Data Protection News
from HEFESTIS Ltd

August 2025

| Data Protection | FOI | Cybersecurity | Unidesk |

Inside: Rollout of the DUAA| Recording & Transcribing Meetings |
Live Facial Recognition Technology| Apple Encryption Battle

Hallucination Consternation

A UK taxpayer, Marc Gunnarsson, was criticised by a judge for relying on an AI chatbot that fabricated (or 'hallucinated') legal precedents in a failed appeal against His Majesty's Revenue and Customs (HMRC).

Gunnarsson, representing himself at the Upper Tribunal, used AI to draft his submissions, which included three fictitious tribunal decisions. HMRC identified the false cases in his skeleton argument, prompting Judge Rupert Jones to caution against unverified reliance on AI-generated legal content. While Gunnarsson was not deemed "highly culpable" due to his lack of legal training, the judge warned that such conduct could be taken seriously in future cases.

Gunnarsson had received £12,918 in coronavirus self-employment support payments, believing himself eligible despite earning income as a company director. Although the First Tier Tribunal initially upheld his claim, HMRC successfully appealed, and the Upper Tribunal ruled the payments recoverable.

This is not an isolated case and reflects broader concerns about AI use in legal proceedings and beyond. Previously, barrister Sarah Forey was reprimanded for citing fictitious cases in the High Court; and another litigant, Bodrul Zzaman, had his AI-assisted defence dismissed in a child benefit dispute. Judges in both cases emphasised the risks of relying on AI without human verification, highlighting the potential for inaccurate or fabricated legal arguments.

HEFESTIS staff have recently undergone specialist training on various aspects of AI: the mechanics, ethics, data protection, regulatory frameworks, and best practice governance in this area.

The benefits of this training will filter through to clients as consideration is given to advise on appropriate checks and balances in this sphere.

Phased Rollout of the Data (Use and Access) Act 2025 (DUAA)

On July 25, 2025, the UK government announced a phased rollout of the Data (Use and Access) Act 2025 (DUAA), which received Royal Assent on June 19, 2025.

The implementation will occur in four stages.

Stage 1, beginning August 20, 2025, introduces technical clarifications to the legal framework, new statutory objectives for the Information Commissioner's Office (ICO), and mandates government reporting on copyright and AI impacts.

Stage 2, expected 3–4 months post-Royal Assent, will activate provisions on digital verification services and data retention by internet providers in cases involving the death of a child.

Stage 3, around six months after Royal Assent, will bring changes to UK data protection law and introduce new standards for health and adult social care data in England.

Stage 4, scheduled for early 2026, involves enforcement-related provisions requiring new technologies or staffing, including ICO restructuring, digitised birth and death registration, and measures relating to the National Underground Register.

HEFESTIS will continue to monitor the progress of the legislation, and will update as changes come into force.

Recording & Transcribing Meetings Using AI

DP Network has explored the growing use of AI-enabled tools for recording and transcribing meetings, highlighting both their benefits and associated privacy risks. While such tools offer convenience, accessibility, and potentially improved documentation, organisations must exercise caution.

Key concerns include unauthorised use, automatic activation, lack of participant consent, and potential inaccuracies in AI-generated transcripts.

It is essential to have human oversight, data minimisation, and clear retention policies. Organisations must also be cautious about indiscriminate sharing of sensitive content, and be aware that use of such tools may increase the volume of data subject access requests, and will be in scope for any FOISA requests.

For sensitive meetings, recording may be acceptable if all parties agree, but stricter controls are essential. A Data Protection Impact Assessment (DPIA) is strongly recommended to address risks. Organisations should also establish internal guidelines, enforce access controls, and update procedures to reflect the inclusion of recordings and transcripts in privacy notices.

This is an area where AI may perform well, but use of innovative tools must be balanced with responsible data governance.

If you need help to undertake a DPIA, you can contact your DPO who can advise. James Nock has recently given a presentation on this topic at Cyberweek Scotland, and if you'd like further details, please contact James at jnock@hefestis.ac.uk

Live Facial Recognition Technology

The UK's Equality and Human Rights Commission (EHRC) has declared the Metropolitan Police's use of live facial recognition technology (LFRT) incompatible with European human rights law.

