



Ashurst

Data Protection Round Up 2024

Thursday 30 January 2025

Ashurst Seminar

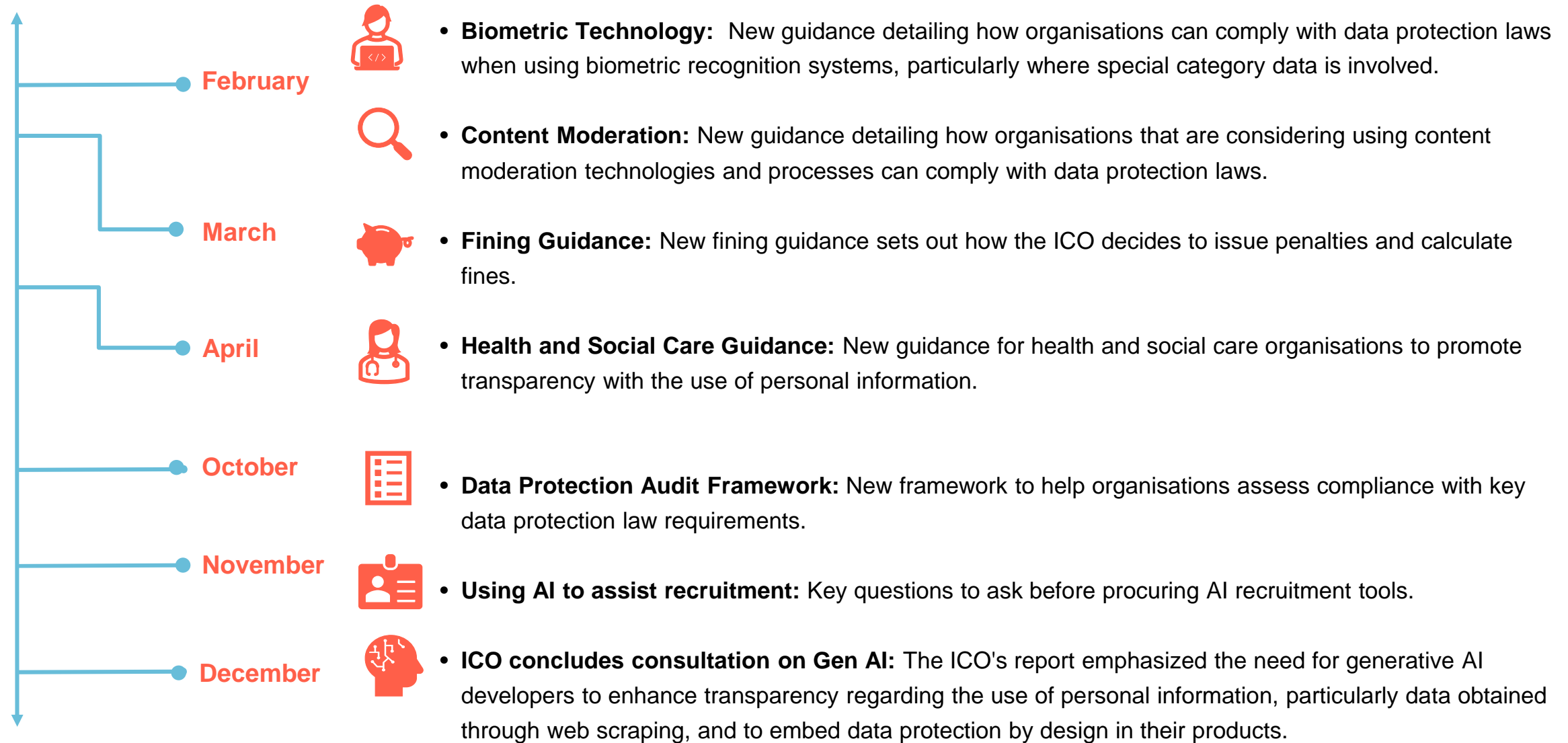
Agenda

- 1 Lessons and trends from the UK
- 2 Key data & AI governance trends
- 3 Employment privacy trends
- 4 Litigation privacy trends
- 5 Lessons and trends from Europe
- 6 2025 predictions

The background of the slide is a solid black field. Overlaid on this are numerous thin, light blue rectangular outlines. These rectangles are of various sizes and are oriented at different angles, mostly tilted towards the right. They are scattered across the entire frame, creating a sense of depth and movement, as if they are floating or falling from the top left towards the bottom right.

Lessons and trends from the UK

Year in review – 2024 ICO guidance



ICO guidance on the horizon for 2025



**Anonymisation &
pseudonymisation guidance**
expected spring 2025



**Profiling and behaviour ID tools
for online safety**
expected spring 2025



**Special category data updated
guidance**
expected spring 2025



**Substantial public interest
conditions updated guidance**
expected winter 2025



**International transfers
guidance**
expected winter 2025

Expected release

Guidance

Early 2025

Data sharing for scams and frauds case studies

Self-service - subject access request – user journey

ICO-CMA position paper on foundations models

Spring 2025

Data protection basics

Consumer internet of things guidance

Handling cyber incidents

Joint guidance: How to build equality & data protection in your
AI procurement process: A guide for councils in England

