



---

| Data Protection | FOI | Cybersecurity | Unidesk |

Inside: Updated IDT Guidance | Your Party Launch | Updated Right of Access Guidance  
| Human Anatomy of a Breach

## Password Manager Provider Fined £1.2m for Data Breach

**The Information Commissioner's Office (ICO) has fined password manager provider LastPass UK Ltd £1.2m [for a 2022 data breach that exposed the personal data](#) of up to 1.6 million UK users.**

The incident stemmed from two linked security failures in August 2022. First, a hacker accessed a corporate laptop belonging to a European-based employee. The attacker then compromised a US-based employee's personal laptop by installing malware and capturing their master password.

Using information obtained from both breaches, the hacker infiltrated LastPass's backup database and extracted customer data including names, email addresses, phone numbers and stored website URLs.

The penalty is the seventh GDPR-related fine issued by the ICO in 2025, all involving cyber security lapses.

Other significant fines last year included a £14m penalty issued to Capita after a cyber-attack compromised the personal data of 6.6 million people, as well as fines against Advanced Computer Software Group Ltd (an NHS IT supplier), DPP Law Ltd, and US genetic testing firm 23andMe.

The ICO has urged organisations to strengthen internal security practices and ensure policies explicitly address data breach risks. It emphasised the importance of restricting access where risks are identified and improving security awareness among staff.

The ICO highlighted resources available on its website, including employer checklists for home-working security and guidance on measures to consider for different remote working options.

Organisations should be confident that their security policies and measures are adequate, and that data sharing and processing agreements are in place where required.

# Updated International Data Transfer Guidance

The Information Commissioner's Office (ICO) has issued [updated guidance on international data transfers](#), introducing a clearer three-step test to determine when an organisation is making a "restricted transfer" under the UK GDPR.

The aim is to help organisations understand when they must apply adequacy regulations, use appropriate safeguards or rely on an exception.

The guidance emphasises that a transfer includes both sending personal data abroad and allowing overseas organisations remote access, but does not include mere transit of data through another country. Transfers into the UK are also excluded.

The new three-step test asks whether the UK GDPR applies to the processing, whether the organisation is initiating a transfer to a location outside the UK, and whether the recipient is a separate legal entity. If all three conditions are met, the transfer is restricted.

The ICO provides clarification on when controllers and processors initiate transfers, noting that the key factor is who designs and instructs the transfer architecture. Processors in the UK transferring data back to their non-UK controllers are not considered to be making restricted transfers—although this differs from the EU GDPR approach.

The guidance includes examples to help organisations navigate complex data flows, with further materials promised.

If you need advice about restricted data transfers, speak to your DPO.



# Your Party Launch May be 'Criminal Matter'

The [Information Commissioner's Office \(ICO\)](#) has advised that the unauthorised launch of a Your Party membership portal promoted by MP Zarah Sultana may have involved "serious criminal activity" and should be referred to the police. The controversy began in September 2025, when an email was sent to about 800,000 people on the party's mailing list urging them to purchase £55 memberships. Shortly afterwards, Sultana publicly unveiled the portal on X, describing it as "safe and secure".

Jeremy Corbyn's Peace and Justice Project (PJP), the party's data controller, quickly disowned the portal as "unauthorised", warned supporters not to use it and sought legal advice. After reviewing the referral, the ICO concluded that formal regulatory involvement was not required but said the PJP should consider reporting the matter to Report Fraud and the police, noting that any potential criminal investigation would take precedence.

Sultana later stated that the ICO had "dropped the case", though the watchdog emphasised this should not be interpreted as a conclusion on whether criminal activity occurred.

Organisations should ensure appropriate oversight of new projects or changes to processing of personal data to avoid potential unlawful activity.

## Updated Right of Access Guidance

The Information Commissioner's Office (ICO) has issued refreshed guidance on Subject Access Requests (SARs), reflecting amendments introduced by the Data (Use and Access) Act 2025 (DUAA).

While the overall framework of individuals' right of access remains unchanged, the ICO has clarified several practical areas, including search obligations, response time limits and when organisations may pause deadlines.

