MAZARS DATA PROTECTION NEWSLETTER

Issue 3

In this newsletter, we will provide guidance on:

- What the Data Protection Commission (DPC) may request following a breach notification
- What organisations should consider in the event of a 'no-deal' Brexit
- How organisations can further demonstrate GDPR accountability by completing a periodic GDPR Health Check covering security, data breach management and privacy by design and default

Additionally, we will discuss the trends in breach notifications and fines across Europe since May 25, 2019, as well as some of the recent data protection related developments and news in Ireland and further afield, including the DPC's public consultation on the processing of children's personal data, Google fine, Japan's adequacy decision and the second annual review of the EU-US Privacy Shield.

WHAT DOES THE DPC REQUEST FOLLOWING A BREACH NOTIFICATION?

Through our experience assisting clients with breach management, we have witnessed the DPC, in the event of a breach, requesting supporting documentation relating to our client's data protection framework, including:

- Data Breach Policy
- Incident Response Plan
- Incident Report
- Forensic investigations
- Information security/ technical controls

Many organisations have put in place a data breach policy, however, many may not have fully established or tested an incident response plan. Following a breach, it is critical that each team within an organisation know their roles and responsibilities in responding to a breach to minimise the potential impact of a breach. Organisations must ensure adequate teams and procedures are in place to deal with the variety of breaches which may impact an organisation (phishing; hacking; malware outbreaks; human error; etc).

We have outlined below what content may be included in an Incident Response Plan to assist organisations in responding to breaches in an efficient manner. It is worth noting that individuals/teams should be assigned to each task, and where possible, highlight the different approaches depending on the type of breach.

Incident Response Plan

Identification & initial assessment	Containment & recovery	Risk Assessment	Notification	Evacuation & response
STEP 1	**STEP 2**	**STEP 3**	**STEP 4**	**STEP 5**
Identify a breach Know who to contact Conduct Initial Assessment, including: • Cause • Extend of breach • The harm to affected data subjects • How to contain the breach	Dependent on type of breach. Establish: Who need to be made aware internally • Service providers to be notified • Steps to recover loses and limit damage • Should affected data subjects be notified immediately	Assess risks and consequences of the breach, including: • Risks for individuals • (severity and likelihood of consequences) • Risks for your organisation (operational, legal, financial, reputation) • Prepare Incident Report • Update Incident Log	Determine whether it is necessary to notify the breach (DPC, affected data subjects, media, legal, etc) Determine what to say and how to communicate it	Review to ensure that the steps taken during the incident were appropriate and to identify areas that may need to be improved

Additionally, we have seen the DPC use a breach investigation as an opportunity to enquire about an organisation's broader approach to data protection, including but not limited to:

- Third party data processors (may request a copy of any contracts in place between the two parties, or the record of processing activities for which the processor acts on behalf of the controller (GDPR - Article 30(2))
- Privacy by Design (software development standards; copies of relevant Data Protection Impact Assessments; etc.)
- General information security technical controls, e.g. use of two factor authentication
- Organisation structure and assessment if a DPO is required
- GDPR project plan and progress against the overall project

DPC ISSUES FURTHER GUIDANCE ON TRANSFERS OF PERSONAL DATA FROM IRELAND TO THE UK, INCLUDING NORTHERN IRELAND, IN THE EVENT OF A 'NO-DEAL' BREXIT

According to DPC guidance (December 2018), any Irish organisation that transfers personal data to the UK will require a transfer mechanism from 30 March 2019 to continue doing so lawfully in the event of a 'no deal' Brexit. Additionally, as the UK's data protection regime will not be recognised as "adequate", the most commonly used safeguard for transfers is standard or model contractual clauses (SCC) which have been approved by the EU Commission that implement contractual safeguards between the data exporter and importer.

The UK Government has transitionally deemed the EEA states as providing adequate levels of protection for personal data, thus allowing data to flow from the UK to any EEA country (and Gibraltar) in the event of a no-deal Brexit.

The DPC (February 2019) states that SSCs can be a stand-alone or a new contract between the Irish based controller and the UK based recipient, or, where the Irish based controller and UK based processor already have a contract in place between them, incorporate the SCCs into that existing contract provided that its terms do not affect the SCCs.

