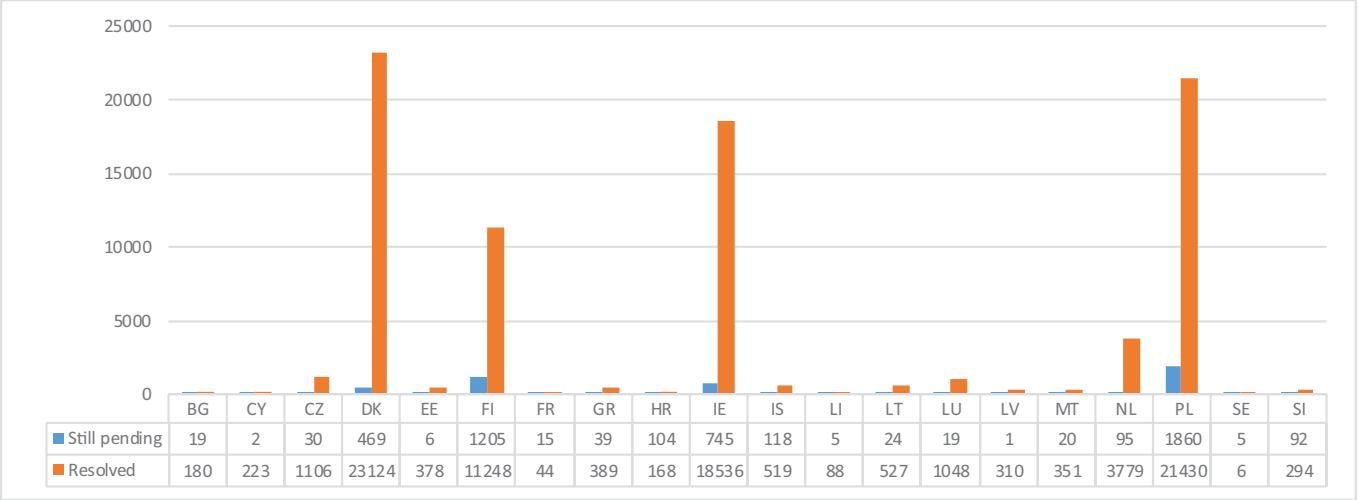
THE DPC BREACH DECISIONS

The first of the recent Irish decisions related to a large and well-resourced bank (DPC Case Reference: IN-19-9-5 In the matter of Bank of Ireland),[10] while a second (the oldest and dating to August 2021) related to a small charity dealing with domestic violence issues (DPC Case Reference: IN-20-7-1 In the matter of MOVE Ireland).[11] A third involved personal data loaded to a USB stick (DPC Case Reference: IN-20-4-8),[12] and the fourth raised interesting issues on the issue of identity theft (DPC Case Reference: IN-19-7-5 In the matter of Slane Credit Union Limited).[13] Both the third and fourth case were delivered within days of each other last January.

These four core decisions contain detailed and useful guidance on the type of assessments, controls and oversight expected of and appropriate to each organisation. Each case involved serious infringements and, while the fines (imposed in three of the cases) were very different, the rationale used to decide them follows the same path.

A number of previous decisions, in particular the Tusla cases from 2020 dealing with children's data protection, are also referred to. All reflect a formulaic and forensic fact-based approach.

A number of key issues, which can be broken down into the following four areas, were examined by the DPC in these four core cases:



	BG	CY	CZ	DK	EE	FI	FR	GR	HR	IE	IS	LI	LT	LU	LV	MT	NL	PL	SE	SI
Still pending	19	2	30	469	6	1205	15	39	104	745	118	5	24	19	1	20	95	1860	5	92
Resolved	180	223	1106	23124	378	11248	44	389	168	18536	519	88	527	1048	310	351	3779	21430	6	294

NL: These numbers cover the data breach notifications where the NL carried out, or intends to carry out an intervention following a data breach notification.

Figure 1: Status on 31st May, 2021 of the cases based on the data breach notifications

1. Was there a breach?
2. If so was it notifiable and should the data subjects be informed?
3. Was there an appropriate risk assessment in place?
4. Were the security measures in place appropriate to the risks.

IDENTIFYING A DATA BREACH

What is a personal data breach?