As the Met plans to deploy LFRT at the upcoming Notting Hill Carnival, the EHRC warns that the technology lacks sufficient safeguards and poses risks to privacy, freedom of expression, and freedom of assembly.

LFRT scans faces in real-time via CCTV and matches them against police watchlists, triggering alerts for officers to engage. EHRC Chief John Kirkpatrick emphasised that biometric data is deeply personal and must be protected by clear, proportionate legal frameworks.

The EHRC has been granted permission to intervene in a judicial review of the Met's use of LFRT, prompted by a case involving Shaun Thompson, a black British man wrongly identified and detained.

Backed by Big Brother Watch, Thompson alleges mistreatment and racial bias. Despite calls from civil liberty and anti-racism groups to halt LFRT use, Met Commissioner Sir Mark Rowley defended its deployment, citing public safety.

The EHRC's intervention marks a significant challenge to the legality and ethics of LFRT in policing, raising broader concerns about surveillance, discrimination, and democratic freedoms.

As the technology becomes more mainstream and affordable, organisations may be tempted to use it for their own security purposes. HEFESTIS advice is to await further guidance / legislation in this area. In the meantime, any deployment of LFRT must fully consider both data protection and human rights issues.

Other News

Age checks for online safety – what you need to know as a user
AI Mining, Big Tech and Copyright
ICO launches consultations on guidance regarding UK Data (Use and Access) Act 2025
Privacy International alerts regulator about the use of algorithms by the UK Government and their impact on migrants
Dozens more UK Afghan data breaches uncovered

Apple Encryption Battle

In a significant reversal, the UK government has dropped its demand for Apple to provide access to encrypted iCloud data, following pressure from the U.S. government and privacy advocates.

The original request, issued via a Technical Capability Notice under the Investigatory Powers Act, would have required Apple to hand over user data upon legal warrant. Apple noted that obtaining data 'via the backdoor' would undermine its ADP feature, and responded by disabling ADP for new UK users and challenging the Notice legally

U.S. Director of National Intelligence Tulsi Gabbard confirmed the UK's retreat, citing concerns over American citizens' privacy and civil liberties.

The UK Home Office declined to confirm the Notice but emphasized ongoing security cooperation with the U.S.

Experts warned that such 'backdoors' could compromise global user security and be exploited by criminals. It remains unclear whether Apple will reinstate ADP in the UK, which will be a matter of concern for UK Apple device users.

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

Data Protection News
from HEFESTIS Ltd

September 2025

| Data Protection | FOI | Cybersecurity | Unidesk |

Inside: SAR Obstruction| Offboarding |DUAA Update| AI Compliance Accuracy

Mandatory ID Cards on the horizon

Prime Minister Sir Keir Starmer has announced that digital ID will become mandatory for individuals seeking employment in the UK, as part of a broader strategy to combat illegal migration.

Speaking at the Global Progressive Action Conference in London, Starmer argued that the scheme would strengthen border security and reduce exploitation of foreign labour, while offering practical benefits to citizens.

The digital ID, expected to be stored on smartphones, will include personal details such as name, date of birth, nationality or residency status, and a photo. It will be required to prove the right to work by the end of the current Parliament, anticipated by 2029. A public consultation on implementation will begin later this year, with legislation to follow in early 2026.

Opposition parties criticised the move. Reform UK labelled it a continuation of Conservative immigration policies, while the Liberal Democrats and SNP condemned it as bureaucratic and intrusive. Northern Ireland's First Minister Michelle O'Neill described the proposal as a threat to the Good Friday Agreement.

Despite existing checks for employers, the government believes a unified digital ID system will reduce document fraud and streamline access to services such as tax records, childcare, and welfare. Starmer emphasised that the scheme would not require individuals to carry ID or present it on demand.

The announcement comes amid rising pressure on the government, with over 50,000 migrants arriving via small boats since Labour took office.

Organisations will need to consider data protection implications if data from such ID documents are copied or stored, though it looks unlikely that they will be introduced till 2028/29 at the earliest.

SAR data: don't interfere

On 3 September 2025, Jason Blake, director of Bridlington Lodge Care Home in Yorkshire, was fined £1,100 and ordered to pay £5,440 in costs after being found guilty of obstructing a data subject access request (DSAR).