Moreover, the guidance provides a non-exhaustive list of examples of ways you might be transferring data to a UK based company, including:

- outsourcing your HR, IT or Payroll function to a UK based organisation
- using a UK based marketing company to send marketing communications
- occupational health provider based in the UK
- pension scheme based in the UK
- translation/transcribing services of a UK based company where you might be sending personal data of employees, customers or suppliers
- using a UK based company to analyse data on visitors to your website
- storing data in the UK on a server or in the cloud

Next steps to consider for organisations transferring data to the UK as being:

- Identify personal data being transferred to the UK
- Determine if transfers will need to continue beyond 30 March 2019
- If this is the case, then assess the various transfer mechanisms and decide which best suits the situation
- Engage with any third-party processors to ensure the required transfer mechanism is in place for 30 March 2019
- Check other contracts for any prohibitions on transfers of personal data outside the EEA and where necessary, amend them to ensure that this transfer may occur to the UK in a no deal scenario

Update privacy noticed to inform data subjects that transfers of their personal data to the UK post-Brexit will constitute transfers outside of the EEA.

GDPR HEALTH CHECKS

Under GDPR, organisations are legally required to implement appropriate technical and organisational measures for information security, data breach management and systems design, development and maintenance. As we approach the first anniversary of the General Data Protection Regulation (GDPR), organisations should consider validating and testing their GDPR related information technology practices.

Challenges

- Technical/legal obligations under Information Security, Data Breaches and Privacy by Design & Default are not fully understood nor fully implemented by organisations
- Organisations often fall short of meeting data protection and security requirements in incident management procedures and systems design, development and maintenance practices
- When using multiple third-party cloud service models, there may be a need for multiple breach response, recovery and investigation procedures, which must be integrated with its own data breach handling and reporting procedures
- Failure to embed privacy by design directly into information systems, processes and architectures at the beginning of the life of a system increases the likelihood of data breaches occurring in the future

What should you do?

Complete a periodic GDPR Health Check to demonstrate GDPR accountability, covering Information Security, Data Breach Management and Privacy by Design and Default:

Information Security

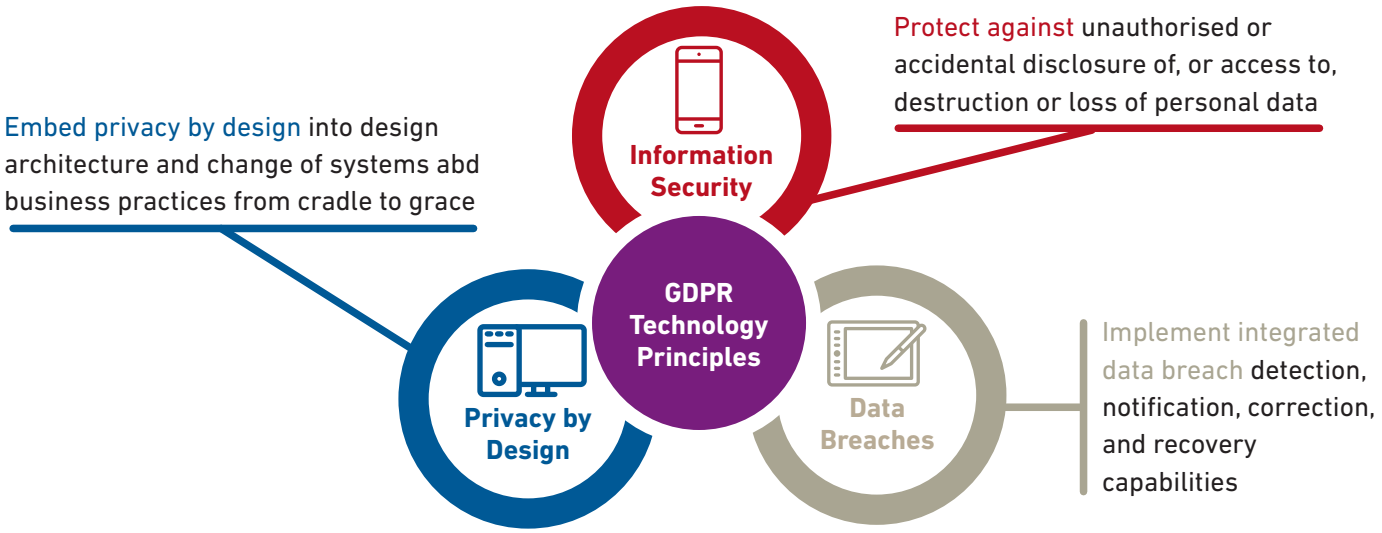
- Use ISO27002 to identify what type of controls are implemented to treat Information Security risks

Data Breach Management

- Review all data breach management procedures, including breach identification, breach response procedures, regular testing of incident response plan, third party assurance, etc.

