



| Data Protection | FOI | Cybersecurity | Unidesk |

Inside: Invasive Social Media| Apple Order |Unlawful Marketing| Peggie Breach

Capita Fined £14 Million

On 15 October 2025, the Information Commissioner's Office (ICO) [imposed a £14 million fine](#) on Capita following a major data breach affecting approximately 6.6 million individuals.

The penalty was divided between Capita plc (£8 million) and Capita Pension Solutions Limited (£6 million), the latter of which manages data for over 600 pension schemes.

The breach occurred in March 2023 when a malicious file was inadvertently downloaded onto an employee's device. Although a security alert was triggered within ten minutes, the device was not quarantined for 58 hours—far exceeding Capita's one-hour response target. During this window, the attacker gained administrator access, moved laterally across systems, and extracted nearly one terabyte of data. Ransomware was later deployed, locking Capita personnel out of their systems.

The ICO's investigation highlighted several failings in Capita's security posture:

- Lack of tiered administrative account controls, enabling privilege escalation.
- Delayed incident response due to understaffing in the Security Operations Centre.
- Inadequate penetration testing and risk assessments, with findings not shared or acted upon across the organisation.

Initially, the ICO proposed a £45 million fine, but this was reduced after Capita demonstrated mitigating actions, including system improvements, offering credit monitoring to affected individuals, and cooperating fully with investigations. Capita accepted responsibility and agreed to pay the fine without appeal.

This case highlights the need for robust security (appropriate for the sensitivity of the data involved), strict access controls, and staff awareness of procedures and protocols to follow in the event of such an incident.



Invasive Social Media

A new study by data protection firm Incogni has identified Facebook, WhatsApp, and TikTok as the most privacy-invasive social media platforms in 2025.

Social Media Privacy Ranking 2025 assessed 15 major platforms, examining their data handling, AI training practices, transparency, and regulatory compliance.

Meta's platforms—Facebook, Instagram, and WhatsApp—alongside TikTok, received the lowest scores, having been penalised across all assessment categories. The study highlights that 12 of the 15 platforms may use personal data to train AI models, with only Discord, Telegram, and Twitch explicitly stating they do not.

Discord emerged as the safest platform, praised for its clear stance against using user data for AI training. Pinterest and Quora followed as relatively privacy-conscious platforms. The study marks a shift from 2024, when Reddit, Snapchat, and Pinterest were deemed most invasive.

The study also draws attention to regulatory scrutiny, with Facebook receiving the highest number of fines globally, including multiple GDPR violations. Additionally, some platforms, including LinkedIn and Meta's services, were found to collect sensitive demographic data, such as race, sexual orientation, and health information.

Head of Incogni, Darius Belejevas, called for stronger transparency and user control, warning that evolving AI practices pose growing risks to personal data privacy.

From an organisational viewpoint, it's important to be aware if, and how, your staff are using such platforms in the workplace.



Apple Order

The UK [government has issued a revised order](#) allowing access to the personal data of Apple users based in the UK, intensifying its dispute with the tech giant over privacy rights.

The move follows a previously withdrawn demand for global access, which had provoked strong objections from the US, including criticism from Director of National Intelligence Tulsi Gabbard.

The new order, reportedly a compromise, excludes non-UK users but still raises concerns. Apple, which removed its Advanced Data Protection (ADP) feature from the UK market, expressed disappointment and reiterated its commitment to end-to-end encryption and user privacy. A legal tribunal is still scheduled for January 2026.

Civil liberties groups, supported by a judge's ruling, successfully argued that the legal proceedings should not be held in secret. The Home Office declined to confirm the order's existence, citing operational confidentiality, but stated that Home Office priority is national security.

Combined with the announcement that the UK Government is considering a Digital ID system, this order has led activists to argue that privacy rights are under threat in the UK, but it's far from clear who will come out on top in this particular battle.

