4I's Consulting

Latest GDPR & Data Protection Updates (2025–2026)

GDPR is a law that protects people's personal data and gives them more control over how organisations use it.

Recent legislation and regulatory guidance have reshaped how organisations apply it in practice. Here's what schools, charities and membership organisations need to know.

What counts as personal data

Anything that can identify someone - like their name, email, address, photos, IP address, or notes about them.

What organisations must do

- Collect only the data they genuinely need
- Be clear about why they're collecting it
- Keep it secure
- Delete it when it's no longer needed
- Let people see, correct or delete their data if they ask

What people have the right to

- To know what data is held about them
- To ask for a copy
- To correct mistakes
- To have data deleted in some cases
- To opt out of certain uses, like marketing
- To move their data to another provider

What happens if organisations get it wrong

They can face complaints, investigations, reputational damage and, in serious cases, large fines.

Key Changes at a Glance

- **Automated decision-making rules updated** Organisations can use automated tools more flexibly but must still tell individuals when a significant automated decision is made about them and offer a route for human review.
- **Subject Access Requests (SARs) simplified** Processes are being streamlined, but the core right of access remains. Organisations still need clear workflows and timely responses.

- **Stronger expectations for children's data** Services likely to be used by children must show enhanced safeguards, age-appropriate explanations and minimal data collection.
- **Cookies and tracking under tougher scrutiny** Some low-risk analytics cookies may be exempt from consent, but enforcement has tightened. PECR fines now align with UK GDPR levels, making cookie compliance a genuine risk area.
- **Recognised Legitimate Interests introduced** Certain activities (e.g., safeguarding, crime prevention) may no longer require a full balancing test when relying on legitimate interests.
- **Higher standards for proving consent** Organisations must be able to demonstrate consent clearly - including retrieving call recordings where consent was given by phone.
- **International data transfers clarified** Updates refine how organisations assess and document overseas transfers, while the UK GDPR framework remains in place.

What this means for your organisation

These updates make compliance more practical but also raise expectations. In particular:

- Review cookie banners, analytics tools and third-party tracking.
- Ensure any AI-driven processes include human oversight.
- Strengthen consent capture and retrieval processes.
- Revisit safeguarding and children's data policies.

What to Do Next: Your GDPR & Compliance Action Checklist

1. Review your data processes

- Map what personal data you collect and why
- Check you're only collecting what you genuinely need
- Update privacy notices if anything has changed

2. Strengthen consent and record-keeping

- Make sure consent wording is clear and specific
- Confirm you can *prove* consent if asked (including call recordings)
- Refresh any old or ambiguous consent records

3. Tighten cookie and tracking compliance

- Audit all cookies, analytics tools and third-party scripts
- Update cookie banners and consent mechanisms
- Remove any tracking you can't justify or explain

4. Prepare for updated SAR expectations

- Review your Subject Access Request workflow
- Ensure you can locate, export and redact data efficiently
- Train staff on timelines and what counts as a valid request

5. Check any automated or AI-driven processes

- Identify where automated decision-making is used
- Add human oversight and clear challenge routes
- Update internal documentation to reflect new rules

6. Revisit children's data safeguards

- Ensure age-appropriate explanations and minimal data collection
- Review parental consent processes where relevant
- Check third-party tools used by children meet UK standards

7. Review international data transfers

- Confirm you have appropriate transfer mechanisms in place
- Update documentation and risk assessments
- Check vendor contracts reflect current requirements

8. Update staff training and internal guidance

- Refresh training on GDPR, PECR and data handling
- Highlight new expectations around cookies, consent and AI
- Make sure staff know how to escalate concerns