A personal data breach is defined under Article 4(12) as '"personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'.[14]

Loss of control

Typically, the breach involved a breach of security which resulted in loss or unauthorised disclosure of a person's data by the organisation in question. The DPC observes that it is a breach, even in the absence of an actual unauthorised disclosure to a third party, as it involves a loss of control over the personal data, as happened in the second case involving the loss of SD memory cards.

In that case, Men Overcoming Violence Ireland (MOVE), the DPC found, referring to the Ryneš judgment[15] involving security camera surveillance, that images and sounds of individuals participating in group therapy sessions and recorded on SD memory cards are personal data. USB devices can likewise contain personal data and, if lost, also provide the vehicle for a breach as occurred in the third case.

The DPC, in the first case, observes that a business credit card is unlikely to contain personal data, unless it is wrongly described and is actually a personal credit card, in which case it will contain personal data. So it's worthwhile to interrogate a description if there is any possibility of ambiguity.

Lost memory cards

In the MOVE case, participants in the group sessions, facilitated by a counselling service, discuss their domestic violence behaviour, attitudes and feelings towards others who may be named in the sessions. The loss of the memory cards recording these sessions concerned such sensitive personal data from 80 to 120 men over 18 recordings. The recordings were not encrypted until loaded onto the laptop. Camcorders were used to transfer the video sound and image onto each memory card which could be inserted into laptops thus forming part of a filing system. Although the ability to encrypt the SD cards, while recording on the camcorders, may not have been readily available on commercial cameras, the use of an unencrypted card was, the DPC found, inherently insecure.

The memory cards contained personal data, and the breach was notifiable as it involved a loss of control of the personal data by the data controller.

DISSECTING A BREACH

In the first case involving the Bank of Ireland, the DPC looked initially at what, under the GDPR, was a personal data breach,[16] noting that just because there was a breach does not mean that an infringement occurred.

Third party involvement?

For a personal data breach to occur, it is not necessary, the DPC opined, that a third party was involved. It can be the result of internal operations. The inability of a system, like the banks, to withstand harms to personal data contained in it, thus becomes part of determining whether a personal data breach has occurred.

Risk to data subject is key

The DPC warns against an overly technical approach to defining a personal data breach, stating that 'the focus of controllers should first and foremost be on the risk to data subjects arising from an event and whether notifying an incident would assist with the protection of data subjects' rights.'[17]

Categorising the breach

In defining a personal data breach, the DPC looked, in the bank breach investigation, at both the three categories of breach and three elements of a breach as guided under the 2018 EDPB Guidelines,[18] namely:

- a confidentiality breach,
- an integrity breach, and
- an availability breach.

Each had been committed by Bank of Ireland in the 22 breaches it notified to the DPC since late 2018.

- In the confidentiality breach, inaccurate personal data was uploaded by the bank.
- The same bank committed an integrity breach where it inaccurately altered customers' data. The majority of its breaches fell into this category.
- It committed an availability breach where it accidentally caused a temporary loss of the personal data.

The three elements of a breach were identified as being:

1. an incident, which can arise from internal processing and as such does not require third party involvement
2. the impact of that incident on personal data, and
3. that a network and information system was unable to withstand certain harms to personal data. This breach of security is distinct from the impact to the personal data itself.

In this case, inaccurate data was accidentally reported by the bank to a statutory Central Credit Register due to an

inadequacy in the bank's security measures. Most of the 22 bank breaches reported were found to be personal data breaches when looked at through the prism identified above.

Having a detailed description of the breach is a good early hurdle to jump. It also informs the next hurdles — whether the breach needs to be reported to the DPC and communicated to those affected by it.

NOTIFICATION

The GDPR breaks down dealing with a data breach into two distinct areas:

1. notification to the DPC,
2. communication with affected data subjects.

Within each of those lies a number of separate issues, each requiring careful assessment, including:

- what to notify and when to notify,
- whether data subjects should be communicated with and how to assess that.

It sounds straightforward but often it is not.