Under the updated guidance, organisations must conduct "reasonable and proportionate" searches to locate personal data, but are not required to undertake searches deemed excessive relative to the importance of providing access. A new clarification confirms that the volume of information to be examined can be considered when determining proportionality. Organisations must still justify why a search would be unreasonable.

On time limits, the response period now begins only when a request, any necessary identity verification, and — where applicable — a fee for manifestly unfounded or excessive requests, have all been received. ID checks must be requested promptly.

The ICO has also restated its position on "stopping the clock": the response deadline may be paused only when clarification about the scope of the request is genuinely required, and organisations must document their reasoning.

Now would be a good time for organisations to review policy and procedure in this area, and issue new local guidance accordingly.



### Other News

[Ofcom launches investigation into X over Grok sexualised imagery](#)

[Cyber Bill and the implications for UK business](#)

[Legality of filming in public for social media content](#)

[UK Gov Software Security Code of Practice](#)

[ICO to investigate Prospect data breach with counterparts](#)

[European Commission Renews UK Data Adequacy Decisions](#)

## Human Anatomy of a Breach

A Finnish woman whose psychotherapy records were stolen in one of the country's biggest-ever data breaches [has spoken about the lasting personal impact](#) of the breach. In 2020, 33,000 patients of Vastaamo, a private therapy provider, were blackmailed after a hacker accessed and leaked highly sensitive clinical notes. Victims were threatened with the publication of their personal data unless they paid a ransom in bitcoin.

Meri-Tuuli Auer said the exposure of her confidential discussions triggered severe anxiety, leaving her unable to leave home and fearful of being recognised. Although she discovered her files had already been released online, she later obtained her full records and was distressed by how her therapist had described her.

Police identified known cybercriminal Julius Kivimäki as a suspect. He was convicted and sentenced to more than six years in prison, though he continues to deny responsibility.

Auer has since publicly shared her experience and written a book about her experience.

Data breaches can have devastating outcomes for the individuals and groups concerned, and this story highlights the need for vigilance and strong security at all times. ICO Resources: [Click Here](#).

Contact: [dpo@hefestis.ac.uk](mailto:dpo@hefestis.ac.uk)  
[www.hefestis.ac.uk](http://www.hefestis.ac.uk)  
Images: [pixabay.com](http://pixabay.com)



---

| Data Protection | FOI | Cybersecurity | Unidesk |

Inside: Social Work & AI | Substack Breach | Record Fine For Reddit | Unlawful Deletion Prosecution

## Data Protection Complaints

The UK Information Commissioner's Office (ICO) [has issued new guidance](#) in regard to statutory obligations requiring all UK organisations to implement a formal process for handling data protection complaints by 19 June 2026, following changes introduced under the Data (Use and Access) Act.

The legislation obliges organisations to provide a clear mechanism through which individuals can raise data protection complaints. This must include acknowledging each complaint within 30 days, responding without undue delay, making any appropriate enquiries, and updating complainants on progress. An outcome must be provided without undue delay.

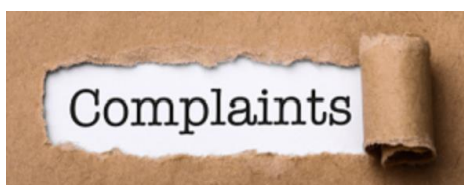
A data protection complaint is defined by the guidance as any expression of dissatisfaction relating to the handling of personal information. Examples include concerns about data breaches, subject access responses, data retention periods, data accuracy, information security measures, or profiling practices. The ICO notes that, historically, individuals have often approached the regulator directly; however, under the new regime, the ICO will usually require individuals to raise the complaint with the organisation first.

The guidance also clarifies what does *not* constitute a data protection complaint. Matters such as general service complaints, employment grievances, or dissatisfaction with processing timelines should not automatically be categorised as data protection complaints when these issues accompany the exercise of a statutory right. Organisations unsure of a request's nature are encouraged to seek clarification.