Encryption updated guidance

The use of storage and access technologies updated guidance

Autumn 2025

Recruitment and selection guidance

Winter 2025

Cloud computing updated guidance

Identity theft updated guidance

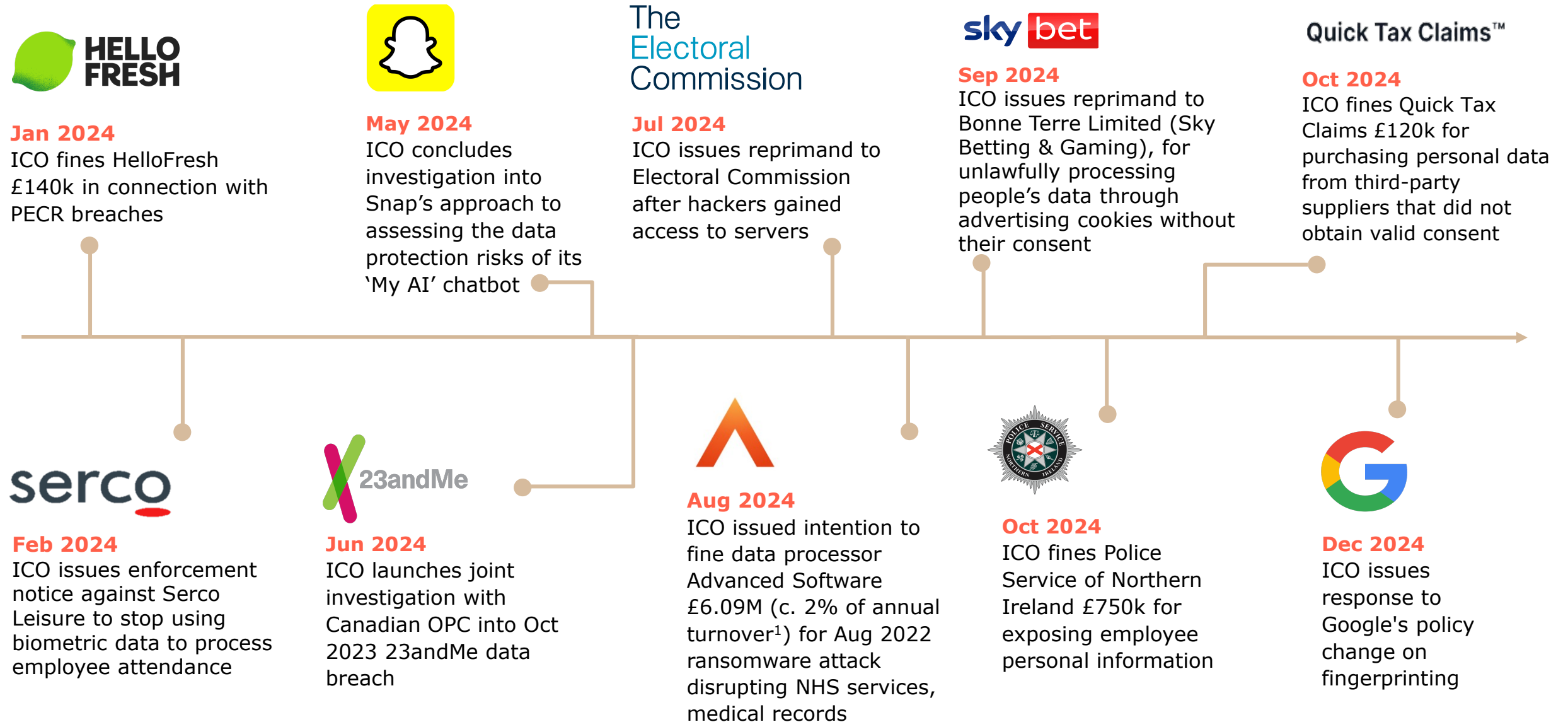
Privacy notice generator for SMEs

Sharing information to safeguard children sector guidance

Employment records guidance

Part 3 law enforcement guidance

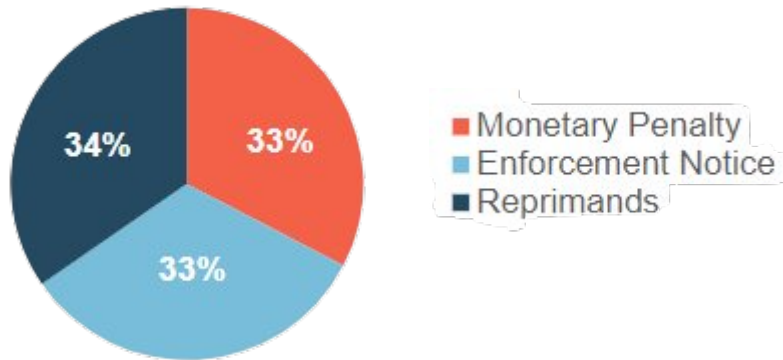
Enforcement and fines in the UK



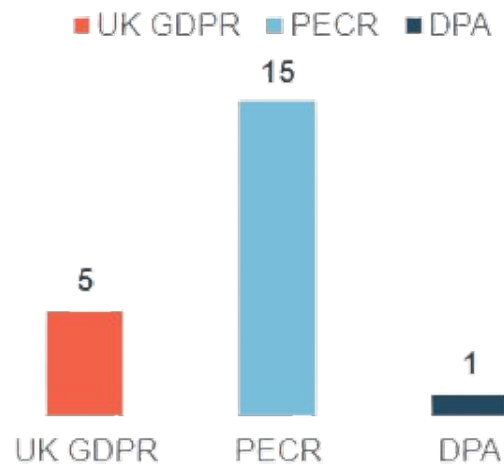
2024 by the numbers

ICO enforcement actions

Types of enforcement



Enforcement legislation – notices & penalties



The majority of enforcement notices or monetary penalties in 2024 were issued for breaches of PECR.