£250,000 Fine for Making Unlawful Marketing Calls

The Information Commissioner's Office (ICO) [has fined two energy firms a combined £250,000](#) for making unlawful marketing calls to individuals and businesses listed on the UK's "do not call" registers.

Crown Glazing Ltd, based in Preston, received a £130,000 penalty for over 500,000 unsolicited calls to people registered with the Telephone Preference Service (TPS), resulting in 37 complaints. The firm was found to have misrepresented itself as acting on behalf of the UK Government in promoting double-glazing and energy tests.

Maxen Power Supply Ltd, an Essex-based supplier, was fined £120,000 following over 100 complaints about aggressive and repeated calls to TPS and Corporate TPS registrants. The company used overseas call centres that falsely claimed to represent National Grid or existing energy providers, requesting sensitive information under the guise of helping customers save on energy bills.

Maxen denied responsibility, citing the use of third-party contractors.

Both companies have been issued with enforcement notices requiring them to cease contacting individuals and businesses who have opted out of marketing calls or previously objected.

The ICO emphasised the importance of respecting consumer privacy and warned of further action against firms breaching direct marketing laws.

If your organisation sends out marketing or promotional materials, you need to be confident in your lawful bases, be aware of different types of subscribers, and general good practice in this area. Contact your DPO for more information.

The ICO has also recently published guidance on [direct marketing and the public sector](#).



Other News

[Digital ID: Some Issues](#)

[A Pinch of GDPR: Gregg Wallace Serves Up a Data Rights Claim](#)

[University Redundancy Letters Breach](#)

[Offboarding: Delete!](#)

[NI parents caught in UK crackdown lose child benefit](#)

[Hundreds of Misplaced Devices Put University Data at Risk](#)

Peggie Breach

Nurse Sandie Peggie has [demanded answers](#) from NHS Fife after discovering the health board shared unredacted personal information about her with SNP ministers without her consent. The disclosures, revealed through a Freedom of Information request, included details of her occupational health and internal employment matters.

Peggie, who previously took NHS Fife and Dr Beth Upton to an employment tribunal after being suspended for objecting to sharing a changing room with the trans medic, is now seeking legal clarification on the data breach.

Her solicitor, Margaret Gribbon, described the disclosure as "concerning" and has written to NHS Fife requesting an explanation. NHS Fife's briefing documents to ministers suggested Peggie's personal circumstances may have contributed to the incident and criticised her handling of the situation.

Although cleared of gross misconduct, Peggie is now pursuing further legal action. The tribunal's outcome is pending, with legal costs for NHS Fife already exceeding £320,000.

Organisations should take special care when processing special category data, and particularly when contemplating disclosure to a third party.

Contact: dpo@hefestis.ac.uk
www.hefestis.ac.uk
Images: [Pixabay](#)



| Data Protection | FOI | Cybersecurity | Unidesk |

Inside: PSNI could 'come to complete stop' | Non-Reporting Fine | Draft UK Cyber Security and Resilience Bill
| Afghan Data Breach

Reform of EU GDPR

The [European Commission has published](#) two major proposals: the Digital Omnibus Regulation and the Digital Omnibus on AI Regulation; aimed at reducing administrative burdens and modernising EU data protection and AI laws.

If adopted, these measures will introduce targeted changes to the EU GDPR and related legislation, with potential implications for future UK reform.

Key EU GDPR amendments include clarifying the definition of personal data, confirming that data is not personal if identification is not "reasonably likely". Processing for AI training may qualify as a legitimate interest under defined conditions. Data breach reporting will be simplified, requiring notification only where there is "high risk" to individuals, with deadlines extended to 96 hours. Harmonisation of Data Protection Impact Assessments is proposed through EU-wide lists, and rules for scientific research processing will be clarified.

The AI Regulation proposals include lighter compliance for SMEs, streamlined technical documentation, and expanded sandbox testing. Oversight will be centralised under an empowered AI Office to reduce governance fragmentation.