When to notify

A notifiable data breach is identified by Article 33(1) as follows:

> In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.[19]

The DPC approach is neatly summarised in its 2019 Annual Report:

> Under GDPR a controller is obliged to notify the DPC of any personal data breach that has occurred, unless they are able to demonstrate that the personal data breach is 'unlikely to result in a risk to the rights and freedoms of natural persons'. This means that the default position for controllers is that all data breaches should be notified to the DPC, except for those where the controller has assessed the breach as being unlikely to present any risk to individuals and the controller can show why they reached this conclusion.[20]

WITHOUT UNDUE DELAY

The requirement to notify a breach to the data protection authority is to do so without undue delay if there is a risk to those people who are affected by the breach. There is a 72-hour window of notification from when the data controller becomes aware of the breach and any delayed notification outside of that period requires explanation.

The requirement to communicate the fact of the breach to those affected is triggered where there is likely to be a high risk to them and they must be notified without undue delay.

Both of these, DPC notification and data subject communication issues and the assessment of their risk potential, played a large part in the DPC's investigation in the first case.

Time taken to notify

The issue of DPC notification divided into two — was the length of time taken to discover the breach reasonable and once aware of it did the bank notify within 72 hours?

Seventeen of the notified bank breaches had been notified outside of the 72-hour window. In a number of the breaches, the reporting was done within the 72-hour period, but the breach had remained

undetected for a considerable period of time before that. Even if the breach was reported within the 72-hour window, the inordinate delay previous to that in discovering the breach was an infringement of the obligation to notify the DPC without undue delay. Investigating personal data breaches was found not to be an adequate reason for failing to comply with the reporting obligations.

Also, a cursory description of the breach when notifying to the DPC is not good enough. It requires precision detail on the nature of the breach.[21]

INFORMING THE DATA SUBJECT

Compliance with Article 34, requiring the bank to tell the data subjects of the breach where likely to result in a high risk to their rights and freedoms, was also forensically examined by the DPC.

Level of risk

The level of risk can be gauged on the possible damage to data subjects. In finding against the bank on a data breach where the risk to the data subject did not materialise, the DPC noted that under the GDPR 'the test is not whether the personal data breach has caused damage to the data subject, but rather whether *"it is likely to result in a high risk to the rights and freedoms"* of the data subject.'[22]

The volume of lenders who could access the incorrectly disclosed credit history of customers was key given the real risk of customers being denied access to credit. This was shown in two cases where customers applied for credit to the Bank of Ireland only to have the inaccurate data actually included in their credit report. That, together with the volume of affected data subjects and the delay in notifying those customers, was a significant determinant of the level of risk in the DPC's analysis of whether each breach required communication with the affected customers.

Informing post rectification?

Waiting to remediate the breach did not justify a delay in informing affected customers, nor did waiting for a postal address for a data subject for whom there was an available phone number nor waiting until the number of affected data subjects could be established.

THE RISK ASSESSMENT

Assessing the risks of destruction, loss, alteration and unauthorised disclosure or access is obligatory under the GDPR in order to correctly identify the security measures appropriate to address those risks. It was an area of close scrutiny by the DPC in each of the decisions.

Posting a USB stick

In a third decision (DPC Case Reference: IN-20-4-8),[23] a USB stick, containing six employee investigation reports done by a consultant employee relations firm, was lost in the post. The unpadded envelope containing the USB stick should have been sent by registered post, but it was not, and it was neither encrypted nor password protected. It held personal data belonging to approximately 18 people.

The DPC looked at the risk assessment and at the adequacy of the measures taken to counter the risks identified. Much of the data — contained in the investigative reports in question — was sensitive, as well as there being a risk of the information being accessed by an unauthorised third party.

DIGITAL RIGHTS CASE GUIDES

The DPC drew on the 2014 CJEU case of Digital Rights Ireland *v* Minister for Communications, Marine and Natural Resources and others[24] for guidance on the factors to inform this assessment. The judgement struck down the Data Retention Directive for failing to ensure effective

protection of retained data against the risk of abuse and unlawful access in circumstances where it did not lay down specific rules in relation to

1. the vast quantity of data retained,
2. the sensitive nature of the data, and
3. the risk of unlawful access.

The DPC stated that these factors must also be considered in this case.

