Matheson

Data Protection, Privacy and Cyber Security Bulletin

Latest Insights and Best Practice

Edition 2 | January 2022

Home

New EDPB Guidance on Data Breaches

Remote Working: Risks and Challenges to Businesses

EEA Fines and Penalties Overview

Cybersecurity and the Metaverse

Combatting Cyber Threats with AI

Cyber Security Tips Videos

Key Contacts

Introduction

Welcome to Edition 2 of Matheson's Data Protection, Privacy and Cyber Security Bulletin.

Cyber perils outrank Covid-19 and broken supply chains as the top global business risk, according to Allianz's Risk Barometer 2022[1].

Our highly experienced team of data protection, technology and litigation lawyers are available to support your business to prepare, react and recover from a cyber attack.

In this edition, our expert team considers significant developments including:

- Recently approved European Data Protection Board guidance on data breaches
- New Irish data breach reporting forms
- Cyber security issues that arise in the context of remote working
- An overview of key security themes in fines and penalties from across the EEA in Q3 and Q4 2021
- Emerging technologies - Artificial Intelligence and the Metaverse

For further information on any of the topics we discuss in this bulletin, please get in contact any member of our Team

[1] Allianz Risk Barometer, published January 2022: www.allianz.com/en/press/news/studies/220118_Allianz-Risk-Barometer-2022.html

Home

New EDPB Guidance on Data Breaches

Remote Working: Risks and Challenges to Businesses

EEA Fines and Penalties Overview

Cybersecurity and the Metaverse

Combatting Cyber Threats with AI

Cyber Security Tips Videos

Key Contacts

New EDPB Guidance on Data Breach Examples

On 14 December 2021, the European Data Protection Board ("EDPB") published examples of data breaches, based on typical scenarios handled by Supervisory Authorities ("SA").

The purpose of the new guidelines is to "shed light on whether or not to notify the breach to the SA and communicate it to the data subjects affected."

Prevention – The Best Defence

Best outcomes arise in cases where "privacy by design" measures are baked in to data protection and security compliance cultures.

Where a controller can demonstrate that accountability and security measures are structured, consistent, tested and reassessed to fit new processing operations, it is more likely to have a routine data breach experience.

Some key examples →

Home

New EDPB Guidance on Data Breaches

Remote Working: Risks and Challenges to Businesses

EEA Fines and Penalties Overview

Cybersecurity and the Metaverse

Combatting Cyber Threats with AI

Cyber Security Tips Videos

Key Contacts

New EDPB Guidance on Data Breach Examples

Some Key Ransomware Examples From The New Guidelines

Example 1

- Type of personal data security breach: availability breach
- **Separate back up in place** that mitigated the effect of the availability breach within hours of the controller becoming aware of the breach resulting in minimum effect on data subjects
- Employees **trained on security awareness**
- Data encrypted at rest and security confirms with state of the art – **no data exfiltration**

Document Internally?	**YES**
Notification to SA?	**NO**
Notify Data Subjects?	**NO**

Example 2

- Type of personal data security breach: availability breach – the amount of time that data is unavailable contributes to the risk assessment regarding notification to the data subject
- Electronic back up did not exist but a hard copy did – cited as a potential reason to report to the SA given the high risk to the data subject
- **No special categories of data were compromised**, the **quantity of data compromised was low and the number of affected data subjects is low**

Document Internally?	**YES**
Notification to SA?	**YES**
Notify Data Subjects?	**NO**

Example 3

- Type of personal data security breach: confidentiality and availability
- **Back up existed but was compromised** in cyber attack
- **High volume of sensitive personal data including credit card data compromised** – possibility that the attackers modified or copied data
- **Breach presents a high risk to data subjects** due to both material (financial loss) and non-material damage (identity theft/ fraud as identity cards were affected)

Document Internally?	**YES**
Notification to SA?	**YES**
Notify Data Subjects?	**YES**

New EDPB Guidance on Data Breach Examples

EDPB Guidance - Key Takeaways

All data breach scenarios must be documented in line with Article 33 (5), GDPR.