Both packages now enter trilogue negotiations with the European Parliament and Council, expected to take several months.

UK Context: The UK's recent Data (Use and Access) Act 2025 introduced modest GDPR changes compared to the EU proposals. While previous Conservative plans for deeper reform were abandoned, current indications suggest the Labour Government is unlikely to pursue major changes soon. It would, however, be ironic if the actions in the EU embolden the UK Government to make further, business friendly, amendments.

HEFESTIS will monitor EU developments and update in due course.



PSNI could ‘come to complete stop’

Northern Ireland Public Service Alliance (NIPSA) [has warned](#) that the Police Service of Northern Ireland (PSNI) could “come to a complete stop” if civilian staff strike over unpaid compensation linked to a 2023 data breach.

The breach saw personal details of thousands of officers and staff mistakenly released in a Freedom of Information response. Despite Stormont agreeing a compensation package, PSNI told the High Court in September that the estimated £100m bill was “not affordable within current funding”. Several test cases are currently before the court to determine damages.

A trade union official said members had given a “clear endorsement” for industrial action, with a strike ballot imminent. She warned that a walkout would halt critical functions, including call handling, custody units, and forensic services, leaving officers without communications. NIPSA accused the UK Treasury of failing to grasp the impact on Northern Ireland, urging it to “pay up”.

PSNI Assistant Chief Constable Melanie Jones said that contingency planning is under way to maintain public safety. Justice Minister Naomi Long branded the Treasury’s refusal to fund compensation as “reckless”, though the Treasury insists that Northern Ireland has received its largest financial settlement since 1998.

Though this is an extreme case, it flags the potential for the ‘ripple effects’ of a data breach: [a phenomenon flagged](#) by the Information Commissioner back in 2024.

Training and guidance in data breach prevention and management are essential to avoid breaches and the potential consequences.



Fined for non-reporting

In news from Poland, Gyncentrum, [a medical centre acting as data controller](#), experienced a breach when an employee mistakenly emailed a bank transfer confirmation to the wrong patient with the same first name.

The document contained the data subject’s full name, address, bank account details, transfer amount, and a genetic test reference, indirectly revealing sensitive health data. The data subject discovered the incident independently, as the controller neither informed them nor reported it to the Statutory Authority (SA). The controller claimed the breach posed no risk to individuals’ rights or freedoms.

The SA ruled that the controller breached Articles 33 and 34 GDPR by failing to report a personal data breach and notify affected individuals promptly. The incident, caused by human error, involved unauthorised disclosure of health-related data, classified as special category under Article 9.

The SA found the controller’s risk assessment incorrect, imposed a PLN 40,000 (€9,000) fine, and issued a warning, stressing timely breach reporting as vital for data security.

Every data security incident must be considered case by case, and appropriate risk assessments carried out regarding both reporting, and the risk of harm to the data subject’s rights and freedoms.

Draft UK Cyber Security and Resilience Bill enters UK Parliament

On 12 November 2025, the [UK government presented](#) the draft **Cyber Security and Resilience (Network and Information Systems) Bill** to Parliament.

The legislation, first announced in July 2024, seeks to amend the Network and Information Systems Regulations 2018, aligning with principles from the [EU's NIS2 Directive](#). Its primary aim is to strengthen protections against escalating cyber threats to essential services.

Key proposals include expanding the scope of regulated entities to cover medium and large data centres, managed service providers, major load controllers, and designated critical suppliers.

These organisations must meet defined security standards, report significant incidents promptly, and maintain contingency plans.

The Bill introduces stricter enforcement through turnover-based penalties for serious breaches and grants the Technology Secretary powers to mandate proportionate measures during national security threats.

It also enhances incident reporting obligations, requiring initial notification within 24 hours and a full report within 72 hours. Additionally, affected customers may need to be informed swiftly following cyber incidents.