But not guided

It is not the only case where the DPC relied on the Digital Rights case to guide it. It did so also in each of the Tusla decisions[25] and each of the other cases considered in this article. While a useful yardstick, there is however no explicit mention of the case in the DPC data breach notification guidance issued in October 2019.[26]

There was no explanation given to the DPC about why the information on the USB stick had not been encrypted in advance of transferring it to the device. Also, there was a lack of explanation as to why Google Drive was not considered a safe way of transferring the data despite the data controller having it in place. These, together with the failure to use a padded envelope and registered post, led to a finding that the measures implemented were not appropriate to the risk.

RISK OF IDENTITY THEFT

Just two days after delivering its decision on the USB case, the DPC issued the fourth decision (DPC Case Reference: IN-19-7-5 In the matter of Slane Credit Union Limited).[27] In this case, the DPC took into account the risk of identity theft in assessing the likelihood of risk to data subjects in the processing of their data and assessing the appropriateness of the security measures implemented by the controller, a small local credit union.

Referring to a recent study commissioned by the European Commission,[28] the DPC quoted Ireland as one of the EU countries with the highest incidences of identity theft and fraud with 50 per cent of survey respondents in Ireland having stated they had been the victim of identity theft in the previous two years. This was shown to be second only to the UK (53 per cent). The DPC found that based on this analysis, the likelihood of unauthorised disclosure was high considering the lack of oversight in place in this case.

The incident, which was unannounced, occurred as a result of an update to a search engine optimisation tool installed on the credit union's website. The breach, which led to personal data being inadvertently publicised on the internet for about one week, did not disclose financial information or special categories of personal data and so was assessed by the DPC as of moderate risk. However, the big flaw was that no risk assessment of the risks was undertaken, which would have highlighted the vulnerability, and that the security measures in place, such as they were, were not regularly tested.

Unsurprisingly the DPC found against the credit union.

HOW GOOD WAS THE PROCESSOR ARRANGEMENT?

This case differed from the other three as it also enquired into the arrangement with the data processor.

Slane Credit Union believed that the use of outsource providers gave it a 'legislative safety net'. The DPC disagreed and looked instead at the due diligence carried out by the data controller on the data processor it engaged. The key question then was whether the processor had put sufficient guarantees in place to protect personal data. In the eyes of the DPC, it did not, given the lack of regard to the risks and the lack of active monitoring of website security or ongoing testing of new releases. The processor simply was not GDPR compliant.

But whose fault was that? It was mandatory under Article 28 that Slane Credit Union and the processor have an agreement which reflects GDPR requirements. The agreement they had predated the GDPR and had not been updated. The data controller, the credit union, was thus at fault for failing to ensure a compliant agreement.

HOW NOT TO DISPOSE OF OLD FILES: DUMPING OF SENSITIVE DATA IN PUBLIC RECYCLING CENTRE[29]

A student nurse on work placement disposed of an in-patient list, containing the personal data of 78 individuals, in a public recycling centre not far from the hospital. The list was discovered by a member of the public, who then notified the Health Service Executive (HSE).

The lack of hard-copy document security in seven other HSE data breaches notified by the HSE to the DPC also featured in this decision. In six of those, hard-copy documents containing personal health data were found outside of the hospital by members of the public or other hospital staff. Another involved hard-copy documents being mislaid during a departmental move to a new building.

The decision looked first at whether the hard-copy documents in question formed, or were intended to form, part of a filing system as required by the GDPR. The decision that they were in scope, states that

> any personal data processed by the HSE that are intended to form part of medical files fall within the scope of the GDPR, regardless of whether such personal data are actually stored in such files. This prevents controllers from attempting to circumvent the GDPR by processing personal data manually and/or outside of their usual filing systems.[30]

In this case, again there was no risk assessment done before the personal data breaches occurred. That was a mistake.

Looking at the likelihood and severity of the risk to the patients affected, the DPC concluded that there was a high risk of one of the 78 data subjects being identifiable given the numbers involved and the locality where found.

The DPC found that the organisational measures implemented by the HSE for staff training and awareness were not good enough. Online GDPR training, supplemented by broadcast emails and town hall style sessions, was provided. However, the amount and nature of this training was not appropriate to the HSE's high-risk processing. Furthermore, there was no evidence of measures to ensure completion of the online GDPR training.

Did COVID-19 play a part?

