MAPLES GROUP

UPDATE

Ireland Update: International Data Privacy Day 2022

The pace of General Data Protection Regulation ("GDPR") developments did not slow in 2021. Throughout the year, we saw significant changes to international data transfers, the Data Protection Commission ("DPC") imposing its largest fine to date, the fallout from the cyber-attack on the Health Service Executive ("HSE"), confirmation of the scope of the exceptions to the competence of the lead supervisory authority ("LSA") under the GDPR's 'one-stop-shop', as well as a host of new regulatory guidance from the DPC and European Data Protection Board ("EDPB").

International Data Transfers

Developments in relation to international data transfers continued a pace in 2021. Here are some of the highlights:

Regulatory Guidance and New Transfer SCCs

- The final version of the EDPB's *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data* provided useful guidance in June on how to comply with the requirements of Schrems II[1].

- Businesses started to incorporate the modernised transfer standard contractual clauses adopted by the European Commission in June ("New Transfer SCCs")[2] into their contracts ahead of the initial 27 September 2021 deadline[3].

- In November 2021, the EDPB opened a consultation on its *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR*[4]. These draft guidelines provide useful examples of what does amount to a transfer for the purposes of Chapter V of the GDPR. For example, there has to be a disclosure of personal data between two separate entities. Remote access of personal data by an employee of an EU employer from a third country will not be a transfer, as the employee is an integral part of its employer and not another controller.

Data Protection Authorities

Member State data protection authorities have been using their enforcement powers to ensure compliance with Schrems II.

- The Bavarian Data Protection Authority issued a notice to a data exporter in relation to its use of the US-based email marketing service, Mailchimp. In response to the notice, the exporter ceased use of Mailchimp as it had failed to carry out a data transfer impact assessment.

- The Portuguese Data Protection Authority ordered the National Institute for Statistics to

[1] https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en
[2] https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en
[3] https://maples.com/en/knowledge-centre/2021/6/international-data-transfers-new-transfer-sccs, https://maples.com/en/knowledge-centre/2021/9/in-the-spotlight-international-data-transfers-new-transfer-sccs
[4] https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-052021-interplay-between-application_en

suspend the sending of personal data from the census 2021 to its service provider in the US as its service provider was directly subject to the US surveillance legislation for the purposes of national security.

- The DPC's investigation into Facebook's data transfers to the US proceeded after the Irish High Court rejected Facebook's challenge to the legality of the DPC's decision to investigate Facebook's transfers to the US.

- The Austrian Data Protection Authority held that the use of Google Analytics by an Austrian website provider led to transfers of personal data to Google LLC in the U.S. in breach of Chapter V. of the GDPR.

GDPR Fines

2021 saw a significant increase in the level of GDPR fines with two record breaking fines:

- The Luxembourg data protection authority issued the largest GDPR fine to date when it fined Amazon €746 million.

- The DPC handed out the second largest GDPR fine to date when it imposed a €225 million fine to WhatsApp Ireland[5].

A number of GDPR fines have been reduced and / or overturned by national courts. It will be interesting to see if these large fines stand and the trend continues.

Cybersecurity

2021 started with the EDPB's publication of its guidelines on examples of personal data breaches[6]. The guidelines include practical case studies on ransomware attacks, data exfiltration and internal human risk. In May 2021, the HSE was rocked by a Conti ransomware attack. All HSE IT systems were switched off and the National Healthcare Network was disconnected from the internet in an attempt to contain and assess the impact of the cyber-attack. It was not until September 2021 that the IT systems were fully restored. The incident highlighted the importance of having robust cybersecurity measures for organisations of all sizes. The full independent post-incident review of the attack was published on 3 December 2021[7].

The 'One-Stop-Shop' System

On 15 June 2021, the Court of Justice of the European Union ("CJEU") released its judgement confirming the application of the GDPR 'one-stop-shop' mechanism. The Belgian Data Protection Authority took an action against Facebook. Facebook argued that the Belgian Data Protection Authority was precluded from investigating the alleged violations as the DPC is Facebook's LSA. The CJEU rejected Facebook's challenge. It confirmed that the competence of the LSA is the general rule but the GDPR does provide for exceptions to the general rule. These exceptions include where provisional measures are justified under the urgency procedure under Article 66 GDPR[8]. The CJEU did not elaborate on the criteria to assess urgency and did not explicitly endorse the Advocate General's view that a LSA's failure to act promptly may justify the adoption of interim urgent measures by other data protection authorities.

