



| Data Protection | FOI | Cybersecurity | Unidesk |

Inside: Arnold Clark Faces Class Action | Commissioner 'Steps Aside' | Calls for Transparency By Design |
Loss Of Trust in US and Chinese Tech Firms

The Right to Erasure and Unfounded Malicious Allegations

There has been an extension to the [UK GDPR right to erasure](#), brought into force by the **Victims and Prisoners Act 2024** and the **Data (Use and Access) Act 2025** through regulations made in **March 2026**.

The change introduces a new ground under UK GDPR Article 17, allowing individuals to request the deletion of personal data arising from unfounded and malicious allegations.

The reform was prompted by the experience of Stella Creasy MP, who in 2023 was investigated by social services following a complaint that her children should be taken into care. Although the allegation was found to be baseless, the council was legally unable to remove the complaint from its records. Ms Creasy subsequently proposed an amendment to address this gap in the law.

The new Article 17(1)(g) gives data subjects the right to erasure where personal data have been processed as a result of an allegation that was made by a malicious person, has been investigated by the controller, and has resulted in a decision that no further action is required. The legislation also introduces a statutory definition of a “malicious person”, limited to individuals convicted of specified offences or subject to a stalking protection order.

The change aims to balance safeguarding duties with fairness to those wrongly accused. The provision has been extended to Scotland and Northern Ireland, and controllers are reminded that the right to erasure is not automatic and must still be assessed against other legal obligations, including record-keeping and public interest requirements.

Organisations should have robust policy and procedure for dealing with erasure requests, and ensure they can be dealt with efficiently and speedily, whilst bearing in mind the controller’s responsibilities in terms of statutory duties, safeguarding, anti-fraud measures, etc.



Arnold Clark Faces Class Action

Scottish motorists have been cleared to pursue a major class action against car dealership group Arnold Clark over a [large-scale data breach](#) that resulted in customer information appearing on the dark web.

The ruling follows a decision by the Court of Session in Edinburgh on 16 April 2026, allowing a separate Scottish action to proceed, despite existing litigation already under way in England.

The cyber attack occurred in December 2022 that was later linked to the Play ransomware group. Although Arnold Clark initially stated there was no evidence of customer data being compromised, it subsequently confirmed that hackers had accessed sensitive personal information, including names, dates of birth, contact details, vehicle data and National Insurance numbers.

Arnold Clark attempted to block the Scottish proceedings, arguing that affected customers should be added to the English High Court claim. However, Lord Sandison rejected this, citing the strong Scottish connection, with the vast majority of claimants based in Scotland and contracts governed by Scots law.

Several Scottish law firms are advancing claims on behalf of customers, with thousands already coming forward. Legal representatives have warned that exposure of financially sensitive data could enable identity fraud and cause significant distress. If successful, the action could result in a multi-million-pound compensation bill for the dealership group.

This is another claim that highlights the importance of appropriate cybersecurity measures, and having robust business continuity plans in place if the worst should happen.



Information Commissioner 'Steps Aside'

The UK's Information Commissioner, John Edwards, has [voluntarily stepped aside](#) from his duties while an independent human resources investigation is carried out, the Information Commissioner's Office (ICO) has confirmed.

Edwards said he had stood back from his role in late February to allow the investigation to proceed without interference and stated that he is fully cooperating with the process.

The ICO said the investigation relates specifically to Edwards and will produce a report with recommendations for the Department for Science, Innovation and Technology (DSIT), which will decide on any next steps. No further details have been disclosed in order to protect those involved and safeguard the integrity of the inquiry.

Edwards, who has led the UK's data protection regulator since 2021, confirmed the situation in a LinkedIn post after POLITICO queried his absence. He was already expected to leave his post later in 2026 as part of a wider restructuring of the ICO under the Data (Use and Access) Act.

The ICO's board, Chief Executive and Executive team continue to run the organisation to ensure leadership and regulatory continuity.

HEFESTIS will report on any updates on this one in due course.