Notification to Supervisory Authorities is required unless there is *unlikely to be a risk* to the rights and freedoms of data subjects.

Notification to data subjects arises where there is *likely to be a high risk* to the rights and freedoms of data subjects.

Key Proofs

Fit for purpose security and accountability mitigation measures.

Data security breaches do not always attract formal enforcement notices, fines or penalties.

Key Takeaways

- Take care to implement compliance recommendations provided by an SA
- Failure to implement will likely result in less sympathy from the SA in the event of future breaches

Case Study

September 2021: Dutch SA fined the Danish Cancer Society €107,000 for failing to implement recommendations provided in an earlier interaction with its office.

FURTHER READING AND RESOURCES

Matheson Insight: GDPR and Data Subject Reporting Obligations - Why, When and How?

EDPB: Examples Regarding Personal Data Breach Notification, December 2021

Article 29 Data Protection Working Party: Guidance on Personal Data Breach Notification, February 2018

Data Protection Commission: Data Breach Notification Practical Guidance

Home

New EDPB Guidance on Data Breaches

Remote Working: Risks and Challenges to Businesses

EEA Fines and Penalties Overview

Cybersecurity and the Metaverse

Combatting Cyber Threats with AI

Cyber Security Tips Videos

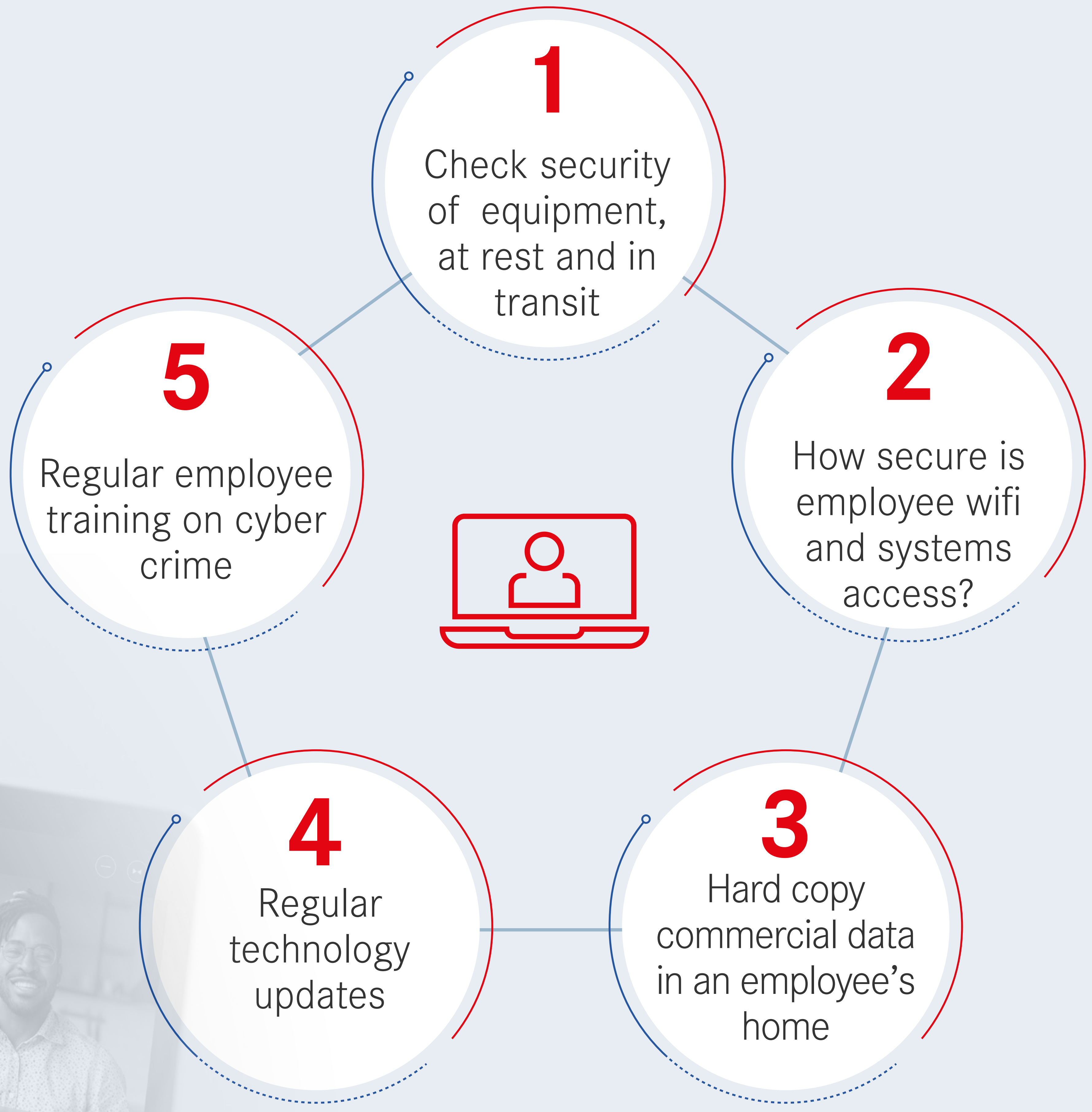
Key Contacts

Remote Working: The Risks and Challenges to Business

Against a backdrop of the relaxation of Covid-19 restrictions and a proposed statutory right to work from home in certain circumstances, it is widely accepted that hybrid working is part of a new norm in Ireland and beyond.

In this context, we consider the data protection issues that arise when working from home. The Data Protection Commission ("**DPC**") has helpfully identified some of the key security and practical data protection considerations for remote working.

Read full article →