The case marks a rare criminal prosecution under Section 173 of the Data Protection Act 2018, which criminalises deliberate data concealment to prevent disclosure.

In April 2023, a woman with lasting power of attorney requested personal data concerning her father, including incident reports and CCTV footage. Blake refused to comply and subsequently deleted or concealed records between 12 April and 12 May 2023. The Information Commissioner's Office (ICO) investigated and found no justification for the refusal.

Unlike typical DSAR breaches, which result in organisational reprimands or civil penalties, Section 173 imposes personal criminal liability. The ICO has increased enforcement activity, with recent reprimands issued to Glasgow and Edinburgh councils for DSAR backlogs.

The case serves as a warning to directors and senior managers: deliberate obstruction of DSARs can result in prosecution. Organisations are urged to implement robust DSAR procedures, train staff, and maintain clear records. Blake's conviction highlights the serious consequences of non-compliance, including criminal records and reputational damage.

Check that your organisations polices are adhered to and contact your DPO if you have any queries about compliance.

Offboarding

Cybersecurity professionals are calling for improved offboarding practices after a series of insider incidents, including a former Intel engineer who stole confidential documents before joining Microsoft. Varun Gupta, who left Intel in 2020, copied sensitive files including pricing strategies and was later fined over $34,000 and sentenced to probation.

Experts warn that poor offboarding procedures leave organisations vulnerable, especially when access to systems isn't revoked promptly. Josh Kirkwood of CyberArk and Damian Garcia of IT Governance stressed the need for swift action and cross-departmental collaboration between HR, IT, and security teams.

Recent cases, such as a dismissed employee deleting 180 virtual servers and another sabotaging Eaton Corp's network, highlight the risks. Garcia emphasised that technical staff with deep system access pose particular threats if offboarding is delayed.

Solutions include automated identity lifecycle management and behavioural analytics tools to detect anomalies, alongside zero-trust and least-privilege access models.

Organisations should consider a revision of policy and procedure in this area, particularly regarding immediate tasks to be implemented when an employee moves on.

Data (Use and Access) Act 2025

Some of the contents of the Data (Use and Access) Act 2025 (DUAA) have started to appear via commencement regulations.

The second commencement regulations under the Data (Use and Access) Act 2025 (SI 2025/982) bring section 124 of the Act into force. These regulations came into effect on 5 September 2025.

Section 124 relates to provisions concerning the retention of information by internet service providers in connection with investigations into the death of a child.

The third set of commencement regulations under the Data (Use and Access) Act 2025 (SI 2025/996) bring into force key provisions of the Act that amend the Data Protection Act 2018.

Effective Immediately:

Section 79 introduces a legal professional privilege exemption, limiting data subject rights where disclosure would breach legal privilege.

Section 88 establishes a national security exemption, allowing restrictions on data rights where necessary for national security.

Effective from 17 November 2025:

Section 89 enables joint processing of data between intelligence services and competent authorities.

Section 90 provides consequential amendments related to joint processing.

There's nothing too earth shattering here for clients, but HEFESTIS will continue to monitor and report as further sections come into effect.

legislation.gov.uk

Other News

ICO consultation on draft changes to data protection complaints
PSNI 'cannot afford' to pay staff compensation over major data breach
Government faces questions after review of 11 major UK data breaches
Government unable to calculate Afghan data breach cost
Students an increasing source of cyber threat in UK schools

AI Accuracy

Microsoft has introduced new AI-powered Copilot features in Excel, designed to streamline tasks such as formula generation, text summarisation, and product description creation using natural language prompts. The new 'COPILOT' function integrates with existing Excel formulas, including LAMBDA and SWITCH, and is available for Windows and Mac users in a pilot phase.

However, the company has issued a caution, advising users not to rely on the tool for tasks requiring precision or legal, regulatory, or compliance accuracy. A support page explicitly warns against using AI-generated outputs for financial reporting or legal documentation, stressing the importance of reviewing and validating results before making critical decisions.

Microsoft also addressed data privacy concerns, assuring users that input data is not used to train its AI models and remains confidential. While the feature promises to reduce spreadsheet workload, experts urge caution due to potential inaccuracies in AI-generated content.

With MS urging caution when using the new features, the handy AI tool looks unlikely to replace your DPO, CISO or lawyer any time soon.

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