The UK Government states that these measures aim to bolster resilience and address supply chain vulnerabilities.

HEFESTIS will monitor progress of The Bill, and in the meantime organisations should consider whether their cyber incident procedures are effective.



Other News

[10 Tips To Avoid Email Errors](#)

[Guidance for Risk Management of AI Systems](#)

[Charitable Purpose Soft Opt-in - ICO](#)

[Gmail Passwords Confirmed Within 183 Million Account Infostealer Leak](#)

[WhatsApp Flaw Exposed 3.5 Billion User Accounts](#)

[ICO consultation on data protection enforcement procedural guidance](#)

Afghan Data Breach

Research submitted to the Commons Defence Select Committee has revealed [the severe impact](#) of the Ministry of Defence's (MoD) 2022 data breach, which exposed details of nearly 19,000 Afghans seeking relocation to the UK.

Of 231 respondents notified by the MoD, 49 reported that a family member or colleague had been killed as a result of the breach. Additionally, 87% said they or relatives had received threats, while 43% faced direct threats to their lives. More than half reported Taliban intimidation of family or friends.

The study, led by Refugee Legal Support and UK academics, criticised the two-year delay in notifying affected individuals, calling it "deeply concerning". Campaigners urged urgent action to accelerate relocations and provide redress.

The breach, initially concealed under a superinjunction, has sparked accusations of negligence and mismanagement. Whilst the MoD insists that targeting based solely on leaked data is "highly unlikely", critics argue the delay placed lives at unnecessary risk.

This story obviously has some way to run before the final resolution.

Contact: dpo@hefestis.ac.uk
www.hefestis.ac.uk

Images: Organisational Websites



Use of employee data during pay talks 'concerning'

[Lloyds Banking Group has admitted using data](#) from the personal bank accounts of more than 30,000 employees during pay negotiations.

The UK's largest lender analysed anonymised, aggregated information on staff spending, saving habits and salary increases, comparing them with the wider public to assess financial resilience amid the cost-of-living crisis. The bank, which owns Halifax and Bank of Scotland, said the practice complied with regulations and reflected common industry standards.

However, unions raised concerns that the analysis could have influenced pay offers. Affinity, which represents Lloyds staff but is not formally recognised, criticised the move as unjustified and claimed loyalty was being used against employees. Correspondence seen by the Financial Times suggested the data was used to argue staff were "more financially resilient", potentially justifying lower awards. Lloyds denies this.

The resulting offer, a multi-year deal, backed by Unite and Accord unions, offers junior staff pay rises of 7–9%, plus £1,200 annual increases in 2026 and 2027, bringing minimum salaries to £27,400. Two-thirds of members voted in favour, though Affinity rejected the proposal.

Legal experts have urged the Information Commissioner to investigate whether the exercise was fair and transparent, questioning if employees were informed or allowed to object. Lloyds said it was "pleased" the recognised unions supported its competitive offer.

The most obvious data protection issues arising here are related to profiling, transparency, lawfulness, and purpose limitation. Reference to the data protection principles would be useful in such situations, even when dealing with 'anonymous' or 'aggregated' data, especially for employees or managers using data analysis tools such as Power BI.



Post Office under scrutiny again

The Information Commissioner's Office (ICO) [has formally reprimanded Post Office Limited](#) following a data breach that exposed personal information linked to the Horizon IT scandal.

In April 2024, the Post Office mistakenly published an unredacted legal settlement document on its corporate website, revealing the names, addresses and postmaster status of 502 individuals involved in group litigation.

This information remained publicly accessible until June 2024, when an external law firm alerted the organisation.

The ICO's investigation found the breach resulted from failures in both technical and organisational safeguards. These included insufficient publication protocols, inadequate staff training on sensitive data, and poor quality-assurance procedures for website content.

While initial recommendations included a fine of up to £1.094 million, the ICO concluded the breach was not "egregious" by its public-sector standards and consequently issued a reprimand rather than a financial penalty.