1 Check security of equipment, at rest and in transit

2 How secure is employee wifi and systems access?

3 Hard copy commercial data in an employee's home

4 Regular technology updates

5 Regular employee training on cyber crime

FURTHER READING AND RESOURCES

Matheson Insight: : Remote working and the Risks and Challenges to Business, January 2021

Data Protection Commission: Protecting Personal Data When Working Remotely, March 2020

Home

New EDPB Guidance on Data Breaches

Remote Working: Risks and Challenges to Businesses

EEA Fines and Penalties Overview

Cybersecurity and the Metaverse

Combatting Cyber Threats with AI

Cyber Security Tips Videos

Key Contacts

Overview of Fines and Penalties from across the EEA: Q3 and Q4 2021

Country	Date of Fine	Amount	Controller	GDPR Provision Breached	Further Information
Netherlands	21 December, 2021	€400,000	Transavia Airlines	A 32	**Cyber attack, Security**: hackers gained access to personal data of 25 million passengers. The DPA found that Transavia failed to apply security measures to ensure a level of security appropriate to the risk to data subjects, resulting in the fine and recommendations for reform.
Lithuania	29 November, 2021	€110,000	UAB Prime Leasing	A 32 (1)(b)(d)	**Cyber attack, Security**: Personal data of over 100,000 CityBee users was published online, that originated from an unsecured backup copy of a database. The company was found to have failed to implement technical and organisational measures to ensure a level of security appropriate to the risk to data subjects. The database had been stored unencrypted and personal codes were stored unprotected and passwords were not sufficiently encrypted.
Norway	18 October, 2021	€412,000	Ostre Toten municipality	A 5 (1)(f), A 32	**Cyber attack, Security**: In January 2021, the municipality's data was encrypted and backups deleted. Stolen data, including sensitive personal data, was published online. An investigation revealed fundamental deficiencies in the municipality's security and internal controls.