[5] https://maples.com/en/knowledge-centre/2021/9/data-protection-key-findings-from-the-edpbs-whatsapp-ireland-decision

[6] Guidelines 01/2021 on Examples regarding Personal Data Breach Notification | European Data Protection Board (europa.eu)

[7] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiTgYHtl8b1AhW-QEEAHYGxA90QFnoECAUQAQ&url=https%3A%2F%2Fwww.hse.ie%2Feng%2Fservices%2Fpublications%2Fconti-cyber-attack-on-the-hse-full-report.pdf&usg=AOvVaw3t2cZyX4L1j45ruz5UxHZM

[8] https://curia.europa.eu/juris/document/document.jsf;jsessionid=03EC2BE00883B72C312814868FFEAA5D?text=&docid=242821&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=16476654

Regulatory Guidance

Throughout 2021, a slew of new regulatory guidance was published by both the DPC and the EDPB. The DPC published seven new guidance notes, including the final version of its Children's 'Fundamentals'[9]. The Fundamentals introduce child-specific data protection interpretative principles and recommended measures.

Meanwhile, the EDPB produced 15 new sets of guidelines and recommendations. This included guidance on the concepts of controller and processor in the GDPR, which will likely form the basis for the assessment of compliance with Articles 26 and 28 GDPR going forward[10]. This guidance indicates that greater specificity as to how the parties will fulfil their particular obligations will now be required in data processing agreements going forward. This will represent a significant shift away from the common practice of many organisations to simply restate the content of Article 28 in their data processing agreements. A new set of Article 28 standard contractual clauses were introduced and it remains to be seen if they will be adopted on a wholescale basis.

What does 2022 have in store?

We expect to see the DPC more readily apply its corrective powers[11]. The DPC will also be reassessing how it prioritises its use of resources, and will prioritise allocating resources to cases that have higher systemic impact on large numbers of people. Guidance on how the DPC is likely to assess such systemic risk is expected in 2022.

More and more decisions on data transfers will come through national data protection authorities and we should see the DPC's decision on its investigation into Facebook's data transfers.

We expect to see the outcomes of the various challenges to the WhatsApp decision. In the meantime, organisations will need to factor in updates to their privacy notices to address the transparency requirements outlined in the WhatsApp decision.

A slew of new legislation is also on the agenda for 2022:

- On 20 January 2022, the European Parliament adopted draft text for the Digital Services Act ("DSA")[12] which, along with the Digital Markets Act[13], is set to face trilogue inter-institutional negotiations this year. Both will have a significant impact on the regulation of online service providers and big tech. The interaction between the approach of Ireland's Online Safety and Media Regulation Bill[14] and the DSA to the regulation of harmful content may present challenges for business designing processes catering for both.

- The proposed Data Governance Act[15] is expected to be adopted in 2022. It aims to increase the availability of public sector data and increase trust in data intermediation services.

- Negotiations on the new ePrivacy Regulation[16], originally published in early 2017, will continue throughout 2022, with the hope that it may finally enter into force

[9] https://www.dataprotection.ie/en/dpc-guidance/fundamentals-child-oriented-approach-data-processing
[10] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en
[11] https://www.dataprotection.ie/en/news-media/latest-news/dpc-publishes-regulatory-strategy-2022-2027
[12] https://www.europarl.europa.eu/news/en/press-room/20220114IPR21017/digital-services-act-regulating-platforms-for-a-safer-online-space-for-users
[13] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en
[14] https://www.gov.ie/en/publication/88404-publication-of-the-online-safety-and-media-regulation-bill/
[15] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767
[16] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010

by 2023. This will replace the previous ePrivacy Directive[17] and bring much-needed modernisation to the EU privacy framework and will include so-called 'over-the-top communication services', instant messaging services and web-based e-mail services in its scope, with the aim of ensuring a level playing field for companies.

- Trilogue inter-institutional negotiations for the Network and Information Security Directive ("NIS II")[18] are expected to commence in 2022. NIS II proposes to expand on the original NIS Directive[19] by effectively obliging more entities and sectors to take measures which will assist in increasing the level of cybersecurity in Europe in the longer term.

For further information, please reach out to your usual Maples Group contact or any of the persons listed below.

Dublin

Claire Morrissey
Head of Data, Commercial & Technology
+353 1 619 2113
claire.morrissey@maples.com

January 2022

[17] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058

[18] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A823%3AFIN

[19] https://eur-lex.europa.eu/eli/dir/2016/1148/oj