Campaigners call for expanded FOISA scope and ‘transparency by design’ reforms

The Campaign for Freedom of Information in Scotland (CFoIS) [has launched its manifesto](#) for the forthcoming Holyrood elections, setting out six actions aimed at strengthening transparency and accountability across public services.

The organisation is calling on all election candidates to endorse the proposals, which it says are the product of a decade of campaigning and evidence-gathering.

Central to the manifesto is support for the Freedom of Information Reform (Scotland) Bill, with CFoIS urging MSPs to back the legislation as it enters Stage 2 at Holyrood from May 2026. The group also calls for equal application of FOI law to all providers of care homes and care at home services, following public consultations held in 2019 and 2025.

Further measures include a proportionate increase in funding for the Scottish Information Commissioner to reflect growing investigative and enforcement demands, and an early commitment to [Anti-SLAPP legislation](#) in the next parliamentary session. CFoIS also urges cooperation with the UK Government to ratify the Council of Europe’s Tromsø Convention and to embed a statutory duty of candour across devolved public bodies.

CFoIS Director Carole Ewart said the proposals offer a non-party-political roadmap to improve democratic scrutiny and public trust.



Other News

[More than 60% of Australian children still using social media despite ban](#)

[Zephyr Energy hackers swiped £700,000 after redirecting a contractor payment](#)

[Civil Service Pension Scheme: Capita confirms data breach](#)

[Booking.com warns customers of hack that exposed their data](#)

[Perth and Kinross Council advised to improve on unacceptable record keeping](#)

8 out of 10 Europeans don’t trust US or Chinese firms with data

More than eight in ten Europeans [do not trust American or Chinese technology companies](#) to handle their personal data responsibly, according to a new POLITICO European Pulse survey. The poll found that 84 per cent of respondents lack trust in US tech firms, while distrust of Chinese companies was even higher, at 93 per cent.

The findings come as the European Union increases efforts to strengthen domestic technology industries and reduce dependency on foreign providers across areas such as artificial intelligence, cloud services and telecommunications.

Although European companies are viewed more favourably, trust remains limited, with only 51 per cent of respondents saying they trust European tech firms with their data. Confidence in national governments was lower still, at 45 per cent.

The survey polled 6,698 people across six EU countries: Spain, Germany, France, Italy, Poland and Belgium. Levels of trust varied by country but consistently showed widespread scepticism towards US and Chinese technology companies’ data-handling practices.

Controllers should note that fair, transparent and lawful data handling raises public trust in organisations.

Contact: dpo@hefestis.ac.uk
www.hefestis.ac.uk
Images: pixabay.com



| Data Protection | FOI | Cybersecurity | Unidesk |

Inside: Southport Victims' Records Accessed 'Inappropriately' | FOI & AI | UK Biobank Breach | Water Leak

Canvas Breach

Instructure, the company behind the widely used Canvas learning management system, has [confirmed a significant data breach](#) that could affect millions of users worldwide.

The incident emerged after the cybercrime group ShinyHunters claimed responsibility for stealing large volumes of data and listing the company on its leak site.

Canvas is used by thousands of schools and universities to manage coursework, communications and student information, making it a high-value target for attackers. Reports suggest that as many as 275 million users across nearly 9,000 institutions could be impacted by the breach.

According to Instructure, the compromised data appears to include names, email addresses, student ID numbers and user messages. However, the company stated there is currently no evidence that more sensitive information—such as passwords, financial data, government identifiers or dates of birth—has been accessed.

The firm confirmed the incident on 2 May 2026 and said it has since taken steps to contain the breach. These measures include deploying security patches, increasing system monitoring, rotating application keys and requiring customers to reauthorise Application Processing Interface(API) access. External cybersecurity experts and law enforcement agencies are also involved in the ongoing investigation.

Despite reassurances, users are being urged to remain vigilant. Security experts warn that exposed contact information could be used in targeted phishing attacks, with scammers potentially exploiting legitimate-looking academic communications. Users are advised to update passwords, monitor account activity and verify unexpected messages through official channels.