36,049

data protection complaints completed



179

investigations completed



£1.1M

in fines issued for UK GDPR and DPA contraventions



18

reprimands issued

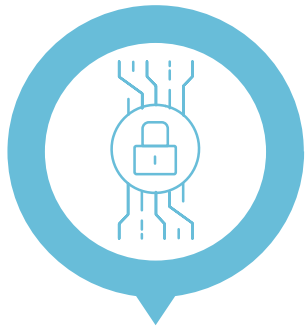
The year ahead for the ICO



Upcoming legislative developments



Data (Use and Access) Bill



Cyber Security and Resilience Bill



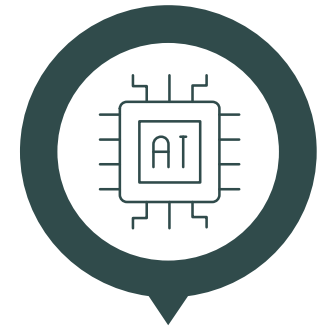
Online Safety Act



UK/EU Adequacy Decisions



Proposed ransomware legislation and consultation



AI Legislation?



Key data & AI governance trends

AI: 2024 Predictions vs. Reality

What we predicted

Developing and embedding traditional and Gen AI use cases

Focus on designing and implementing AI governance frameworks

Continued guidance on the implementation of AI



What we saw

Rush to procure and deploy Gen AI tools and platforms

Focus on AI policy development

Diverging AI legislation, regulation and guidance

2024 Trends in Data Governance



1

**Enhancing data
for AI**



2

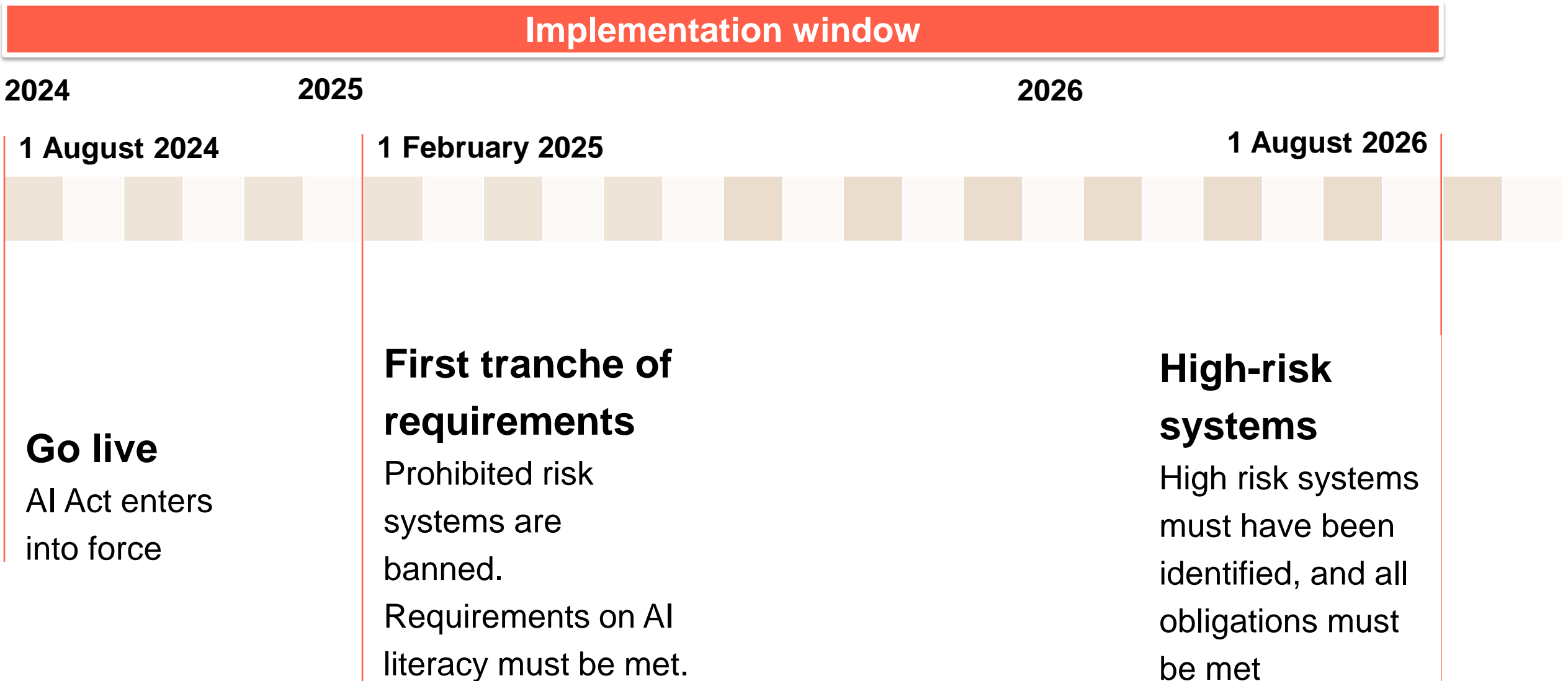
**Managing cyber
threats and
regulatory
scrutiny**



