



## UK GDPR Info for Education since the New DUAA Data Usage and Access Act (June 2025)

**Donna Flynn** – Schools Lead Data Protection Consultant

**Jo Puckering** – Learning Technology Consultant & GDPR Practitioner

Email: [dpo@theictservice.org.uk](mailto:dpo@theictservice.org.uk)  
Website: [www.theictservice.org.uk](http://www.theictservice.org.uk)  
Telephone support: 0300 300 0000 option 4

# Intro

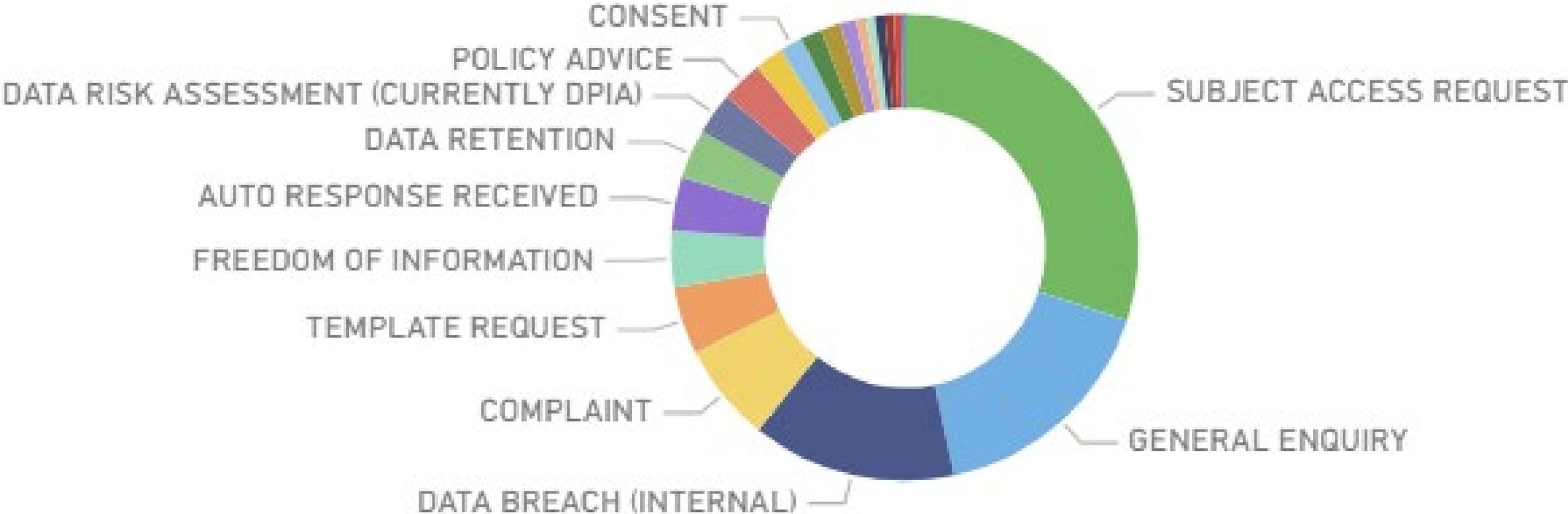
- Today we aim ensure that you are aware of the changes in legislation and how this affects us all in the education sector.

# Agenda

- **Trends across the past year** and how we can ensure we're moving forward
- **DUAA** what's new and how does this impact us
- **'Reasonable and Proportionate'** when it comes to Subject Access Requests
- **'Making things clearer'** improvements in the way the law is written and structured
- **'Greater Focus'** on children and online services
- **'Introduction of an electronic complaints'** form for schools.