Organisations affected will be contacted directly.

If you use this learning tool, but have not received a direct notification, contact your DPO for advice and assistance.



NHS staff accessed Southport victims' records 'inappropriately', hospital trust admits

An [NHS hospital trust has admitted](#) that nearly 50 staff inappropriately accessed the medical records of victims of the Southport knife attack, in what has been described as a serious breach of patient confidentiality.

The incident occurred at Aintree University Hospital in Liverpool in the days following the July 2024 attack, which left three young girls dead and several others injured. Among those affected were a teenage girl and adult survivor Leanne Lucas, who was critically wounded.

University Hospitals of Liverpool Group (UHLG) said the breach was “inexcusable” and was identified through a routine audit. The trust confirmed that 48 members of staff accessed records without clinical justification. Disciplinary measures were taken, ranging from counselling to final written warnings, but no staff were dismissed.

Ms Lucas said she was “devastated and horrified” and criticised the trust for failing to inform her for almost two years, accusing it of attempting to conceal the incident. Lawyers representing victims described the breach as a “deeply disturbing abuse of power”.

The trust denied any cover-up, stating it delayed informing patients on clinical advice to avoid further distress.

This horrendous case highlights the need for a zero trust framework for sensitive data, and ensuring that only those that have a genuine business need to access data, can actually access that data.



FOI and AI

The Information Commissioner's Office (ICO) [has issued guidance](#) on the growing use of artificial intelligence (AI) in Freedom of Information (FOI) requests, noting a rise in complex and high-volume submissions during 2025.

Practitioners report that AI-generated requests are often lengthy, repetitive and unclear, sometimes including irrelevant material or inaccurate references to legislation. This can make them more difficult and time-consuming to process. However, the ICO emphasises that the use of AI does not, in itself, make a request invalid, provided it meets the requirements of the Freedom of Information Act (FOIA) (FOISA in Scotland).

Public authorities are advised to continue applying existing FOI principles, including seeking clarification where requests are unclear and offering advice to help refine overly broad submissions. Requests may still be refused if they exceed cost limits or are deemed vexatious, particularly where AI is used to generate repeated or burdensome enquiries.

The ICO also highlights that information generated using AI tools by public bodies is subject to FOI, including prompts and stored interactions. While AI may offer efficiencies in handling requests, organisations must ensure accuracy, transparency and compliance with data protection law.

In some cases, it may be possible to clarify matters quickly with a direct chat with the requestor. If you need FOISA advice, contact jnock@hefestis.ac.uk

UK Biobank Breach

Confidential health records from the [UK Biobank have been exposed online](#) on multiple occasions, raising serious concerns about data security within one of the country's leading medical research projects.

UK Biobank, which holds detailed medical and genetic information from around 500,000 UK volunteers, is widely regarded as a critical resource for research into conditions such as cancer, dementia and diabetes. However, an investigation found that datasets had been inadvertently published dozens of times, often by authorised researchers.

The leaked files did not contain direct identifiers such as names or addresses, but experts warned they could still pose significant privacy risks. In one case, a dataset included hospital diagnoses and dates for more than 400,000 participants. Using limited details such as birth date and surgery history, it was possible to identify an individual record, raising fears over re-identification.

The breaches are thought to have occurred when researchers accidentally uploaded data to public platforms such as GitHub while sharing code. Although such sharing is increasingly required by academic publishers, it has created new vulnerabilities.

UK Biobank said it had seen no evidence of participants being identified and insisted strong safeguards remain in place. It has issued legal takedown notices and strengthened controls, but experts described the scale of the issue as "shocking" and warned of growing risks in the age of artificial intelligence.

Organisations should consider whether their staff are going 'off-piste' with data storage, particularly researchers who handle large volumes of sensitive data. Staff should be advised to store data within organisationally approved areas and tenancies.