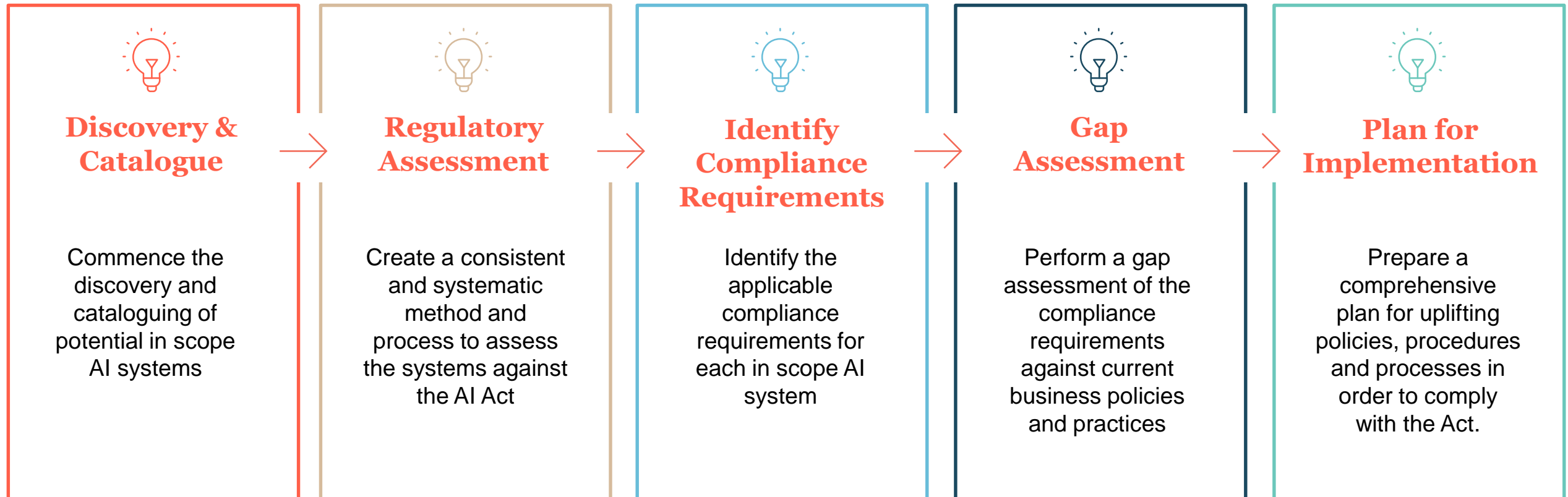
3

**AI-powered data
governance**

2025: time for action on the AI Act



AI Act – practical steps to compliance



Employment privacy trends

Employment trends (issues for employers)

1

HR processes,
recruitment and the
use of AI

2

Employee monitoring
and return to office

3

Disciplinary
processes and data
sharing/disclosure

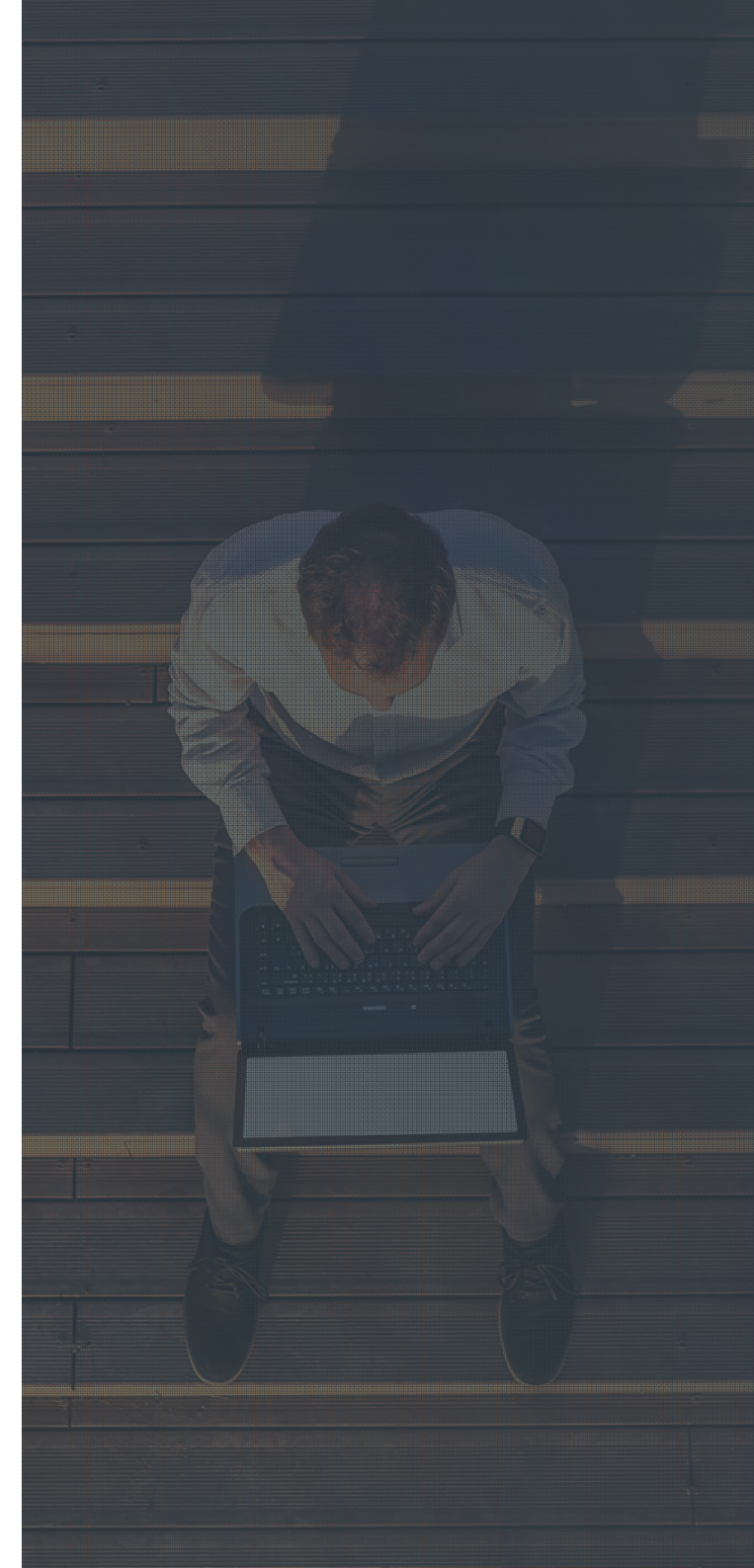
HR, recruitment and the use of AI

Areas that AI is used:

