GDPR and Beyond:
Navigating Global Data Protection Regulations

Speaker - Duncan Gillespie

Date - 18th June 2024

Introducing your Speaker

Duncan Gillespie

Data Protection Partner

- Engineering Degree
- 10 years working in IT for Midland Bank/HSBC
- Qualified as a Solicitor in England and Wales 1998
- Hong Kong Overseas Lawyers Examination 2019
- Specialises in commercial law, with emphasis on competition, State aid/subsidy control, trade and data protection
- Partner in DLA Piper in the City for nearly 10 years
- Consultant with 360 for 7 years

Agenda

- A Look Back on Developments in 2023
- What's New in the Data Protection World in 2024?
- The Act that never was
- Artificial Intelligence and Data Protection
- Cybersecurity
- Enforcement and Breach Notification

Sign Up for Webinars On Demand to Watch

Developments in 2023

- NIS 2 Directive (Directive 2022/2555) enacted by EU on 16 January 2023, to be transposed by Member States by 17 October 2024
- EU Regulation on Digital Operational Resilience for the Banking Sector (**"DORA"**) entered force on 17 January 2023
- UK Government publishes White Paper on Regulation of Artificial Intelligence (**"AI"**)
- Meta fined €1.2 billion by Irish Data Protection Commission for transferring personal data to USA in reliance (solely) on the SCCs
- ICO and CMA issue joint position paper on Harmful Design in Digital Markets: "How Online Choice Architecture practices can undermine consumer choice and control over personal information"
- UK:US Data Bridge came into effect
- UK Data Protection and Digital Information Bill (No 2) receives first reading in House of Lords

Lets take a closer look

The NIS2 Directive

- Sets out measures that aim to achieve a high level of cybersecurity across the EU
- Requires EU Member States to adopt national cybersecurity strategies and set up “cybersecurity and computer security critical incident response teams” (“**CSIRTs**”)
- Specifies cybersecurity risk management measures and reporting obligations for entities defined as “*essential entities*” and “*important entities*”
  - trust service providers and top-level domain name registries and DNS service providers
  - operators of public electronic communication networks or providers of public electronic communication services
  - some public administration entities
  - operators of vital services
  - enterprises operating in the sectors defined in Annexes I and II to the Directive

The NIS2 Directive

Continued....

- Applies to entities providing essential or important services from a base within the EU but also, e.g. cloud computing services within the EU, regardless of domicile
- Non-EU based entities must have a representative in the EU
- Main obligations on essential and important entities are under Articles 20, 21 and 23
  - Article 20: appropriate cybersecurity risk management measures to be implemented and overseen by senior management
  - Article 21: appropriate and proportionate technical, operational and organizational measures to be taken to manage cybersecurity risk, based on an “all hazards” approach. Detailed requirements specified as to what this should cover
  - Article 23: essential and important entities must report significant cybersecurity incidents to CSIRT and/or competent authority (and users) within defined timescal
- Detailed implementation up to the Member States
- Provides for fines for non-compliance of up to 2% or global group turnover of €10 million, whichever is larger, for essential entities. Lower cap for important entities.

Data Transfer

- Under GDPR Article 44, personal data may not be transferred from the EEA to a third country unless:
  - that country has been found by the EU Commission to have an “adequate” system of data protection in place (NB the UK benefits from an EU Adequacy Decision and vice versa) [Article 45]; or
  - appropriate safeguards have been put in place [Article 46]; or
  - the transfer is made subject to binding corporate rules approved by the relevant supervisory authority [Article 47]
- Article 49 sets out various derogations from Article 44:
  - data subject has consented to the transfer, having been informed of the potential risks
  - transfer is necessary for the performance of a contract between the controller and the data subject or a contract between the controller and another person which is in the interests of the data subject
  - transfer is necessary for important reasons of public interest, the defence of legal claims or to protect the vital interests of the data subject or another person where the data subject is incapable of giving consent

Data Transfer

Continued....

See now EU:US Data Privacy Framework and the UK:US Data Bridge

- The "*appropriate safeguards*" typically used are:
  - under the GDPR, the transfer is made subject to the standard contractual clauses ("**SCCs**") adopted by the EU Commission in 2010 and updated in 2021; and
  - under the UK GDPR, either of the following is used: (i) the SCCs plus the "UK Addendum to the SCCs" drafted by the ICO; or (ii) the International Data Transfer Agreement ("**ITDA**") drafted by the ICO.
- The USA is not deemed an adequate country for the purposes of Article 45.
- The ECJ in the Schrems II judgment made it clear that the SCCs cannot necessarily be relied upon in isolation. Supplemental measures, such as a "*transfer risk assessment*" ("**TRA**") (or "*transfer impact assessment*" or "**TIA**" in UK parlance) need to be carried out and any additional safeguards identified implemented.
- In the Meta case, it had transferred huge amounts of personal data to the USA using only the SCCs and had not carried out a TRA. In addition, none of the Article 49 derogations was available so Meta had no legal basis for the transfers: fined €1.2 billion.