Other News

[Five steps to protect your organisation from AI-powered cyber threats](#)

[Summary of the King's Speech Legislation](#)

[Announcements](#)

[Palantir's access to identifiable NHS England patient data is 'dangerous', MPs say](#)

[AI facial recognition oversight lagging far behind technology, watchdogs warn](#)

[Collateral Damage: Grok AI and the Human Cost of Generative AI](#)

Water Leak

The Information Commissioner's Office (ICO) [has fined South Staffordshire Plc and South Staffordshire Water Plc](#) £963,900 following a significant cyber attack that led to the personal data of more than 633,000 individuals being published on the dark web.

The breach originated from a phishing email, which allowed attackers to install malicious software that remained undetected within the company's systems for around 20 months. In May 2022, the attacker escalated access to domain administrator level, gaining extensive control over the network.

The company reported the incident in July 2022, after which a ransom note was discovered. Subsequent investigations revealed that approximately 4.1 terabytes of data had been exfiltrated and later released online. The compromised information included employee records, customer account details, and banking information such as account numbers and sort codes.

The ICO found that the organisation had failed to implement appropriate technical and organisational measures as required under UK GDPR. Weaknesses included inadequate monitoring, poor vulnerability management, and the use of outdated systems.

The regulator reduced the original penalty by 40% due to the company's early cooperation and has urged organisations to strengthen cyber resilience and security controls.

This reinforces the need for organisations to keep reminding staff about phishing emails, and how to spot them.

Contact: dpo@hefestis.ac.uk
www.hefestis.ac.uk
Images: pixabay.com



| Data Protection | FOI | Cybersecurity | Unidesk |

Inside: Sky High Fine | Complaints | New Coworker | Empires Strike Back

Information Commissioner Resigns

John Edwards [has resigned as UK Information Commissioner](#) and Chair of the newly formed Information Commission, following the outcome of an internal workplace investigation.

The announcement, made via LinkedIn on Friday, comes as the Information Commissioner's Office (ICO) prepares to transition into a new statutory structure under the Data (Use and Access) Act 2025.

The resignation follows an ICO HR investigation which found there was a "case to answer" regarding Edwards' conduct. In his statement, Edwards acknowledged that he had, on occasion, exercised poor judgement and made attempts at humour that were inappropriate and caused offence. An official ICO statement confirmed that the investigation concluded his behaviour fell short of what is expected of a public official.

Further details emerged on Saturday from the Secretary of State for Science, Innovation and Technology, Liz Kendall, who expressed serious concern about evidence of "vulgar and highly sexualised language" in interactions with staff. She criticised Edwards' characterisation of the incidents as humour, stating that such behaviour has no place in the workplace, particularly from a senior leader.

Despite the leadership upheaval, the ICO's regulatory work is expected to continue without interruption. Senior officials have been carrying out the Commissioner's functions during Edwards' suspension and will maintain operations while a successor is appointed. The episode has also prompted criticism of the ICO's lack of transparency in handling the matter.

Whilst this is of interest to the data protection community, there seems to be little to say regarding data protection (aside from the suggestion that social media may not be the best place to make announcements in such cases). In any event, as any HR department will tell you: no matter the seniority of the role, always keep it professional.



Sky High Fine

Spain's data protection authority has imposed a record €18 million fine on Amadeus IT Group for GDPR breaches linked to the reuse of traveller data without appropriate safeguards.

The sanction follows an investigation by the Agencia Española de Protección de Datos (AEPD) into a pilot profiling project using booking data processed through Amadeus's global distribution system. The case originated from a complaint alleging that passenger information was repurposed to create detailed traveller profiles without proper transparency or consent.

Regulators found that Amadeus relied on "legitimate interests" but failed to demonstrate a valid legal basis under Article 6 GDPR. It also breached Article 14 by not adequately informing individuals about how their data—often obtained indirectly from airlines and travel agents—would be reused.

The project involved combining passenger name record data, including historical booking information, with other datasets to analyse behaviour and support commercial insights. Authorities concluded that this secondary use was incompatible with the original purpose for which the data was collected.

Although the penalty was reduced to €14.4 million following voluntary payment, the decision highlights increasing regulatory scrutiny of data repurposing and profiling.