- Recruitment and onboarding
- Monitoring attendance and analytics
- KPI tracking
- Security & phishing
- Grievance and disciplinary processes
- HR queries and engagement

The ICO and AI tools in recruitment

- Sourcing, screening and selection tools.
- The risks around use of AI and automated decision making – fairness, accuracy and bias.
- Transparency & minimisation issues.
- When to use DPIAs.



Employee monitoring and return to office

What have we been discussing with clients?

How to monitor
office attendance

ICO Guidance on
Monitoring and
the need for
DPIA's

What are the
employment law
considerations
and risks?

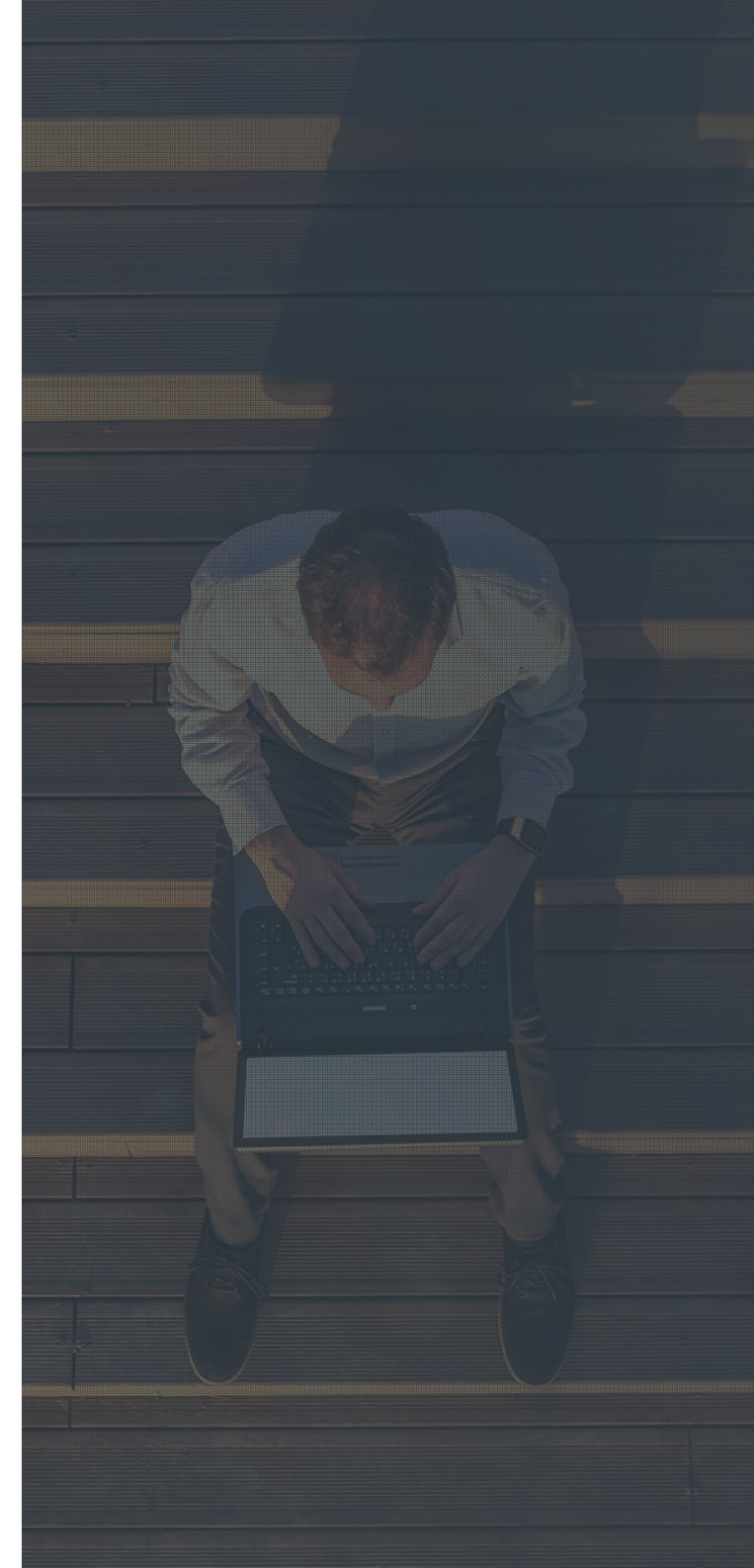
Disciplinary matters and data privacy

What has changed?

- New obligation to prevent sexual harassment in the workplace
- Updated ECHR guidance

What hasn't changed?

- Underlying obligations of privacy regarding employee data and data sharing
- Need to balance employment considerations alongside data privacy principles
- Document your decision-making process!





Litigation privacy trends

Case Updates

The environment post *Lloyd v Google*

**Prismall v
Google &
DeepMind**

Dismissed by
Court of Appeal

**Farley v
Paymaster
(Equiniti)**

Appeal listed for
June 2025

**RTM v Bonne
Terre
(Sky Betting &
Gambling)**

Successful, but no
remedy (yet)

**Gormsen v
Meta**

Novel use of CAT

Lessons and trends from Europe

EU – Non-material Damages Cases 2024



What's the damage?