# Trends across the past year

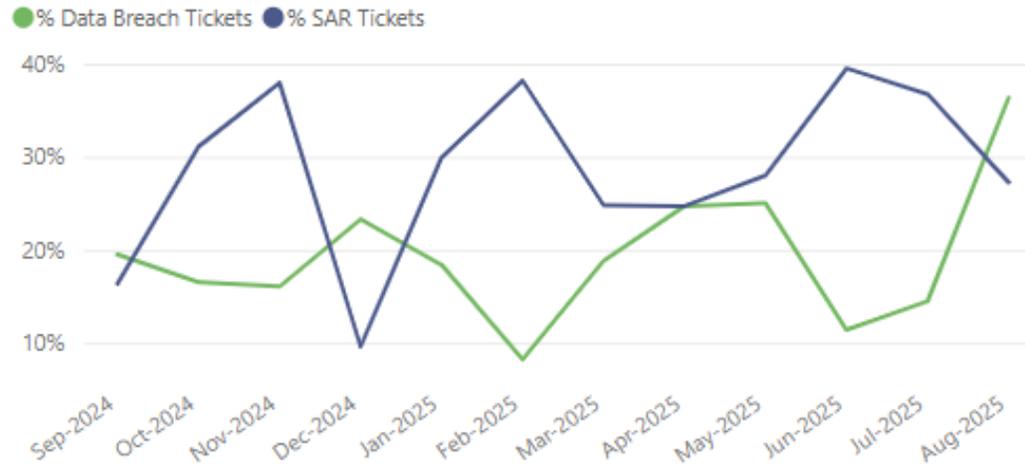
28/08/2024 – 27/08/2025 = Total DPO Tickets = 1535