Post Office Limited has since taken remedial measures: it offered compensation to those affected, provided two years of identity protection services, removed cached documents from search engines, convened an emergency internal review group, and implemented a formal publishing policy.

The ICO emphasised that robust publication protocols, staff training and data classification are essential to prevent similar errors.



SIC orders release

The Scottish Information Commissioner, David Hamilton, has ruled that the Scottish Government must publish portions of the written evidence provided to James Hamilton KC for his inquiry into whether former First Minister Nicola Sturgeon breached the Ministerial Code.

In Decision 279/2025, issued on 27 November, the Commissioner found that the Government had wrongly withheld certain documents using exemptions related to public affairs and legal privilege. Back in December 2023, the Court of Session determined that the Scottish Government did indeed hold the requested material, prompting the present ruling.

While some information is rightly classified — for instance, to comply with court orders or protect legal advice — the Commissioner demanded release of additional redacted content, noting that disclosure would not significantly impede future inquiries. He also raised concerns over procedural missteps: the Government initially failed to supply all materials under an Information Notice issued in March 2024, and adjusted its exemption claims inconsistently during the investigation.

Hamilton acknowledged no evidence of bad faith but remarked that the Government's handling "reflects poorly" and urged immediate corrective actions. A revised response must be issued by 12 January 2026.

A reminder that information held under FOISA should generally be released unless exemptions can be genuinely and appropriately applied.

AI Awareness

Organisations and individuals [are increasingly exposed](#) to AI features embedded in everyday tools, often enabled by default without clear explanation of how they operate or what data they use.

Recent developments, such as LinkedIn sharing user-generated content for large language model training, highlight the need for active opt-outs to protect privacy.

Businesses are also adopting AI capabilities within HR, finance and data management systems, sometimes without proper oversight, raising concerns for data protection teams.

Experts warn that seemingly harmless functions, like meeting transcription or location tracking in Microsoft Teams, can amount to workplace monitoring and require legal and proportionality checks.

Organisations should conduct due diligence before enabling AI tools, ensuring clarity on objectives, roles, and compliance with data protection law.

Key considerations include whether personal data is used for model training, where processing occurs, and whether anonymisation is effective. Providers should support Data Protection Impact Assessments; reluctance to do so may signal risk.

Whilst AI offers benefits, transparency and accountability remain essential to safeguard personal data.

JISC has published many guidance documents on the use of AI, and organisational policy and procedure in this area: for more information [this is a good place to start](#).



Other News

[Civil liberties groups call for inquiry into UK data protection watchdog](#)

[HMRC 'function creep' means spying on your travel plans to block benefits](#)

[European Commission accused of 'massive rollback' of digital protections](#)

[ICO Fine LastPass £1.2m](#)

[Children's online privacy in mobile games under spotlight](#)

Council Attacks

Several London councils have been [hit by cyber-attacks](#), disrupting shared IT systems and phone lines. Kensington & Chelsea and Westminster City Councils confirmed they were responding to an incident and working with the National Cyber Security Centre and cyber specialists to restore services.

Emergency plans were activated to maintain critical operations, and residents were warned of potential delays. Hammersmith & Fulham Council reported a "serious cyber security incident" linked to the same issue, urging staff to avoid links from affected councils. The Metropolitan Police's Cyber Crime Unit is investigating, with enquiries at an early stage and no arrests made.

Hackney Council, which suffered a major breach in 2020, raised its threat level to "critical" and warned staff against phishing attempts, though it has not been directly targeted. The Information Commissioner's Office has been notified.

Mayor Sadiq Khan said City Hall is working to improve councils' cyber resilience amid growing threats.

System security is a mainstay of data protection, and organisations should always remain alert in this regard.

Contact: dpo@hefestis.ac.uk
www.hefestis.ac.uk
Images: [Pixabay](#)