CJEU - MediaMarktSaturn

- Controller must prove appropriateness of its data security measures.
- Breach is no implicit prove of inappropriateness.
- Claimant must prove well-founded fear of misuse of their data which cannot be only hypothetical.
- No punitive damages and no relevance of degree of fault of controller.



Paving the way for class actions?

EGC - T-354/22 - Bindl v Commission

- IP address, browser and terminal date were transferred to AWS in the US via "sign in with Facebook" link on Commission operated website
- No damage for delay in DSAR response.
- EUR 400 damages for illegal data transfer due to uncertainty regarding processing of IP address.
- Bindl is the founder of EUGD.org, a German-based litigation funding firm focused on EU data protection claims



How to substantiate a non-material damage

BGH – VI ZR 10/24

- Claimant must substantiate facts evidencing loss of control (always carefully shared email and telephone number) and their fear of misuse of data (receives unknown calls, SMS and emails since breach).
- No need to submit with whom email and telephone number were shared.
- Breach of data is equal to injury of body. BGH considers EUR 100 appropriate. "One-digit" damage not sufficient. May be higher if psychological impairment can be substantiated.

EU – Data Protection Litigation Risks Increase

Class actions

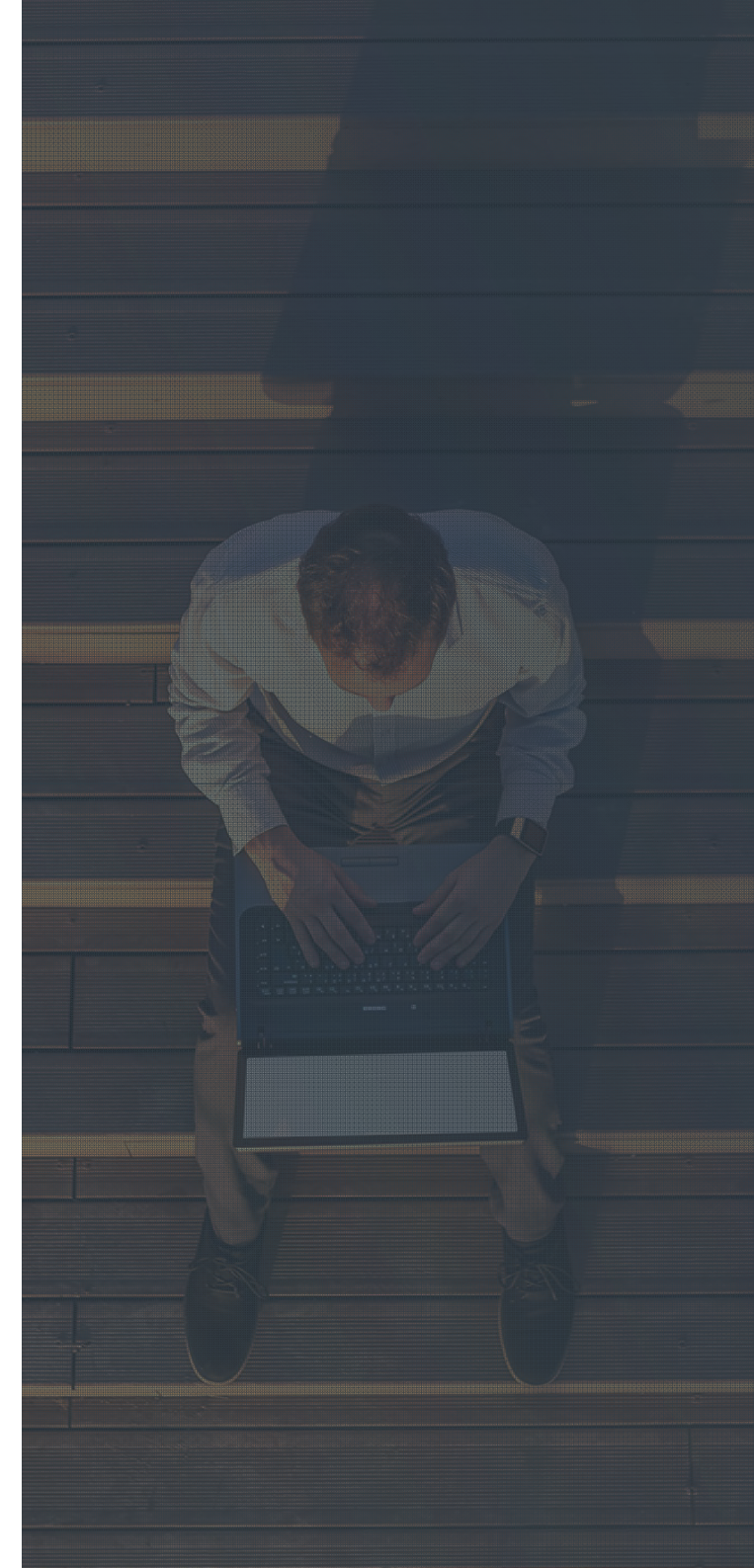
- Class actions in the EU are governed by the Representative Actions Directive.
- Class actions must be initiated by qualified entities that are authorized to bring enforcement actions (e. g. NOYB, The Centre for Consumer Protection in Europe)
- Member states can permit, restrict, or prohibit third-party funding
 - Germany: The third-party funder must not receive more than 10% of the claim's proceeds (Sec. 4 para. 2 no. 3 VDuG)
 - France: Third-party funding is not subject to a specific regulation
 - Spain: Third-party funding is not subject to a specific regulation
- Class actions are particularly well-suited for cases with similar circumstances, especially in instances of data breaches.