By late 2019 the COVID-19 emergency was dominating the health service and a majority of the national HSE workforce had not completed the training. It is not clear if this was put forward as a mitigating factor given the absence of any reference to the COVID-19 crisis in the decision.

The lack of:

- a standard operating procedure setting for secure shredding;
- a standard operating procedure for the secure creation, use and disposal of handover lists and in-patient lists;
- measures taken to ensure completion of staff data protection training and refreshers;
- a process for regularly testing, assessing and evaluating the effectiveness of its existing security measures;
- and measures for recording the location of, and accountability for, hardcopy documents containing personal data throughout future office moves

all indicated a failure of security for patient personal data. On that basis, the DPC found the HSE negligent and imposed a fine of €65,000.

PROPER DATA SECURITY

Under Article 32, a data controller is obliged to implement appropriate technical and organisational measures that reflect the risk to personal data in their care. The DPC's assessment, in the first case, was based on whether the bank had implemented measures appropriate to that risk. In deciding that, the DPC looked at how robust the banks procedures were when the breaches occurred.

It found that having robust validation measures in place would have helped the bank detect design failures in its systems to pre-empt data breaches. The inadequacy of its reporting flags and staff training and the lack of an error management system, quality assurance controls and oversight mechanisms were all failings that infringed.

The majority of the breaches had occurred before most of the training was delivered, which led to the finding that the bank did not have adequate training in place at the time of the breaches. Also, the training materials failed to emphasise the importance of communicating with affected data subjects where the breach was likely to carry a high risk to them.

All of these failings fed into a number of compliance orders against the bank and a significant administrative fine.

ENFORCEMENT ACTION

In each of the Bank of Ireland and MOVE decisions, the organisations argued that their reporting of the breaches should mitigate their liability, and, in both cases, the DPC rejected this.

The DPC wants compliance

The DPC has five regulatory goals, two of which are to regulate consistently and effectively and to bring clarity to stakeholders. Part of that is: 'Applying corrective powers proportionately — including fines, where appropriate — to produce changed behaviours and an improved culture of data protection compliance.'[31] Fines, while important, are just part of the regulatory toolkit. The aim is to achieve compliance in preference to imposing large fines.

In the absence then of specific EU guidance on the calculation of fines, the DPC was 'not bound to apply any particular methodology'.[32] That has recently changed, with the EDPB Guidelines on Administrative Fines,[33] and so future decisions will reflect this new guidance. However, while that aims to achieve a level of consistency of approach among Europe's data regulators, each regulator still retains autonomy in respect of their own national rules, and so some divergence will continue.

In the detailed 61-page Bank of Ireland decision, the DPC issued a reprimand with orders directing implementation of a number of compliance actions. It also imposed a series of administrative fines totalling €463,000. Noting again that it was (then) not bound to apply any particular methodology to calculate the fines, the DPC looked at the issues of effectiveness, proportionality and dissuasiveness as required by the GDPR.

Opaque fining

The DPC offers sparse detail on how it assessed each of its range of fines, instead referring to having considered the large number of data subjects affected and the inordinate delay in reporting the data breaches after the bank became subjectively aware of them. With regard to the failure to implement appropriate technical and organisational measures, the DPC regarded the lack of such measures as being negligent in character.

But, while undoubtedly the DPC analysed and considered each breach in great detail, how it actually arrived at each particular fine remains somewhat unclear. With only limited guidance from the EDPB

in 2017, it considered the requirements of the GDPR and set what it considered an objective and justifiable fine that meets the required criteria of effectiveness, proportionality and dissuasiveness.

Fines were also imposed in the second and fourth cases. None was applied in the USB stick decision, given the limited number of those impacted and the finding that the risk of the USB stick falling into the wrong hands was low to moderate. A reprimand was imposed instead.[34]

Decisive action in child cases: Children's data breaches[35]

Ireland's first GDPR fines were the result of these data breach inquiries initiated by the DPC. As might be expected, most of the inquiries looked at compliance with the GDPR principles of processing and with the 72-hour or without undue delay notification period requirement.

The third common thread revolved around the security of processing. But some of the more troubling breaches were in respect of children's data, in particular the sensitive data processed by the child welfare agency Tusla.