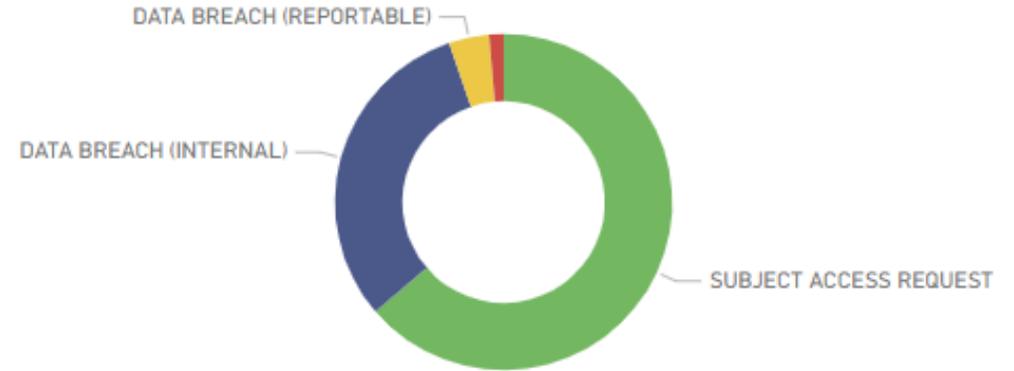
# Trends across the past year

Of 1535 | 17.3% (263) = Data Breaches, 30% (462) = Subject Access Requests

% Data Breach Tickets and % SAR Tickets by MonthYear



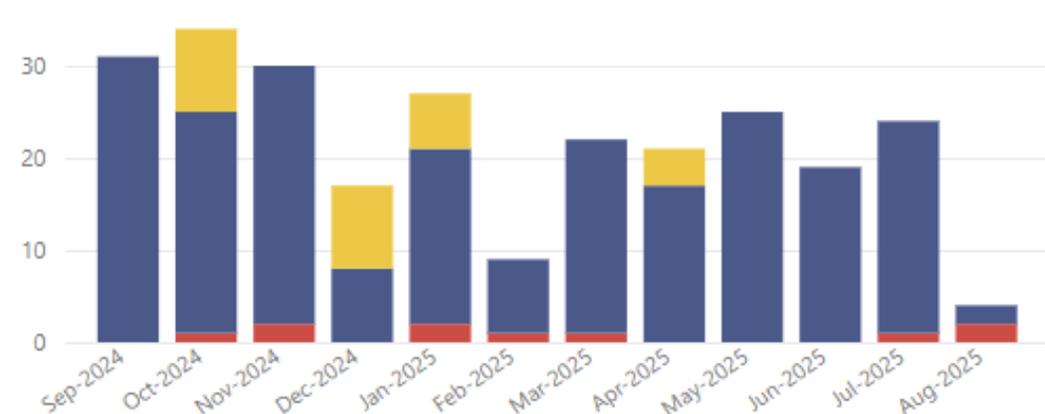
Tickets by ServiceSubType\_UPPER



SAR Tickets by MonthYear



Data Breach Tickets by Month/Year and Service SubType



# Data Usage and Access Act (DUAA) Royal Assent - June 19<sup>th</sup> 2025

## What's new and how does this impact us:

- Although introduced June 2025, key sources (GOV.UK and the ICO) identify that this will take between 2 and 12 months to come into full effect following Royal Assent.
- There are some significant updates which will affect the Private Sector.
- There are updates to the current 'Articles' associated with the UK GDPR legislation; this will result in a requirement to review and update key documentation to ensure continued compliance.
- It is important to note, that none of the recommendations forecast in the previous release of this associated Bill have been brought forward.

# Data Usage and Access Act (DUAA) Royal Assent - June 19<sup>th</sup> 2025

## Why has it been introduced (ICO guidance)

- The DUAA is a new Act of Parliament that updates some laws about digital information matters.
- It changes data protection laws in order to promote innovation and economic growth and **make things easier for organisations, whilst it still protects people and their rights.**
- Most of the changes **offer you an opportunity to do things differently, rather than needing you to make specific changes to comply with the law.**
- The changes will be phased in between June 2025 and June 2026.

# Data Usage and Access Act (DUAA) Royal Assent - June 19<sup>th</sup> 2025

## Are there any new requirements for you to meet?

- **Children and online services:** if you provide an online service that is likely to be used by children, the DUAA explicitly requires you to take their needs into account when you decide how to use their personal information. You should already satisfy this requirement if you conform to our Age appropriate design code (AADC).
- **Data protection complaints:** if you don't already do so, the DUAA requires you to take steps to help people who want to make complaints about how you use their personal information, **such as providing an electronic complaints form**. You also have to acknowledge complaints within 30 days and respond to them 'without undue delay'.

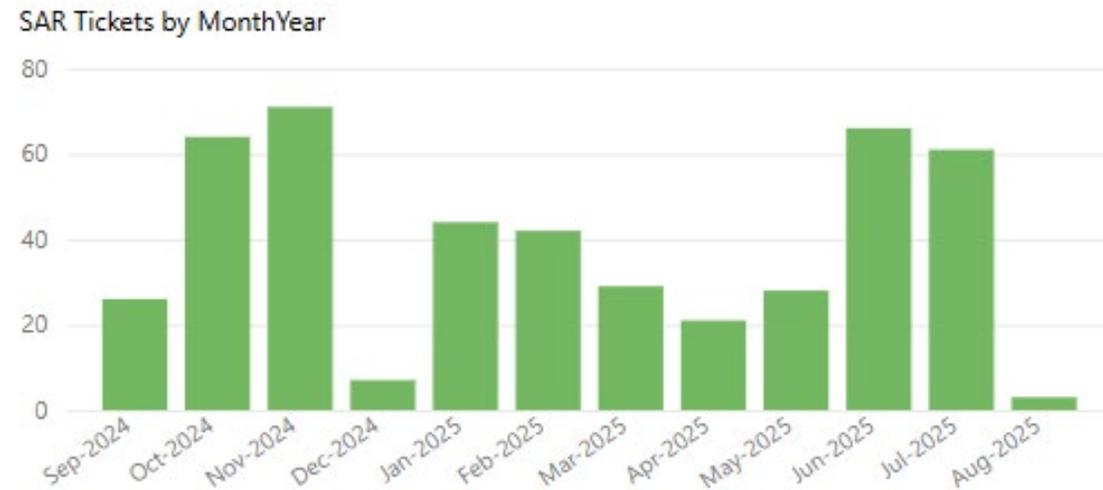
# 'Reasonable and Proportionate' when it comes to Subject Access Requests

**Title:** Data subjects' rights

## Description of measure:

These measures clarify rules around subject access requests for organisations and individuals.

They make provisions on time limits to respond to data subject requests; and codify existing case law around reasonable and proportionate searches.



# ‘Reasonable and Proportionate’ when it comes to Subject Access Requests

Does this make a difference to you: **Yes**

**How is this different from previous legislation:**

Previously, the one-month deadline to respond to a Subject Access Request (SAR) started as soon as the request was received, regardless of whether data controllers had all the information they needed to take the required action.