It is important to have visible, accessible complaints processes. The new requirement ensures that organisations address concerns early and transparently, reducing premature escalation to the ICO and strengthening public trust in data-handling practices.

In Scotland, organisations may have to consider two regulators: ICO (for data protection issues) and SPSO (for complaints issues). Charities may also have to consider Office of the Scottish Charity Regulator (OSCR) regulations in this regard.

If you need further support with what a Data Protection Complaints Policy would look like, please contact your DPO.



## Social Work & AI

There [is growing concern](#) over the increasing use of AI transcription tools within social work practice. As contemporary AI-driven systems become more widely adopted, some are worried about the fallibility of such systems.

The scrutiny arises from evidence that AI tools may introduce transcription errors, distortions, or omissions into official social care records, potentially affecting assessments, decision-making, and the safety of vulnerable individuals. Sector research, including recent studies by the Ada Lovelace Institute, has identified risks such as hallucinations, bias, and inconsistent performance across different accents and communication styles.

These inaccuracies can lead to misleading or harmful interpretations of service users' statements, particularly where frontline staff rely on AI-generated outputs to relieve significant workload pressures.

These concerns sit within a broader context of rapid technological deployment across local authorities. Whilst AI transcription tools promise efficiency gains and reduced administrative burdens, the emerging evidence underscores a need for rigorous evaluation, clearer governance, and stronger safeguards.

Without robust oversight, these tools risk undermining trust in social work processes and the integrity of care records.

If you have concerns about the use of AI within your own organisation, speak to your DPO who can help with input about policy and risk assessment.

$$2 + 2 = 5$$

## Substack Breach

Substack (an online publishing platform) [has confirmed a significant data breach](#) in which an unauthorised third party accessed user information in October 2025.

The intrusion went undetected for approximately five months before discovery in February 2026, prompting widespread concern about Substack's security oversight. Exposed data included email addresses, phone numbers and internal metadata; however, no financial information, credit card details or passwords were affected.

Substack CEO Chris Best issued an apology to affected users, acknowledging that email addresses had been shared without permission and expressing regret for the lapse in data protection.

He confirmed that Substack has fixed the vulnerability and launched a full investigation into the incident. Despite assurances, questions remain regarding the scale of the breach and the company's delay in detecting it.

The breach raises broader concerns about platform security and user trust, particularly given Substack's role in handling large volumes of subscriber data.

Organisations should be robust with their cyber security activities, and mindful that there are statutory timescales for breach reporting.

## Record Fine For Reddit

Reddit [has been fined £14.47m](#) by the UK Information Commissioner's Office (ICO) after investigators found the platform unlawfully collected and used the personal data of children under 13.

The ICO concluded that Reddit failed to implement any meaningful age-assurance mechanism before July 2025, despite its own terms prohibiting under-13s from using the service. As a result, significant numbers of children are believed to have accessed the platform, with their data processed without a lawful basis and potentially exposing them to harmful or inappropriate content.

The regulator also found that Reddit had not carried out a required Data Protection Impact Assessment before January 2025, meaning risks to children were neither identified nor mitigated. Following the investigation, Reddit introduced age-verification and self-declaration measures, though the ICO criticised the latter as insufficient because it is easily bypassed.

Information Commissioner John Edwards said the failures represented a serious breach of duty, stressing that children's data had been used in ways they could not understand or control. Reddit has indicated it will appeal, arguing that mandatory collection of more personal information conflicts with its privacy-focused approach.

Organisations should be aware that ICO has a hard line approach to the misuse of children's data, or of opaque practices when dealing with children. This is reflected in the content of ICO's [Age Appropriate Design Code](#), which Reddit has fallen foul of.



### Other News

[UK privacy watchdog opens inquiry into X over Grok AI sexual deepfakes](#)

[A single compromised account gave hackers access to 1.2 million French banking records](#)

[Unlawful cookies: a new avenue for the ICO to issue fines?](#)  
[Imgur owner MediaLab fined over children's privacy failures](#)

[UK GDPR and PECR – key DUAA reforms take effect](#)

[China 'hacked the mobile phones of senior officials in Downing Street for years'](#)

## Unlawful Deletion

A [former council Chief Executive was prosecuted](#) under Section 77 of the Freedom of Information Act 2000.