Tusla is the dedicated state agency providing family and child welfare services in Ireland. It received 60,000 child protection reports, 6,000 referrals and 8,000 school absence reports in 2019. It processes medical records, contact details, social work files and care plans as it deals with highly sensitive personal data of children and their families. Its data breaches were particularly concerning and the DPC took early and decisive action.

Tusla notified 71 data breaches in 2018 and then had another batch of 130 breaches in 2019. Most of it was down to human error. However, the processes and procedures in place to avoid and avert breaches simply weren't good enough and did not meet GDPR standards. It made front page headlines and caused much debate in Ireland. It was easy pickings for the DPC, and not surprisingly it gave the DPC its first and eagerly awaited GDPR fine. And then it delivered a second and a third fine.

What went wrong?

Employee error and sloppy processes were the main culprits. Just under a quarter of the breaches involved emailing the wrong recipient. Another quarter were postal address errors. The remainder included a repeated failure to redact correctly, sharing in error together with a small number of intentional disclosure breaches.

The lack of appropriate training was a root cause.

NEW EDPB FINES GUIDANCE

The EDPB had issued detailed guidance on how to set administrative fines.[36] Aiming for a consistent approach across all EU data protection authorities, it gives a framework for each authority to use in navigating what fine it should set when exercising that GDPR enforcement option.

Mathematical approach

While much of what is considered has already been considered by the DPC in the bank breach case, a more mathematical approach is adopted, which slots behaviour into ranges with matching financial ranges. The financial range is limited to 10 per cent for the lower and mid-levels of seriousness but increases substantially to a range of 80 per cent for breaches carrying a high level of seriousness. From there it refines further depending on the size of the offending organisation and whether there were aggravating measures (such as repeat offending or profiting from the breach) and mitigating circumstances involved. The bigger the organisation the higher the potential fine range. That linked with

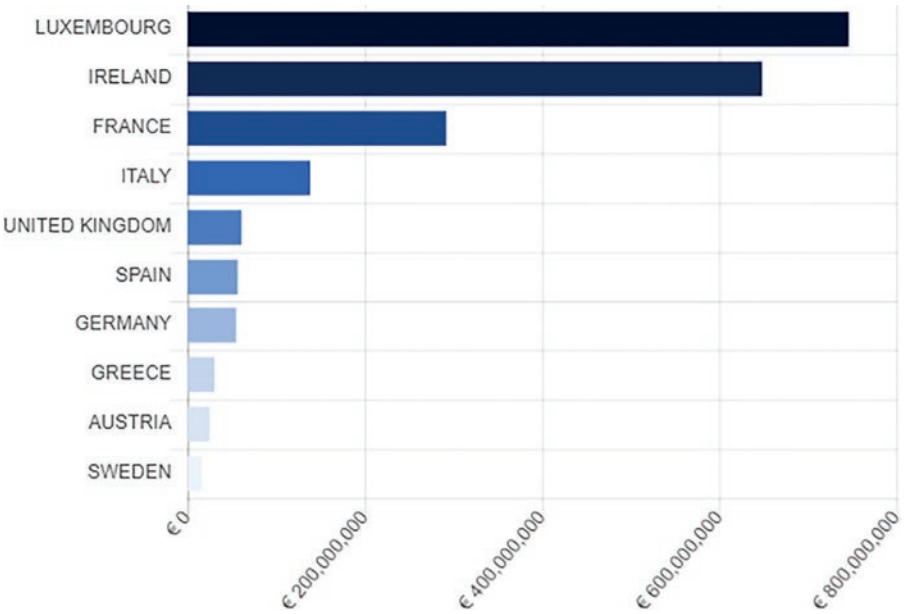


Figure 2: Statistics: Countries with highest fines (Top 10)[37]
The following statistics show how many fines and what sum of fines have been imposed per country to date (only top 10 countries).
Note: Only fines with valid information on the amount of the fine are taken into account.

the greater range when the breach is very serious suggests, on the face of it, greater encouragement of larger penalties for larger organisations.

While the CJEU has been asked to consider the issue of fines in a recent referral, the recent EDPB guidelines may well generate further referrals (Figure 2).