Harmful Design in Digital Markets

- The joint position paper issued by the CMA and the ICO identified a risk that certain "*Online Consumer Architecture*" ("**OCA**") features implemented by website operators could steer users into making decisions that do not reflect their privacy preferences
- Examples of such features include:
  - harmful nudges and sludge
  - confirmshaming
  - biased framing
  - bundled consent
  - default settings
- In November 2023, the ICO wrote to a number of leading website operators in the UK giving them 30 days to bring their sites into compliance with the UK GDPR or face enforcement action.

What's NEW for 2024

Some forthcoming attractions:

- EU's Artificial Intelligence Act expected to enter force over the next two years
- Commission to review GDPR in 2024 (not expected to result in significant changes)
- NIS 2 Directive to be transposed by the Member States and enter force by 17 October
- ICO to issue guidance on ITDA and UK Addendum to SCCs
- Continued EU and UK enforcement with regard to cookies, behavioral advertising and cybersecurity
- New data protection legislation to be adopted in various countries, including:
  - Canada
  - India
  - Various US states are considering legislation and a draft federal American Privacy Rights Act ("**APRA**") has been published by the Commerce Committees of the US Senate and House of Representatives

The Act That Never Was

- The UK Data Protection and Digital Information Bill nearly completed its Parliamentary journey but did not quite do so before the dissolution of Parliament

- The Bill was intended to relax certain of the GDPR requirements while maintaining the UK's adequacy status. Key reforms would have been:

  - the removal of the requirement for a Data Protection Officer ("**DPO**"). Instead, organisations would have had to have a "*Senior Responsible Individual*" ("**SRI**") who would be a member of senior management.
  - a change to the definition of "personal data" such that it covered only data that could allow the controller or processor and individuals likely to receive that data to identify the subject rather than considering anyone in the world
  - clarifying that "legitimate interests" can be used as a lawful basis for direct marketing
  - clarifying the regime applicable to automated decision making
  - restricting the obligation to have records of processing in place only to high-risk processing;

The Act That Never Was

Continued....

- potentially making international data transfers out of the UK easier by changing the requirement for an adequacy decision to an “approved transfer”, the new test being whether the standard of protection in the receiving jurisdiction is not materially lower than the UK regime
- widening the circumstances under which a controller can refuse to, or charge for a response to a Data Subject Access Request (i.e. if it is “vexatious or excessive” c/f “manifestly unfounded or excessive” under the GDPR)

Unlikely to be resurrected by a Labour Government?

360 LAWGROUP

Artificial Intelligence & Data Protection

- Although not mentioned specifically in the GDPR, it is clear that AI has the potential to raise significant data protection issues, including:
  - the vast amounts of data required to train systems potentially conflicts with the data minimisation principle
  - the volume of data collected and processed, and the potentially unexpected ways in which it may be processed, makes compliance with the lawfulness, fairness and transparency principle challenging
  - AI facilitates profiling and automated decision-making relating to individuals
- In view of these and other concerns, the European Parliament has adopted the EU Artificial Intelligence Act, which will enter into force over the next two years.
- Key features of the AI Act include:
  - AI systems which meet the definition of “unacceptable risk” AI systems (such as social scoring systems or manipulative AI) will be prohibited.

Artificial Intelligence & Data Protection

Continued....

- AI systems defined as “high risk” AI systems will be regulated (such regulation takes up most of the text of Act)
- systems described as “*limited risk*” will be subject to light touch regulation
- “minimal risk” AI systems will be unregulated

Obligations for high risk AI systems:

- establish a risk management system throughout system’s lifecycle
- conduct data governance, ensuring that training, validation and testing datasets are relevant, sufficiently representative and, to the best extent possible, free of errors and complete according to the intended purpose
- draw up technical documentation to demonstrate compliance and provide authorities with the information to assess that compliance
- design the system for record-keeping to enable it to automatically record events relevant for identifying national level risks and substantial modifications throughout the system’s lifecycle

Artificial Intelligence & Data Protection

Continued....