Home

New EDPB Guidance on Data Breaches

Remote Working: Risks and Challenges to Businesses

EEA Fines and Penalties Overview

Cybersecurity and the Metaverse

Combatting Cyber Threats with AI

Cyber Security Tips Videos

Key Contacts

Overview of Fines and Penalties from across the EEA: Q3 and Q4 2021

Country	Date of Fine	Amount	Controller	GDPR Provision Breached	Further Information
🇮🇪 Ireland	2 September, 2021	€225,000,000	WhatsApp Ireland Ltd	A 5(1)(a), A 12, A 13, A 14	**Transparency**: Fine is subject to appeal: The DPC criticised WhatsApp's sharing of personal data between group entities without users and non users express consent. The fine is composed as follows: EUR 90,000,000 for the violation of A5 (1) (a) GDPR; EUR 30,000,000 for the violation of A12 GDPR; EUR 30,000,000 for the violation of A13 GDPR; and EUR 75,000,000 for the violation of A14 GDPR.
🇪🇸 Spain	30 November, 2021	€20,000	Daviser Servicios, S	A 5(1)(c)	**Transparency**: The company was found to have processed biometric data (fingerprints) of employees for secure access to certain rooms, when less intrusive means (such as key cards) could have been used to protect the privacy of the data subjects.

Home

New EDPB Guidance on Data Breaches

Remote Working: Risks and Challenges to Businesses

EEA Fines and Penalties Overview

Cybersecurity and the Metaverse

Combatting Cyber Threats with AI

Cyber Security Tips Videos

Key Contacts

Overview of Fines and Penalties from across the EEA: Q3 and Q4 2021

Country	Date of Fine	Amount	Controller	GDPR Provision Breached	Further Information
United Kingdom	25 November, 2021	€585,000	Government Cabinet Office	A 5(1), A 32	**Security and Transparency**: Following an error in the set up of a new IT system, the Cabinet Office published a file on their website containing the names and uncensored addresses of 1000 high profile individuals who had received New Years honours. The ICO found that the Cabinet Office failed to implement appropriate technical and organisational measures to ensure a level of protection appropriate with the risk to data subjects.
France	4 November, 2021	€400,000	Régie autonome des transports parisiens (RATP)	A 5(1)(c), A 32	**Security and Transparency**: RATP were found to have used unnecessary data for evaluating employee performance and promotions. In addition, data was retained for longer than it was required to do so. In addition, the CNIL found that RATP did not adequately differentiate between staff data access levels, allowing more staff than necessary to access certain data.

Emerging Technologies

Cybersecurity and the Metaverse

What is the Metaverse?

The term “Metaverse” has rocketed from obscurity to the top of our newsfeeds in recent months. Up until now, the concept has only been found in the R&D departments of Big Tech companies. Rapidly, the majority of these companies are launching products to the market.

At its simplest, the Metaverse represents the next iteration of the internet – a 3-dimensional version of the internet which fully immerses the user, rather than simply looking in from the outside. This will lead to an ever increasing blurring of the lines between the virtual and physical world.

What Will it Mean in Reality?

- A new way of training or storytelling, using shared gaming platforms
- Advances in virtual / augmented / extended reality experiences
- Enabling growth of the digital or virtual economy, non-fungible tokens and cryptocurrencies
- A new space in which to more freely allow for user-generated content

The Legal Challenge →

Home

New EDPB Guidance on Data Breaches

Remote Working: Risks and Challenges to Businesses

EEA Fines and Penalties Overview

Cybersecurity and the Metaverse

Combatting Cyber Threats with AI

Cyber Security Tips Videos

Key Contacts

Emerging Technologies

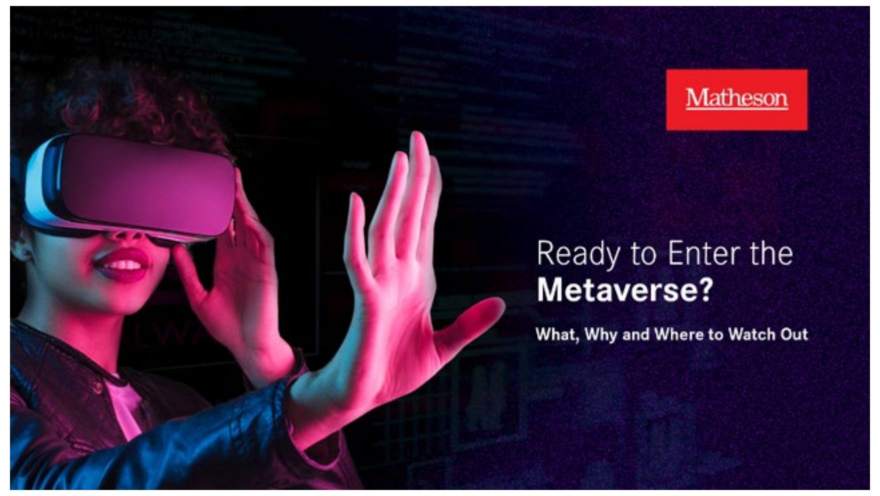
Cybersecurity and the Metaverse

As the Metaverse expands its offerings as a marketplace for both commerce and personal data, more and more consumers will shift their digital lives from the current computer and mobile internet model to the Metaverse.