IN CONCLUSION

It is clear from these cases that the DPC is forensic in its approach to investigating data breaches. It leaves no stone unturned in dissecting the nature of the breach, what caused it, the risks it posed and the approach taken to limit the potential damage to data subjects. Lifting the veil on mistakes that led to the breach is important, and the decisions reviewed here illustrate the importance of early and earnest disclosure. Tardiness, at whatever stage of the breach, simply compounded the problem.

There are data protection officers and in-house counsel who will doubtless have been made aware of a data breach on a Friday evening of a bank holiday weekend by a colleague eager to escape the problem until the next working week. The obligations to notify and communicate will not wait for the weekend, and usually many hours of forensic and sometimes frenetic activity are required in order to properly inform those notifications — if they prove necessary. It is not a job for the faint-hearted.

The lessons to be learned from these detailed DPC data breach decisions may appear sensible, but they are often not easy to attain. They nevertheless show the benchmark for avoiding data breaches. This includes:

- having a clear and rehearsed internal procedure,
- knowing what the regulator requires and providing it. The DPC revised its data breach notification form in 2021 to make the notification process easier and clearer,

- checking descriptions are correct, which acts as an early filter, as does knowing what was lost and how it was lost. Correct and early identifications are important and will save time and effort in the long run,
- Co-operating with the DPC. The implementation of any subsequent DPC recommendations/requirements may be difficult, but it is necessary to contain further breaches.

References

1. Data Protection Commission (2021) 'Annual Report 2021', p. 49, available at https://www.dataprotection.ie/sites/default/files/uploads/2022-02/Data%20Protection%20Commision%20AR%202021%20English%20FINAL_0.pdf (accessed 16th August 2022).
2. Ibid., page 51.
3. European Data Protection Board (2022) 'Guidelines 9/2022 on Personal Data Breach Notification under GDPR', available at https://edpb.europa.eu/system/files/2022-10/edpb_guidelines_202209_personal_data_breach_notification_targetedupdate_en.pdf (accessed 16th August, 2022).
4. Data Protection Commission, ref 1 above, page 49.
5. Data Protection Commission, Homepage, available at https://www.dataprotection.ie/ (accessed 16th August, 2022).
6. Irish Government (2022) Press Release, 'Government Approves Expansion of the Data Protection Commission — The Department of Justice' available at https://www.gov.ie/en/press-release/0379c-government-approves-expansion-of-the-data-protection-commission/ (accessed 16th August, 2022).
7. European Parliament and Council Regulation (EU) No. 2016/679 of 27th April, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 56, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679 (accessed 16th August, 2022).
8. European Union, 'Commission Staff Working Document (2020)', para. 2.2, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020SC0115 (accessed 16th August, 2022).
9. European Data Protection Board (2021) 'Overview on Resources Made Available by Member States to the Data Protection Authorities and on Enforcement Actions by the Data Protection Authorities', p. 13, available at https://edpb.europa.eu/system/files/2021-08/edpb_report_2021_overviewsaressourcesandenforcement_v3_en_0.pdf (accessed 16th August, 2022).
10. Data Protection Commission, Decision: In the Matter of the General Data Protection Regulation and the Data Protection Act 2018: In the Matter of the Bank of Ireland, DPC Case Reference: IN-19-9-5, 14th March, 2022.
11. Data Protection Commission, Decision: In the Matter of the General Data Protection Regulation: In the Matter of MOVE Ireland, DPC Case Reference: IN-20-7-1, 20th August, 2021.
12. Data Protection Commission, Decision: In the Matter of the General Data Protection Regulation: In the Matter of [redacted], DPC Case Reference: IN-20-4-8, 24th January, 2022.
13. Data Protection Commission, Decision: In the Matter of the General Data Protection Regulation: In the Matter of Slane Credit Union Limited, DPC Case Reference: IN-19-7-5, 26th January, 2022.
14. European Parliament and Council, ref 7 above, p. 34.
15. Case C 212/13, František Ryneš v Úřad pro ochranu osobních údajů, available at https://curia.europa.eu/juris/document/document.jsf?text=&docid=160561&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1130797 (accessed 16th August, 2022).
16. European Parliament and Council, ref 7 above. Under Article 4(12) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
17. Data Protection Commission, ref 10 above, at 6.16.
18. European Data Protection Board, ref 2 above.
19. European Parliament and Council, ref 7 above, p. 52.
20. Data Protection Commission (2019) 'Annual Report 2019', p. 35, available at https://www.dataprotection.ie/sites/default/files/uploads/2020-04/DPC%20Annual%20Report%202019.pdf (accessed 16th August 2022).
21. European Data Protection Board, ref 2 above, Paragraph 52 states: 'Where precise information is not available (e.g., exact number of data subjects affected) this should not be a barrier to timely breach notification. The GDPR allows for approximations to be made in the number of individuals affected and the number of personal data records concerned. The focus should be directed towards addressing the adverse effects of the breach rather than providing precise figures.'