***The Act introduces a “stop the clock” provision which will allow organisations to pause the response time – without the risk of missing the deadline – if they need data subjects to clarify or refine their requests or to provide more information.*** Once the organisation has the information they need, the response time continues.

In addition, ***the previous law did not explicitly state that searches needed to be “reasonable and proportionate”, although this has been established by case law.***

# 'Reasonable and Proportionate' when it comes to Subject Access Requests

## What action can you do to enforce this:

- As part of your subscription to the ICT Service DPO support, you can download a 'Subject Access Request Form Template'.

Thereafter the timescales of the 'calendar month' will not resume until this paperwork has been received by your school. [A guide to subject access | ICO](#)

- **A reasonable and proportionate search**, will also support schools with the more ambiguous requests they receive.

There will be data that simply doesn't fall into this remit!

The ICO website wording references these updates, however, we believe that there will be greater clarity provided over the next few months. We'll of course let you know when this is finalised.

Your DPO Resource Hub offers easy access to a comprehensive suite of resources specifically developed to support schools and educational institutions in meeting UK GDPR and Freedom of Information (FOI) obligations.

Our materials are structured into themed documents and templates, each serving a distinct compliance or operational purpose. Designed for you to adapt to meet your own branding, they offer a structured approach to data governance, transparency, and accountability, with clear links to ICO guidance and legal obligation, helping you to meet statutory and best practice requirements.



## Select the category headings for a list of all resources

The file will automatically download to your device for you to file as needed

Policy Templates   Privacy Notices   **Subject Access Requests**   Data Breaches  
Complaints

Tools and templates for managing SARs, including response workflows and evidence logs

- Record of Subject Access Requests - August 2025.docx
- Subject Access Request: Form Template - Version 2 August 2025.docx**
- Subject Access Requests: Useful Guidance.docx

## Your Main UK GDPR Practitioners



Lead Schools Data Protection Consultant, Advanced GDPR Practitioner, Advanced NVQ Accredited Adult Learning and Development, MIS Consultant and School Governor



UK GDPR Practitioner, Apple Teacher, Microsoft Innovative Educator Expert, Trainer and Learning Technology Consultant



**The Ripple Effect**

One admin error – a data breach – is all it takes for someone to lose their job.

01:40

*Imagine a person who has recently escaped an abusive relationship, only to have their confidential address exposed due to a data breach. Or think about someone living with HIV whose medical information is accidentally disclosed. These are not rare or exaggerated scenarios – they are real, and they happen. Such breaches can lead to*

# ‘Making things clearer’ improvements in the way the law is written and structured

**Title:** Purpose Limitation

## **Description of measure**

Under the UK GDPR, the purpose limitation principle ensures that an individual’s personal data is re-used only in ways that they might reasonably expect.

This measure clarifies the circumstances in which “further processing” or data re-use is compatible with the original purpose, **including when personal data is being re-used for a very different purpose from which it was originally collected. For example, when a company may wish to disclose personal data for crime prevention.** The measure also clarifies the position when there is a change of controller and the requirement for an Article 6(1) lawful ground to be satisfied for all further processing or data re-use.

# 'Making things clearer' improvements in the way the law is written and structured

**Does this make a difference to you:** Yes

**How is this different from previous legislation?**

Previously, the legislation on personal data re-use was difficult for controllers and individuals to navigate, particularly as it was not clear about certain specific public interest circumstances in which further processing would be permitted.

**These measures rectify this.**

**Which provision(s) in the UK GDPR and/or the DPA 2018 are changing?**

Section 71 of the DUAA amends Articles 5 and 6 of the UK GDPR and inserts new Article 8A into the UK GDPR.

This will ultimately require updates to your associated policies and privacy notices.

# ‘Making things clearer’ improvements in the way the law is written and structured

**Title:** Lawfulness of Processing

## **Description of measure**

This measure creates a new lawful ground for processing personal data under Article 6 of the UK GDPR. It is designed to give non-public bodies greater confidence about processing personal data for a limited number of **“recognised legitimate interests”**.