Competition law

- CJEU - C-252/21 - Meta vs Bundeskartellamt: National competition authorities can investigate and sanction GDPR violations
- CJEU - C-21/23 – Lindenapotheke: Competitors can challenge violations of the GDPR in court as unfair commercial practices under national law.

Takeaway

- The Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband) has filed a model declaratory action against Meta
- Significant risk in data breaches, as millions of individuals can be affected (see in BGH - VI ZR 10/24: approximately EUR 100 in damages per affected person).



EU – Data Protection Highlight Cases 2024



DSAR – Quo Vadis?

CJEU – Addiko Bank; LG Ellwangen – 6 O 65/24

CJEU: "Copy" does not mean copy of document but copy of personal data. But: Copy of document if needed to verify accuracy and completeness.

Purpose of request (here: to prepare a claim) is irrelevant.

LG: Data subject may request specific electronic format of data delivery (e.g. Excel).



The court is open

CJEU - Lindenapotheke

Competitors have the right to sue for GDPR breaches if allowed under national law.

In particular so, if breach is an unfair commercial practice. Sale of pharmacy medicines creates SCD.

EU – Data Protection Highlight Cases 2024



Address for sale?

*CJEU - Koninklijke Nederlandse
Lawn Tennisbond*

A purely commercial interest can be a legitimate interest if it is lawful.

But sale of addresses to 3rd parties in the specific case likely not lawful.



Watch your mailing lists...

CJEU – DP v juris GmbH

GDPR breach must cause actual damage or harm. Loss of control as such is not enough. Controller is liable for data breaches caused by employees, even if they act negligently. Criteria for calculating fines are not relevant for calculation of damages. No punitive damages.



Targeted ads game changer?

*CJEU - C-446/21 – Meta Platforms v Max
Schrems*

Platform operators may not store user data for targeted advertising without limitation in time and type.

Collecting user data on and off platform for creating profiles for targeted advertising may be extensive and is a factor to be considered when assessing legitimacy.

Most significant EU fines 2024



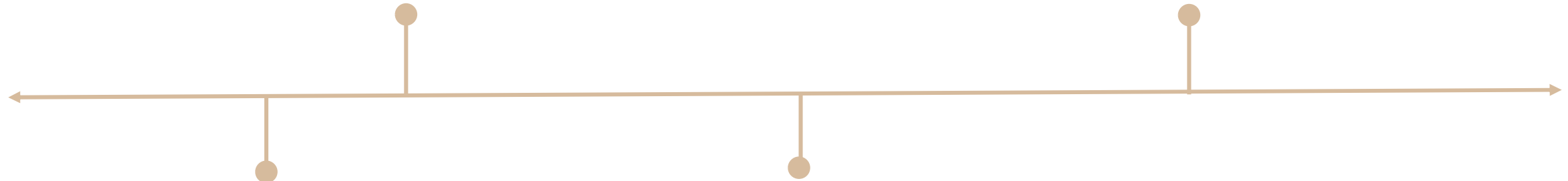
Sep 2024

Meta Platforms Ireland Limited –
EUR 91 million fine (approx. 0.13%
of annual turnover)



Dec 2024

Meta Platforms Ireland Limited –
EUR 251 million fine (approx. 0.36%
of annual turnover)



Aug 2024

Uber Technologies Inc., Uber B.V.
– EUR 290 million fine (approx.
0.8% of annual turnover)



Oct 2024

LinkedIn – EUR 310 million
fine (approx. 1.94% of annual
turnover)

Examples of EU fines



amazon

France's CNIL fined Amazon **€32M** - overly **intrusive employee monitoring system**, inadequate video surveillance measures (scanner to track employees in realtime). Unlawful processing, lack of transparency, excessive data collection for intrusive monitoring and security issues



Vinted

Lithuania DPA fined Vinted **€2.3M** - failure to process data deletion requests; use of "stealth banning" to unfairly block flagged users (excessive impact on users' rights); inadequate responses to data access requests; Cooperation among EU data protection authorities



Openbank 
CaixaBank 

Spain's AEPD fined Openbank **€2.5M** and CaixaBank **€5M**. Openbank – **insufficient security measures** (financial data collected required enhanced safeguards) (appealed); CaixaBank – **security breach** allowed customers to view data on transfers made by others (to be appealed)



 **Clearview AI**

Dutch DPA fined Clearview AI **€30.5M** - unlawful data collection and processing of unique **biometric data for facial recognition without consent** or knowledge. – access to data online cannot be used as pretext for unfair data collection, consent must be obtained

EU Digital regulations 2024-2025

Digital Services Act

Passed on 25.08.2023

Effective from 17.02.2024



Online intermediaries offering services, VLOPs and VLOSEs



Establish a safer, fairer and transparent digital space in the EU for online intermediaries and their users



Key obligations:

- Content moderation and transparency
- Consumer protection in e-commerce
- Risk assessments



Fines of up to 6% global annual revenue

AI Act

Passed on 01.08.2024

Effective partially from 02.02.2025



Prohibited AI systems, High-risk systems, Limited-risk systems, Minimal-risk systems



Key Obligations:

Providers

- Quality management
- Documentation and traceability
- Transparency
- AI by design
- Conformity assessment

Users

- Monitor
- Human oversight
- Relevant data
- Keep logs
- Notify if risk



Prohibited AI: up to €35 million or 7% of global annual turnover **⚠ effective February 2025.**

High-risk obligations: up to €15 million or 3% of global annual turnover

Data Act

Passed on 11.01.2024

Effective partly from 12.09.25



Data holders and users



Key Obligations:

- Data access
- Data sharing
- Transparency
- Data security
- Non-Discrimination
- Cloud switching



Penalties: up to €20 million or 4% of the global annual revenue for data access and data sharing.