As with any current underlying legacy system, this increase in traffic raises the risk and attractiveness for a potential cyber attack. For example, research into a number of popular VR platforms previously found that there was little in the way of protection at the time for VR being hosted on a compromised computer. Hackers faced little in the way of encrypted software and were able to interfere with a platforms proprietary content to alter a user's VR experience to their own ends.

Elements such as integrated contactless payment systems, the increased prevalence and storage of biometric data and massive amounts of cross-platform data transfers will all increase the risk profile for consumers and businesses in the Metaverse. Enhanced, and perhaps yet uninvented, security frameworks will be required to protect against malware attacks, fraud and data breaches.

Simultaneously, new and updated legislation will be required to address the enhanced security risks presented by the Metaverse. While business players wait for this they may want to follow a predicative rather than reactive approach to regulation.



FURTHER READING AND RESOURCES

Are You Ready to Enter the Metaverse?

Matheson's recent Bulletin outlines the potential benefits, opportunities and risks associated with this emerging technology.

Home

New EDPB Guidance on Data Breaches

Remote Working: Risks and Challenges to Businesses

EEA Fines and Penalties Overview

Cybersecurity and the Metaverse

Combatting Cyber Threats with AI

Cyber Security Tips Videos

Key Contacts

Emerging Technologies

Combatting Cyber Threats with Artificial Intelligence (“AI”)

Cyber threats have been trending to increased ransomware attacks, commodity malware and heightened Dark Web enablement.

With the acceleration to cloud, companies are taking advantage of cybersecurity tools and emerging technologies in an effort to meet the threat of fast-evolving cyber attacks.

AI and machine learning are a way to keep ahead of criminals, automate threat detection, and respond more effectively than before. At the same time, more sophisticated, centralised security operations centres are being set up to detect and eliminate vulnerabilities.

In April 2021, the European Union published its Proposal for a Regulation on Artificial Intelligence (the “AI Regulation”).

At this early stage in the legislative process, these are the key takeaways:

- The first legislation of its kind that aims to provide a regulatory AI framework
- Some AI systems will be banned completely (“unacceptable risk”) – such as those causing, or likely to cause, physical or psychological harm
- A risk-based approach to regulation is likely to apply, with systems deemed “high-risk” expected to comply with extensive obligations, with “limited risk” and “minimal risk” systems expected to require less
- The regulation will have an extra-territorial effect; impacting companies outside the EU that provide services into the EU
- In line with penalties available under the General Data Protection Regulation (“**GDPR**”), the AI Regulation allows for the imposition of fines, up to €30 million or up to 6% of annual global turnover, whichever is the higher

The Pros & Cons →

Home

New EDPB Guidance on Data Breaches

Remote Working: Risks and Challenges to Businesses

EEA Fines and Penalties Overview

Cybersecurity and the Metaverse

Combatting Cyber Threats with AI

Cyber Security Tips Videos

Key Contacts

Emerging Technologies

Combatting Cyber Threats with Artificial Intelligence ("AI")

"software that is developed with one or more of the techniques and approaches. . . and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with."

European Union Definition of an AI System

As expected, the debate around this legislation has already started. We will hear more on this around the world before it becomes law, currently expected in 2023.

Potential Benefits

This regulation may become the global standard, in the same way GDPR has become.

It may also make AI systems more trustworthy and offer extra protections to the public.

Potential Disadvantages

It may stifle innovation, add more costs and red-tape, which may hinder start-ups from entering the market.

How Could The AI Regulation Improve Cyber Security?