    Paragraph 56 states 'Depending on the nature of a breach, further investigation by the controller may be necessary to establish all of the relevant facts relating to the incident.'
22. European Parliament and Council, ref 7 above, emphasis added, para. 8.5.
23. Data Protection Commission, ref 12 above.
24. 1 Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the

Garda Síochána, Ireland, The Attorney General, intervener: Irish Human Rights Commission, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others, judgment of 8th April, 2014 (ECLI:EU:C:2014:238).
25. Data Protection Commission, Decision, 7th April, 2020: In the Decision of the Data Protection Commission under Section 111 of the Data Protection Act 2018 on foot of the Own-Volition Inquiry under Section 110 of the Data Protection Act, 2018 regarding Tusla Child and Family Agency Inquiry Reference: IN-19-10-1; Decision of the Data Protection Commission, 21st May, 2020, under Section 111 of the Data Protection Act 2018 on foot of the Own-Volition Inquiry under Section 110 of the Data Protection Act, 2018 regarding Tusla Child and Family Agency Inquiry Reference: IN-19-12-8; Decision of the Data Protection Commission, 2nd August, 2020, under Section 111 of the Data Protection Act 2018 on foot of the Own-Volition Inquiry under Section 110 of the Data Protection Act, 2018 regarding Tusla Child and Family Agency Inquiry Reference: IN-18-11-04.
26. Data Protection Commission (2019) 'A Practical Guide to Personal Data Breach Notifications under the GDPR', available at https://www.dataprotection.ie/en/dpc-guidance/breach-notification-practical-guide (accessed 16th August, 2022).
27. Data Protection Commission, ref 13 above.
28. European Commission (January 2020) 'Survey on "Scams and Fraud Experienced by Consumers" FACTSHEET', p. 13, available at https://ec.europa.eu/info/sites/default/files/factsheet_fraud_survey.final_.pdf (accessed 16th August, 2022).
29. Data Protection Commission, Decision: In the Matter of the General Data Protection Regulation: In the Matter of The Health Service Executive (HSE South), DPC Case Reference: IN-19-9-1, 18th August, 2020.
30. Ibid., and Data Protection Commission, ref 10 above, at 4.8.
31. Data Protection Commission (n.d.) 'Regulatory Strategy 2022–2027', available at https://www.dataprotection.ie/sites/default/files/uploads/2021-12/DPC_Regulatory%20Strategy_2022-2027.pdf (accessed 16th August, 2022).
32. Data Protection Commission, Decision, In the matter of the General Data Protection Regulation DPC Case Reference: IN-19-9-1 In the matter of The Health Service Executive (HSE South) Decision of the Data Protection Commission Paragraph 6.5.
33. European Data Protection Board (2022) 'Guidelines 04/2022 on the Calculation of Administrative Fines under the GDPR Version 1.0 Adopted on 12 May 2022', available at https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-042022-calculation-administrative_en (accessed 16 August 2022).
34. Data Protection Commission (2022) In the matter of the General Data Protection Regulation DPC Case Reference: IN-20-4-8, p.14 of the decision: 'I consider the personal data breach in this case caused a low to moderate risk of damage to data subjects. I consider that the risk of damage to the data subjects was low to moderate because if the unencrypted USB key were found by a member of the public and the data accessed, it is of very limited use. In light of the fact that a very limited number of data subjects could be impacted, and the relatively low risk of damage in the case, I do not consider it appropriate to impose an administrative fine.'
35. 1 Joined Cases C-293/12 and C-594/12, ref 24 above.
36. European Data Protection Board, ref 33 above.
37. Enforcement Tracker (n.d.) available at https://www.enforcementtracker.com/?insights (accessed 16th August, 2022).