The case underlines the importance of transparency, lawful basis and purpose limitation under GDPR, particularly where organisations seek to reuse customer data for analytics or commercial innovation.

For educational organisations, the biggest risks here are liable to be in the areas of AI use, and commercialisation of organisational services. When data is being used beyond its original purpose, a screening process or full DPIA is recommended.



Complaints

[A new legal duty](#) governing how organisations handle data protection complaints has come into force across the UK on 19th June 2026.

All organisations processing personal data must now provide clear routes for individuals to raise complaints, acknowledge them within 30 days, investigate appropriately and communicate outcomes.

The ICO said the reforms, introduced by the Data (Use and Access) Act, aim to embed consistent complaints handling as standard business practice. Research indicates more than two-thirds of businesses aware of the Act either misunderstand it or believe it does not apply to them.

Latest [guidance issued by the regulator](#) outlines expectations and practical examples, including common issues such as subject access requests, inaccurate data and marketing concerns.

Deputy Commissioner Emily Keaney stressed the importance of trust, transparency and early resolution, adding that effective complaint handling reduces escalation. The ICO said it will support organisations as the new requirements are implemented.

Consult with your DPO if you need further advice.

New Coworker

Microsoft has announced the general availability of Copilot Cowork, its latest “agentic” AI capability within Microsoft 365, marking a shift from assistive tools to systems that can execute work on behalf of users.

Unlike traditional Copilot features, which generate drafts or summarise content, Cowork is designed to carry out complex, multi-step tasks across applications, files and organisational data, returning completed outputs rather than suggestions.

The service is now available globally to licence holders of Microsoft 365 Copilot, following a preview phase that reportedly saw strong enterprise uptake.

A key feature is its ability to run tasks in the cloud using organisational context, enabling it to analyse large datasets, automate workflows and coordinate actions across tools such as Teams, Outlook and Excel.

Pricing introduces a hybrid model. Users must hold a Microsoft 365 Copilot licence, while Cowork itself is billed separately on a usage basis through “Copilot Credits”, with costs varying depending on task complexity, model use and processing time.

Administrators can manage deployment through controls, including spending limits and access restrictions, and the feature is disabled by default.

The launch reflects Microsoft’s broader push towards autonomous workplace AI, though concerns remain over cost, predictability and governance.

Organisations should be cautious about switching on new AI tools unless they are sure about how they work, what data they use for AI training purposes, and whether data stays within the MS365 tenancy.



Other News

[Italy's privacy watchdog fines Emirates over handling of passenger health data](#)

[Met to expand use of live facial recognition into central London by Christmas](#)

[Shared NHS patient records could cut 20,000 A&E visits a year, ministers claim](#)

[Meta workers can opt out of being tracked at work - but only for half an hour at a time](#)

[Biobank data incident caused by 'a few bad apples', boss says](#)

Empires Strike Back

Social media companies [have criticised UK government plans to ban under-16s](#) from accessing major platforms, warning the move could expose young people to greater risks online.

Prime Minister Sir Keir Starmer announced the proposed ban, arguing that social media contributes to bullying, unhappiness and potential harm to children’s mental health. The policy would prevent younger teenagers from using named services and is expected to be introduced by next spring.

Technology firms including Meta, YouTube and Snapchat have strongly opposed the measure. They argue that a blanket ban could drive children towards unregulated or less safe online spaces, undermining existing safeguards such as parental controls and moderated environments.

The plans go further than similar measures adopted internationally, including in Australia, and may extend to restricting features such as chatting with strangers on other digital services, including gaming platforms.

Despite industry opposition, ministers are pressing ahead, framing the policy as a decisive intervention in response to growing concerns about young people’s online safety and wellbeing.

There are general privacy concerns about this measure, not least that over-16s may be forced to prove their age, thereby introducing Digital ID by the back door, as claimed by some.

Contact: dpo@hefestis.ac.uk
www.hefestis.ac.uk
Images: pixabay.com