These include processing that is necessary for crime prevention, safeguarding vulnerable people, responding to emergencies, safeguarding national security or assisting other bodies deliver public interest tasks that are sanctioned by law.

# ‘Making things clearer’ improvements in the way the law is written and structured

**Does this make a difference to you:** This should reinforce any misunderstandings around ‘legitimate interests’

## How is it different from previous legislation?

Previously, most organisations would have relied on the “legitimate interests” lawful ground in Article 6(1)(f) UK GDPR to process personal data for such purposes. That ground requires organisations to undertake a “legitimate interests assessment” before the processing begins.

While the requirement for the processing to be necessary remains, the need for a **detailed legitimate interests assessment which balances the data controller’s interest against the individual’s interest has been removed.** This is in recognition of the societal value of the processing in specified situations and the potential negative impacts of any delay.

This will ultimately require updates to your associated policies and privacy notices.

# 'Greater Focus' on children and online services

**Title:** Data protection by design: children's higher protection matters

## **Description of measure**

This measure introduces **a new duty for information society services that are likely to be accessed by children**, building on existing obligations under Article 25 of the UK GDPR. It requires these services to take account of the "children's higher protection matters" specified in the new Article 25(1B) of the UK GDPR when designing processing activities carried out when providing services to children.

**These matters include how best to protect and support children when using the service; the fact that children may be less aware of the risks and consequences associated with the processing of their personal data; and the fact that children have different needs at different ages and different stages of development.**

# 'Greater Focus' on children and online services

**Does this make a difference to you: Yes**

**How is this different from previous legislation?**

Article 25 of the UK GDPR already requires data controllers to implement appropriate technical and organisational measures to ensure data protection by design and by default. This requires consideration of varying risks for rights and freedoms of individuals but does not expressly refer to children's needs.

**This measure changes this by adding a new explicit duty for information society services likely to be accessed by children to take account of children's needs when designing their services.**

**Which provision(s) in the UK GDPR and/or the DPA 2018 are changing?**

Section 81 of the DUAA amends Article 25 of the UK GDPR.

# ‘Greater Focus’ on children and online services

## What action do you need to take:

When introducing a new organisation / company to provide data processing linked to children, or looking to introduce a new online learning platform that your children are going to access, you will need to ensure that they are compliant with the latest legislation around “**higher protection matters**” (linked to the Age appropriate design code – AADC).

You may need to consider completing a Data Protection Impact Assessment (DPIA) or if you are happy that the data processor of your online platform has met all the required commitments linked to the new guidance, then you can simply add their details to your school’s Information Asset Register (IAR).

# 'Greater Focus' on children and online services

## What action do you need to take:

**DPIA:** DPIAs are an essential part of your accountability obligations. Conducting a DPIA is a **legal requirement for any type of processing**, including certain specified types of processing that are likely to result in a **high risk to the rights and freedoms of individuals**. Under UK GDPR, failure to carry out a DPIA when required may leave you open to enforcement action, including a fine of up to £8.7 million, or 2% global annual turnover if higher.

By considering the risks related to your intended processing before you begin, you also support compliance with another general obligation under UK GDPR: data protection by design and default.

# 'Greater Focus' on children and online services

## What action do you need to take:

**IAR:** You have an asset register that records assets, systems and applications used for processing or storing personal data across the organisation.

### Ways to meet our expectations (ICO Website):

Your organisation has an asset register which holds details of all information assets (software and hardware) including:

- asset owners;
- asset location;
- retention periods; and
- security measures deployed.

You review the register periodically to make sure it remains up to date and accurate.

You periodically risk-assess assets within the register and you have physical checks to make sure that the hardware asset inventory remains accurate.

# 'Greater Focus' on children and online services

## What action do you need to take:

- Prevent the 'silent data breaches' of inputting personal data into AI tools;
- Ensure clarity for what users can and can't do, with clear boundaries;
- Provide and ensure the use of approved tools **only**;
- Risk assess and log the decisions from the reviews in IAR and DPIAs;
- Give transparency for any use of AI publishing a statement on your website;
- Increase awareness across all stakeholders of
  - How AI work, to better understand the implications;
  - Potential Bias and limitations particularly in reference to automated decision making;
- Support innovation while protecting rights, especially those of children and vulnerable groups.
- Align with KCSiE and Safeguarding regulations including monitoring use;
- Ensure there is always a 'human' factor in any use of Generative AI Content.