Cyber security AI systems play a crucial role in ensuring IT systems are resilient against malicious actors. The new AI Regulations will undoubtedly affect these systems. Exactly how these systems will be affected will depend on the system (e.g. for law enforcement use of biometrics, facial recognition) which may lead to conformity assessments, explainability testing, registration, and more.

Considering the speed and agile process that technology is developed today, companies and innovators should consider how might the future AI Regulation affect such technology development.

Home

New EDPB Guidance on Data Breaches

Remote Working: Risks and Challenges to Businesses

EEA Fines and Penalties Overview

Cybersecurity and the Metaverse

Combatting Cyber Threats with AI

Cyber Security Tips Videos

Key Contacts

Top Tips From Matheson's Data Protection, Privacy and Cyber Security Conference, October 2021

Matheson
P cid ent Management:
T Role f Legal Technology
Deirdre Crowley
Partner, Technology and Innovation, Matheson

Matheson was delighted to host its first Data Protection, Privacy and Cyber Security Conference last October, on the theme of managing a cyber attack.

During the event, Matheson partners Deirdre Crowley and Michael Byrne were joined by expert speakers from the areas of forensic investigation and law enforcement.

Click on any of the video links to hear 1 – 2 minute video snippets outlining key points and practical tips for businesses in the areas of contract law, litigation, legal technology and cyber attack readiness planning.

Home

New EDPB Guidance on Data Breaches

Remote Working: Risks and Challenges to Businesses

EEA Fines and Penalties Overview

Cybersecurity and the Metaverse

Combatting Cyber Threats with AI

Cyber Security Tips Videos

Key Contacts

Key Contacts: Matheson's Data Protection, Privacy and Cyber Security Expert Team

Our highly experienced team of data protection, technology litigation lawyers are available to support your business to prepare, react and recover from a cyber attack.

Anne-Marie Bohan
Partner | Head of Technology and Innovation
E: anne-marie.bohan@matheson.com
T: +353 1 232 2212

Deirdre Crowley
Partner | Technology and Innovation
E: deirdre.crowley@matheson.com
T: +353 21 465 8219

Rory O'Keeffe
Partner | Technology and Innovation
E: rory.o'keeffe@matheson.com
T: +44 7732 901 893

Davinia Brennan
Partner | Technology and Innovation
E: davinia.brennan@matheson.com
T: +353 1 232 2700

Carlo Salizzo
Consultant | Technology and Innovation
E: carlo.salizzo@matheson.com
T: +353 1 232 2011

Michael Byrne
Partner | Commercial Litigation and Dispute Resolution
E: michael.byrne@matheson.com
T: +353 1 232 2075

Nicola Dunleavy
Partner | Commercial Litigation and Dispute Resolution
E: nicola.dunleavy@matheson.com
T: +353 1 232 2033

Questions, Suggestions, Feedback?
Let us know here!

Matheson

This document is confidential and commercially sensitive and is submitted to you on a confidential basis, solely to facilitate the decision whether or not to appoint Matheson to provide legal services to you. It is not to be copied, referred to or disclosed, in whole or part (save for your own internal purposes in connection with the consideration of this submission), without our prior written consent. Matheson retains ownership of the document and all rights in it, including ownership of copyright.

DUBLIN
70 Sir John Rogerson's Quay,
Dublin 2
Ireland

T: +353 1 232 2000
E: dublin@matheson.com

CORK
Penrose One,
Penrose Dock, Cork,
T23 KW81

T: +353 2 1240 9100
E: cork@matheson.com

LONDON
1 Love Lane
London EC2N 7JN
England

T: +44 20 7614 5670
E: london@matheson.com

NEW YORK
200 Park Avenue
New York, NY 10166
United States

T: +1 646 354 6582
E: newyork@matheson.com

PALO ALTO
530 Lytton Avenue
Palo Alto, CA 94301
United States

T: +1 650 617 3351
E: paloalto@matheson.com

SAN FRANCISCO
156 2nd Street
San Francisco CA 94105
United States

T: +1 650 617 3351
E: sf@matheson.com