Section 77 (England, Wales, NI) makes it a criminal offence for any person to act with the intention of preventing the disclosure of information requested under the FOI regime. The offence may be committed through actions such as destroying, altering, or concealing records to frustrate an FOI request.

Such prosecutions are relatively rare, reflecting the evidential difficulty of proving deliberate intent to obstruct disclosure. However, the prosecution highlights the significance of the case within the wider context of information governance, and reinforces the statutory obligations placed upon public authorities and their senior officers.

It also underscores the broader importance of accountability and transparency in public administration, particularly where information rights legislation is intended to ensure openness in government and public operations.

Unless organisations have a valid exemption, the expectation is that information should be released. It should certainly never be deleted for the purposes of avoiding disclosure.

Contact: [dpo@hefestis.ac.uk](mailto:dpo@hefestis.ac.uk)  
[www.hefestis.ac.uk](http://www.hefestis.ac.uk)  
Images: [pixabay.com](http://pixabay.com)





---

| Data Protection | FOI | Cybersecurity | Unidesk |

Inside: SIC v ScotGov | Voters' Data | CCTV Faux Pas | Monzo Shaming Shame

## Data Use and Access Act 2025 Guidance

The ICO [has issued updated guidance](#) to support organisations implementing changes under the Data Use and Access Act (DUAA).

A key development is the introduction of a new UK GDPR lawful basis, recognised legitimate interest, which allows pre-approved uses of personal data in the public interest, without the need for a balancing test.

These include responding to emergencies, preventing or detecting crime, safeguarding vulnerable individuals, protecting national or public security, and responding to public task disclosure requests. The DUAA also clarifies that direct marketing, intra-group administrative data sharing, and network security measures may fall under the existing legitimate interests basis.

The ICO has updated both its brief and detailed guidance on legitimate interests to reflect these changes. Organisations already relying on legitimate interests for activities now covered by recognised conditions will not need to amend their practices. However, organisations must still be able to show that the processing is necessary and proportionate for the specific condition relied upon and that it aligns with broader UK GDPR requirements.

Revisions to the purpose limitation guidance explain how to assess whether a new processing purpose is compatible with the original one, alongside separate guidance on when personal data can be reused for different purposes.

Draft guidance has also been published for organisations involved in research, archiving, and statistics, with the ICO inviting feedback. The consultation remains open until 27 April 2026.

The guidance also includes a reminder of the upcoming changes to complaints handling. “By 19 June 2026, organisations must have a clear and accessible process for handling data protection complaints. A complaint can come from anyone who believes their personal information has been handled in a way that infringes data protection law and so having the right procedures in place is essential.”



# Scottish Information Commissioner v Scottish Government

**The Scottish Government [faces the prospect](#) of renewed legal action after the Scottish Information Commissioner, David Hamilton, said he no longer trusts ministers to manage key documents related to an ethics inquiry involving Nicola Sturgeon.**

Hamilton condemned what he described as “preposterous and unacceptable” excuses for repeated failures to comply with orders to release material linked to the 2021 investigation, that cleared Sturgeon of breaching the ministerial code in relation to the handling of harassment complaints against Alex Salmond.

Ministers have missed multiple deadlines to publish correspondence and legal advice, prompting Hamilton to consider “more intrusive options” to ensure compliance. He also expressed concern over what he characterised as unusual delays and poor case-handling, contrasting sharply with the government’s usual approach to freedom of information (FOI) requests.

Permanent Secretary, Joe Griffin insisted that the government had acted with integrity, denied any withholding of information and attributing recent issues (including the temporary removal of a large document bundle) to the scale and complexity of releasing more than 700 files. First Minister, John Swinney has previously said redactions were necessary to protect the anonymity of women who made allegations against Salmond.

The FOI dispute stems from a long-running battle over transparency dating back to 2021, and highlights the potential difficulties when considering the use of exemptions, when there is a high level of public interest present. The HEFESTIS FOI Team are always happy to advise on FOI requests, and the use of exemptions where appropriate.