# Additional 'new' guidance

**Guidance for organisations on how to handle data protection complaints following the requirements introduced by the Data (Use and Access) Act.**

**Stage:** **Drafting**

**Public consultation:** **Yes (due to launch August 2025)**

**Final version of guidance due for publication:** **Winter 2025/2026**

(current guidance available here: [Dealing with complaints | ICO](#))

# 'Introduction of an electronic complaints' form for schools.

## Requirements:

- to help people who want to make complaints about how you use their personal information
- To acknowledge within 30 days
- To respond to the complaints 'without due delay'

The ICT Service Data Protection Consultancy Team have provided you with this

**Microsoft DUAA Complaint Form Template**

Please feel free to duplicate and adopt for your own needs.

# Other updates to be aware of

## **Title:** **Meaning of research and statistical purposes**

**Description:** This measure makes it clearer when you can use personal data for scientific research, and statistical purposes.

## **Title:** **Processing reliance on relevant international law**

**Description:** This measure clarifies that under the UK GDPR, data controllers can process personal data on grounds of public interest under Article 6(1)(e) and Article 9(2)(g) UK GDPR where the basis of such processing is set out in relevant international law.

## **Title:** **Automated decision making [UK GDPR]**

**Description:** This measure facilitates the responsible use of automation to help grow the economy and enable a modern digital government. With stringent safeguards in place, it creates a more permissive framework for making decisions based solely on automated processing that have legal or similarly significant effects for individuals.

**There are many additional updates, however, most are irrelevant to those of us working in the public sector**

# Other updates to be aware of

- **Fines under PECR have increased:** From £500,000 to align with GDPR's maximum limits of £17.5 million, or 4% of total worldwide annual turnover.
- **Cookie Rules:** The DUAA revises cookie regulations, making cookie banner, and other tracking technology requirements more flexible in certain contexts.
- **International Data Transfers:** The DUAA introduces the concept of the "Data Protection Test", which must be applied by the Government when determining adequacy of a particular country. This test takes a lot of the current guidance and case law on international data transfers and sets it out in law.
- **Privacy Notice Changes:** Which do not affect subscribers to our DPO service as the templates we provide include the recommended / suggested updates.

# Concerns raised

- This year, the Data Protection Consultancy Team only received only a handful of DPIA's
- Based upon this past year's annual audit process, many school's we support do not have an 'up to date' and 'working' IAR.
- Some schools who subscribe to the DPO service have never completed an annual audit, despite signing up to the service for several years.
- Many of the calls logged by the Team are in response to reactive requests / incidents, and rarely of a proactive nature.
- There may be schools who currently subscribe and are not lawfully compliant!
- Please support our team in our efforts of 'helping' you: The ICO **do** audit schools and Trusts for compliance [Audits and overview reports | ICO](#)

# Updated Accountability Tracker

## **New resource available for schools to download and evidence compliance:**

- Leadership and oversight
- Policies and procedures
- Training awareness
- Information rights
- Transparency
- ROPA and lawful basis
- Contracts and data sharing
- Risks and DPIAs
- Records management and retention
- Breach response and monitoring.

[Tracker template | ICO](#)

# Upcoming Data Protection Related Workshops

- **Record Management and Data Retention**
- **Fundamental Awareness and Skills**
- **Subject Access Requests and Consent**
- **Consent and Legitimate Interest**
- **Copyright - wrong**
- **The audit process – what your DPO expects**
- **Data Breaches, when it goes wrong and how best to avoid them**
- **Data Protection Impact Assessments (DPIAS) and the Information Asset Register (IAR)**

For more details and dates see our content at

<https://theictservice.org.uk/course-category/uk-gdpr-and-data-protection-courses>

Not seeing what you need or are interested in? [Let us know on our Form](#)