Privacy by Design and Default

- Access how data protection is embedded into information systems, processes and architectures at the beginning of the life of a system,
- Gain assurance from third parties on privacy engineering practices when new processing or technologies are introduced or revised.
- Analyse misuse cases, data flows and data classification techniques to determine the threat level of potential system breaches.
- Discover exploitable flaws in a systems source code through code reviews and enforce secure coding standards



MAZARS

ONLY 91 REPORTED FINES FROM 59,430* DATA BREACH NOTIFICATIONS ACROSS EUROPE

According to a recent report by DLA Piper, there have been 59,430* data breach notifications between May 25, 2018, and January 28, 2019 (Data Protection Day) across Europe. However, the report highlights that only 91 reported fines have been imposed under the new GDPR regime.

The majority of fines have been relatively small, e.g., in Germany, a €20,000 fine was imposed on a company for failing to hash employee passwords, resulting in a data breach, while in Austria a €4,800 fine was issued for operating an unlawful CCTV system that was deemed excessive for its partial surveillance of a public sidewalk.

The following chart shows the top ten countries in terms of reported breaches, where Ireland ranks fourth highest:

Number of data breaches notified from 25 may 2018 - 28 january 2019 (top 10)

1	2	3	4	5	6	7	8	9	10
Netherlands	Germany	UK	Ireland	Denmark	Sweden	Finland	Poland	France	Norway
15,400	12,600	10,600	3,800	3,100	2,500	2,500	2,200	1,300	820

Per capita country ranking (number of data breaches per 100,000 people) (top 10)

1	2	3	4	5	6	7	8	9	10
Netherlands	Ireland	Denmark	Finland	Liechenstein	Finland	Slovenia	Sweden	Malta	UK
89.8	74.9	53.3	45.1	53.3	45.1	35.2	24.9	22.3	16.3

Results would suggest that Irish organisations may be over-reporting data breaches when compared to our European counterparts. This may be the result of Irish organisations wanting to manage their perceived risk without adequately assessing the potential risk to the affected data subjects or just a general misunderstanding as to what is 'unlikely to result in risk' to data subjects.

*The European Commission reported 41,502 data breach notifications for the same period. However, these were based only on the voluntary contributions of 21 (out of 28 EU Member States) data protection regulators. The DLA report covers 23 of the 28 EU member states, as well as Norway, Iceland and Liechtenstein.

MAZARS

PUBLIC CONSULTATION ON THE PROCESSING OF CHILDREN'S PERSONAL DATA AND THE RIGHTS OF CHILDREN AS DATA SUBJECTS UNDER THE GDPR

The DPC is running a public consultation on the processing of children's personal data and the rights of children as data subjects under the GDPR, which open to both adults and children.

The first stream of this consultation, which aims to collect the views of adult stakeholders, was launched on 19 December 2018 in the form of an online consultation document, with the closing date for this stream being 1 March 2019.

The second stream of the consultation, launched on international Data Protection Day (28 January 2019), aims to engage children and young people directly in the classroom. The DPC have invited all schools and Youthreach centres nationwide to participate in this consultation. This stream of the consultation is open until 5 April 2019.

Arising from this consultation, the DPC intends to produce a series of guidance materials about children and data protection.

For more information on the adult stream, please click HERE, while further information on the children-focused stream can be found HERE.

GOOGLE FINED €50 MILLION

France's Supervisory Authority (CNIL) has fined Google €50 million for failing to provide data subjects with transparent and understandable information on its data use. Additionally, the CNIL found that, even when user consent was collected, it did not meet the standards under GDPR that such consent be "specific" and "unambiguous". To date, this is the largest fine under GDPR.

EUROPEAN COMMISSION ADOPTS ADEQUACY DECISION ON JAPAN

On 23 January 2019, the European Commission adopted its adequacy decision on Japan, allowing personal data to flow freely between the two economies based on strong protection guarantees.

After two years, a first joint review will be carried out to assess the functioning of the framework. Subsequently, a review will take place at least every four years.

Japan is the first non-EU country to be granted adequacy since the GDPR came into effect.

EUROPEAN COMMISSION PUBLISHES THE SECOND ANNUAL REVIEW OF THE EU-US PRIVACY SHIELD

In December 2018, the European Commission published the second annual review of the EU-US Privacy Shield. The Report concluded that the Privacy Shield "continues to ensure an adequate level of protection" for personal data transferred from the EU to the US. However, the Commission identified several recommendations from the first annual review which still required implementation. In particular, the Commission requires the US administration to appoint of a permanent Ombudsperson to oversee complaints 28 February 2019, failing which the Commission will "consider taking appropriate measures."

If you are transferring/considering transferring data from your organisation to the US, inquire whether the US organisation are certified under the Privacy Shield.

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