- provide instructions for use to downstream deployers to enable the latter's compliance
- design their system to allow deployers to implement human oversight

AI systems used in certain specified applications will have to be registered in an EU database:

- management and operation of critical infrastructure
- education and vocational training
- employment, worker management and access to self-employment
- access to and enjoyment of essential private services and public services and benefits
- law enforcement
- migration, asylum and border control management
- assistance in legal interpretation and application of the law

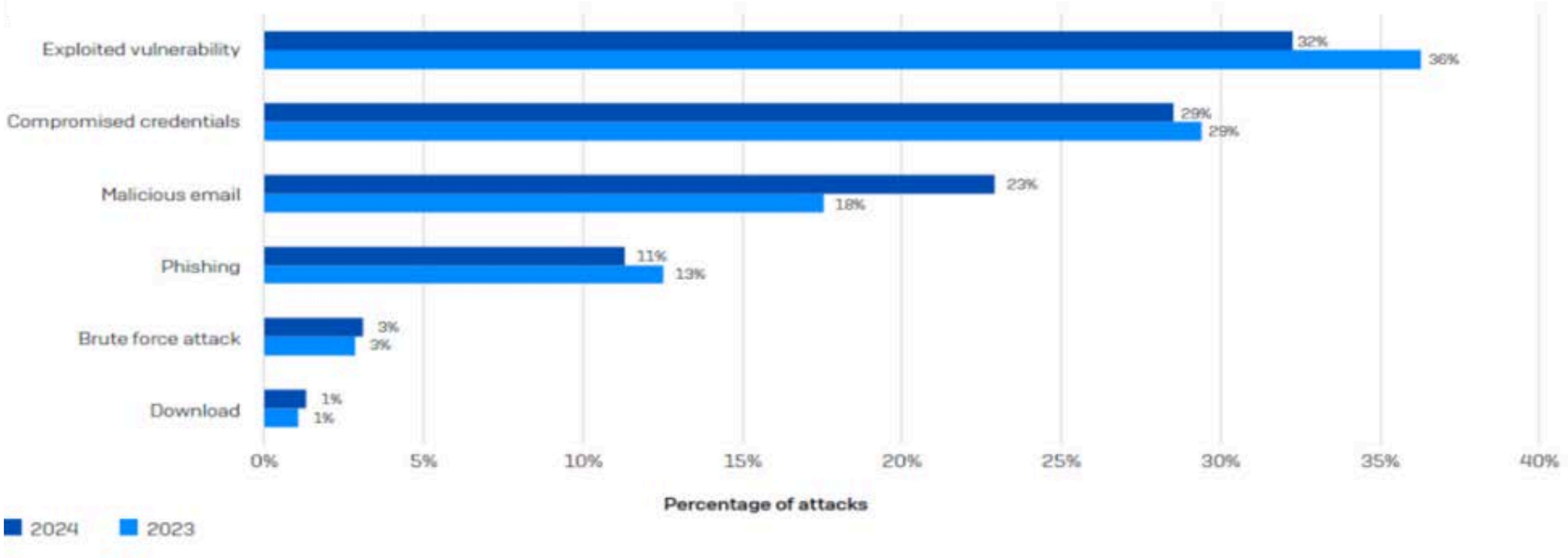
Artificial Intelligence & Data Protection

Continued....

- Generative AI, like ChatGPT, will not be classified as high-risk, but will have to comply with transparency requirements and EU copyright law:
  - disclosing that the content was generated by AI
  - designing the model to prevent it from generating illegal content
  - publishing summaries of copyrighted data used for training

Cybersecurity

- A survey carried out by Sophos “The State of Ransomware 2024” identified the following as the root causes of ransomeware attacks



Enforcement & Breach Notification

- Article 33 of the GDPR states that:
  1. 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 (emphasis added)
  2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach."
- No need to notify if breach unlikely to risk the rights and freedoms of data subjects
- Article 32(3) specifies the details to be provided (which can be provided in stages if necessary)

Enforcement & Breach Notification

Continued....

- Article 33 of the GDPR states that:

  1. 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 (emphasis added)
  2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach."

- NB. The phrase "*becoming aware of [the breach]*" does not mean that "*Nelsonian Blindness*" is condoned – controllers and processors should have systems in place so that they become aware of breaches

Enforcement & Breach Notification

Continued....

- For example, it is common to see data processors trying to negotiate DPAs such that they have 2 or 3 days to investigate a suspected breach before notifying the controller – controllers should resist this.

- ICO has prepared a data breach notification self-assessment tool and online self breach notification form.

Enforcement & Breach Notification

Continued....

Article 34 of the GDPR provides that:

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.
2. The communication shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in Article 33(3).
3. Communication to the data subject is not required if:
   - (i) the data was encrypted or otherwise made unintelligible to non-authorised users; or
   - (ii) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise; or
   - (iii) it would involve disproportionate effort – in which case there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner

Enforcement & Breach Notification

Continued....

- So, the bar for notifying data subject (likely to result in a high risk to rights and freedoms) is much higher than that for a notification to the supervisory authority (cannot say that there is unlikely to be a risk to rights and freedoms).
- NB supervisory authority may order a notification to data subjects to be made if it has not been
- Fines of up to 2% of global group turnover or €10 million (whichever is higher) for breach of Articles 33 / 34

Copyright Statement

No part of this publication may be reproduced, stored in or introduced into a retrieval system or transmitted in any form or by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior written permission of a director of 360 Law Group.