⚠ effective September 2025

EU Digital regulations 2024-2025

NIS 2

Passed on 16.01.2023

Implementation deadline expired in October 2024

New target date: March 2025



+50 employees, +€10 million annual revenue, operating in one of the 18 business sectors

Sectors : energy, transportation, banking, financial market infrastructure, healthcare, digital infrastructure, public administration...



Key obligations :

- Risk management and security measures
- Incident reporting
- Supply chain security
- Information sharing
- Governance and accountability



Up to €7 million or 1.4% of the worldwide annual turnover for Important Entities and €10 million or 2% for Essential Entities

Digital Operational Resilience Act

Passed on 16.01.2023

Effective from 17.01.2025



Financial entities (and their ICT vendors)



Key obligations :

- ICT risk management
- ICT-related incidents
- Digital operational resilience testing
- ICT third-party risk management
- Information sharing
- Oversight of critical third-party providers



National authorities take effective, proportionate and dissuasive measures in case of non-compliance

Cyber Resilience Act

Passed on 14.10.2024

Effective from 11.06.2026 on notification and otherwise on 11.12.2027



Manufacturers, importers and distributors of products with digital elements: hardware / software / IoT devices /



Key obligations :

Manufacturers :

- Design and development
- Vulnerability management

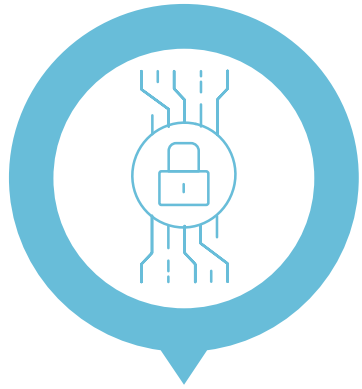
Importers / Distributors :

- Compliance of the product
- Verify cybersecurity risk / proper documentation



Up to €15 million or 2.5% of annual revenue for serious breaches or up to €10 million or 2% of turnover for minor breaches

Landmark Guidelines and Opinions 2024



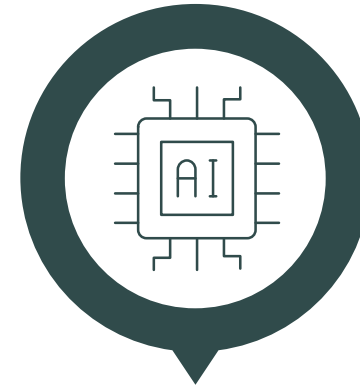
**Guidelines 2/2023
on Technical Scope
of Art. 5(3) of
ePrivacy Directive**



**Guidelines 1/2024
on processing of
personal data based
on Article 6(1)(f)
GDPR**



**Opinion 22/2024 on
certain obligations
following from the
reliance on
processor(s) and
sub-processor(s)**



**AI Guidance: EDPB
Opinion 28/2024**



**Guidelines 01/2025
on
Pseudonymisation
(consultation)**

Key take aways



Consistency

Ensure consistency and adopt a holistic approach in translating these regulations within your organization



Governance and Accountability

Implement risk mgt process, proportionate security measures and document – maintain up to date



Incident notification

Consistent approach on notification – and cooperation process with Authorities



Flow down to supply chain

Sometimes mandatory (GDPR, DORA, NIS2), and otherwise good practice/necessary to allow your organization to comply with your own obligations (e.g. notification)



Data valorisation

Also include IP clause, confidentiality clause etc.

Outlook 2025



2025 predictions

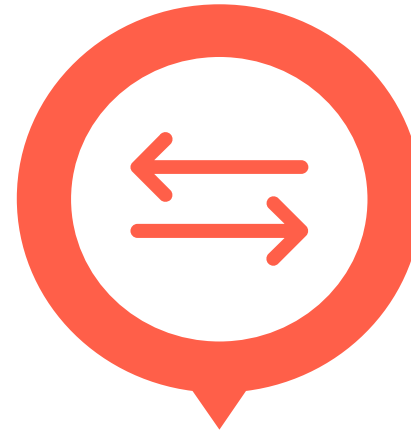
What's next for 2025



Continued cyber
security developments
in the UK and EU
[https://www.ashurst.com/
en/insights/cyber-
readiness/](https://www.ashurst.com/en/insights/cyber-readiness/)



Greater focus on
supply chain
responsibilities




Fracturing of
regulatory environment
between US, UK and
EU



Heightened
accountability
documentation
expectations

Ashurst AI Assess

 This content is for testing purposes only

Ashurst

Welcome to the Ashurst AI Act Assessment Tool

The Ashurst AI Act Assessment Tool is designed for you to identify if AI systems and use cases within your organisation are likely to be within the scope of the EU AI Act.



Next →



Our experts



Rhiannon Webster
Partner
Head of UK Data Privacy and
Cybersecurity



Andreas Mauroschat
Partner
Data Privacy, Frankfurt



Hannah Martin
Senior Associate
Employment



Matthew Worsfold
Partner
Data & Analytics, Risk Advisory



Nicolas Quoy
Partner
Data Privacy, Paris



Rosie Stanger
Senior Associate
Dispute Resolution



Shehana Cameron-Perera
Senior Associate
Data Privacy, London



Cristina Grande
Counsel
Data Privacy, Spain



Tom Brookes
Senior Associate
Data Privacy, London



Subscribe to Data Bytes