# Any Questions



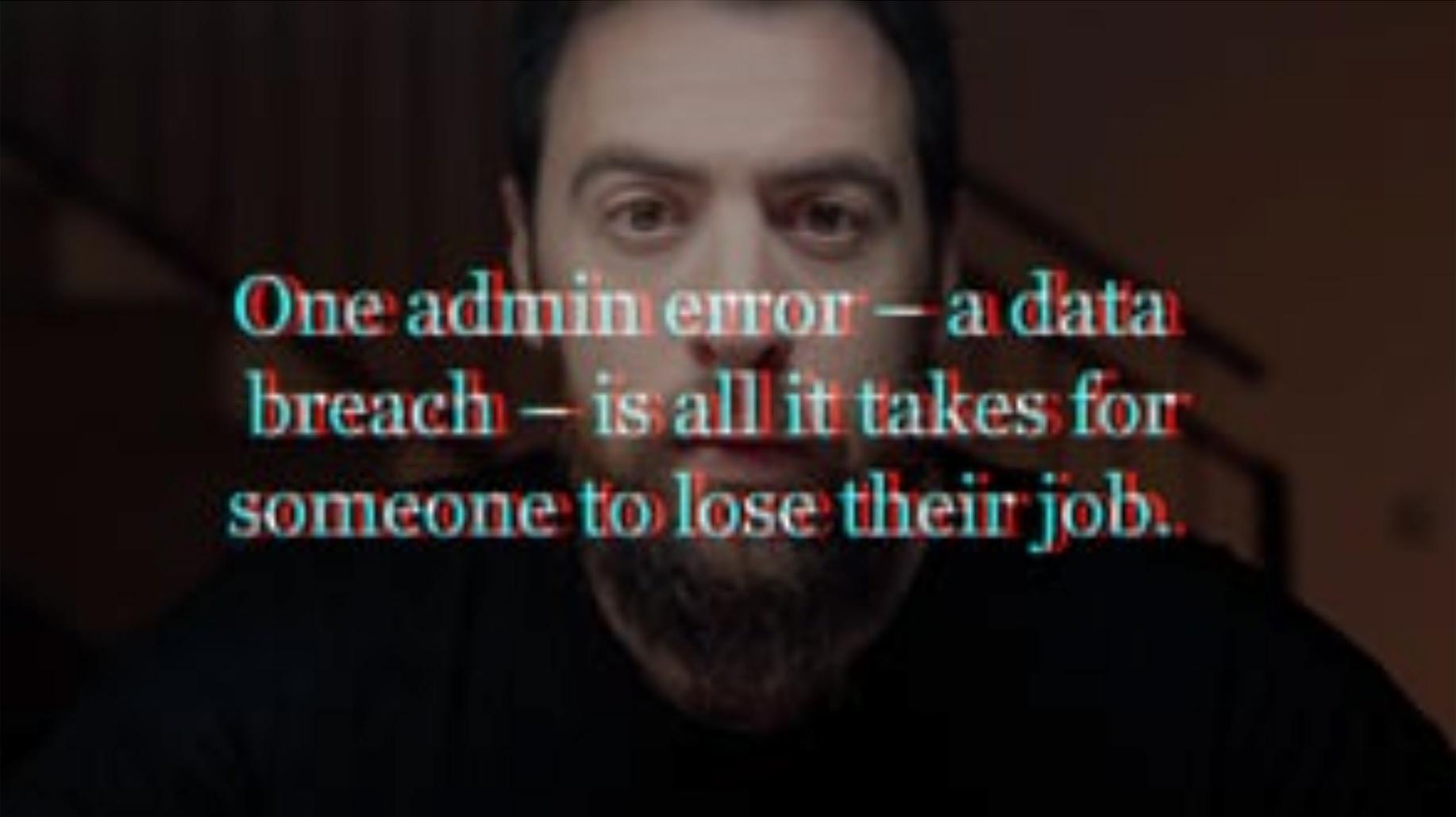
Email: [dpo@theictservice.org.uk](mailto:dpo@theictservice.org.uk)

Website: [www.theictservice.org.uk](http://www.theictservice.org.uk)

Telephone support: 0300 300 0000 option 4



Why is  
GDPR  
Awareness  
Important?



One admin error – a data breach – is all it takes for someone to lose their job.