## Voters’ Data

Wales [has moved to end the sale](#) of voters’ personal data to commercial organisations under new regulations coming into force later this year. The Representation of the People (Removal of the Edited Register) (Wales) Regulations 2026 will abolish the open register from 1 October, following May’s Senedd elections. The change is expected to offer greater protection to young people and vulnerable groups by preventing their details being accessed for direct marketing or other commercial purposes.

The reform also enables the next phase of Welsh electoral modernisation. Under the Elections and Elected Bodies (Wales) Act 2024, automatic voter registration cannot be introduced until the open register is removed. Automatic registration, already piloted in four Welsh local authorities, aims to boost participation and reduce the administrative burden on individuals.

Separately, the Senedd has approved updates to local government election rules ahead of the 2027 polls, including exempting safety-related spending from campaign finance limits—a reform recommended by the Jo Cox Foundation.

Cabinet Secretary, Jayne Bryant said the move strengthens voter protection and marks Wales as the first part of the UK to introduce such safeguards, paving the way for a fairer and more accessible electoral system.

It will be interesting to see if other UK parliaments will follow suit.



## CCTV Faux Pas

The [Austrian Data Protection Authority \(DSB\)](#) investigated a sole proprietor running a flower shop after the operator installed three surveillance cameras: one covering the sales area, one monitoring the checkout, and one recording the public pavement outside.

The outdoor camera captured passers-by, and all footage was retained for 72 hours with live access available via a mobile phone app.

The controller also extracted two images from the system and posted them on social media, identifying an alleged thief and asking for public assistance. The post, which contained criminal data, was later removed.

The DSB found multiple GDPR infringements. It ruled that the outdoor camera breached the principles of data minimisation and lawful processing under Articles 5(1)(a) and (c) and 6(1)(f), as recording uninvolved passers-by was unnecessary.

Publishing the images constituted unlawful further processing of criminal data under Article 10, with no legal basis and without informing the data subject as required under Article 13(3). The authority stressed that any reuse of personal data requires a compatibility assessment, and while protecting property may justify identifying a suspect, public posting was not proportionate.

The controller also failed transparency duties under Article 13. The DSB imposed a €1,500 fine, plus €150 in costs, and ordered the cessation of unlawful processing.

In plain terms, this flags the importance of considering where your cameras are pointed, and how footage should be used (or not used) after an incident.



### Other News

[Police Scotland fined £66k for extracting and sharing mobile phone data](#)

[Meta's 'consent or pay' data grab in Europe faces new complaints](#)

[UK regulator examines IT glitch that enabled bank customers to see others' accounts on app](#)

[Clubs complain to X about 'sickening' Grok posts](#)

[MPs urge UK government to halt contract giving Palantir FCA data access](#)

## Monzo Shaming Shame

[Monzo is facing criticism](#) over the tone of its annual "Year in Monzo" spending reviews after a customer complained that the bank used "shaming" language based on her financial data. Fiona Taylor, 42, said the digital bank generated "humiliating behavioural commentary", including comments about her reliance on fast food and high spending on Just Eat, which she found distressing due to her chronic fatigue and past eating disorder.

Modelled on services such as Spotify Wrapped, the review aims to provide a light-hearted summary of customers' spending habits. However, some users have said the feature feels judgmental, with online forums showing mixed reactions. Taylor argued that Monzo could not understand the personal circumstances behind her spending and that its remarks amounted to inappropriate moral commentary and potential misuse of data.

Monzo apologised but maintained the content is automatically generated and optional. After the bank rejected her complaint, Taylor escalated the matter to the Financial Ombudsman Service, where a senior ombudsman is now reviewing the case.

The lessons are clear here in terms of purpose limitation, fair use of data, and the effect of such processing on the data subject.

Contact: [dpo@hefestis.ac.uk](mailto:dpo@hefestis.ac.uk)  
[www.hefestis.ac.uk](http://www.hefestis.ac.uk)  
Images: [pixabay.com](http://pixabay.com)