DPAS

DATA PRIVACY
ADVISORY SERVICE

DATA USE AND ACCESS ACT 2025: DETAILED PRACTITIONER GUIDANCE

DPAS DATA PRIVACY ADVISORY SERVICE

Disclaimer

This opinion is provided for general informational purposes only and reflects our interpretation and opinion on the **Data Use and Access Act 2025** as at the date of publication. It does not constitute legal advice and should not be relied upon as such. While we aim to provide accurate and current insights, the legislation and related guidance are subject to change. Organisations seeking advice on specific circumstances or compliance obligations should obtain **formal legal advice** from our team. At this time, we are unable to provide detailed responses to case-specific queries until further regulatory clarification is available.

INTRODUCTION

The Data Use and Access Act 2025 (DUA Act) is a significant legislative reform aimed at modernising the UK's data protection framework while retaining compatibility with existing laws like the UK GDPR and the Data Protection Act 2018 (DPA 2018). Rather than replacing these frameworks, the DUA Act introduces clarifications, procedural enhancements, and modernisation measures to reduce burdens on organisations, foster innovation, strengthen individual rights, and align data regulation with digital realities.

Practitioners must note that while some changes simplify compliance obligations, others significantly heighten enforcement risk—particularly in marketing, automated decision-making, and child protection.

INDICATIVE TIMELINES

Phase	Indicative Timing	Focus Areas
Phase 1 – Enabling Powers & Early Commencement	**June–Aug 2025**	Royal Assent (19 June 2025); powers for ministers and regulators to draft regulations; initial technical provisions commence.
Phase 2 – Secondary Legislation & Consultations	**Aug–Dec 2025**	Consultations on detailed rules for data access, verification, and privacy amendments; soft opt-in expansion for charities; ICO guidance issued.
Phase 3 – Core Regime Activation	**Dec 2025 – Early 2026**	Key parts of the Act (smart data schemes, digital verification, ICO governance changes) come into force via Commencement Regulations.
Phase 4 – Full Implementation & Regulatory Embedding	**By June 2026**	All major provisions operational; full integration of new data access mechanisms and compliance standards; ongoing evaluation and guidance updates.

INDICATIVE TIMELINES – RISKS AND CAVEATS

- Because much of the DUAA's operation depends on **delegated / secondary legislation**, the actual timelines are **conditional** on when the government drafts, consults, finalises, and enacts those regulations.

- Delays are possible due to political, technical, or administrative constraints.

- Some commencement dates shown in government guidance are provisional.

- Some functions (e.g., changes to ICO governance or the establishment of a new board) depend on appointments or transitional arrangements and may lag behind legislative readiness.

A NEW COMPLAINTS PROCEDURE

LEGISLATIVE INTENTION

Strengthen transparency and trust by ensuring individuals have clear routes to raise and escalate data complaints.

WHAT IS CHANGING?

- Mandatory complaints-handling procedures for all controllers.
- Time-bound responses: acknowledgement within 7 days, resolution within 30 days.
- Reporting obligations for larger or regulated entities.

EXAMPLES

- Public Sector: NHS Trust launches a dedicated complaints web portal with automatic updates.
- Commercial: Bank integrates complaints handling into CRM with SLA tracking.
- Non-Profit: Charity integrates “Report a Data Concern” into donation workflow.

A NEW COMPLAINTS PROCEDURE

PRACTITIONERS ACTIONS

DATA COMPLAINTS POLICY

Draft a standalone Data Complaints policy for your organisation, and ensure all employees are aware.

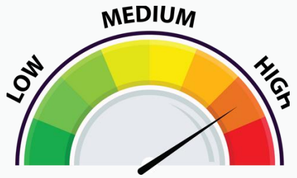
CASE LOGGING

Implement case-tracking tools to log complaints, timelines, and outcomes.

WORKFLOW MANAGEMENT

Design escalation workflows mirroring FOI or HR grievance procedures.

HIGHER FINES FOR MARKETING BREACHES



LEGISLATIVE INTENTION

Align Privacy and Electronic Communications Regulations (PECR) penalties with UK GDPR levels to deter unlawful marketing practices

WHAT IS CHANGING?

- Maximum fines rise to £17.5m or 4% global turnover.
- Enforcement scope widens to include unsent or blocked marketing messages.

EXAMPLES

- Public Sector: Council checks SMS campaign consent records.
- Commercial: Retailer restructures email workflows with automated opt-outs.
- Non-Profit: Fundraising charity adopts a double opt-in mechanism for new subscribers.

HIGHER FINES FOR MARKETING BREACHES

PRACTITIONERS ACTIONS

MARKETING COMPLIANCE AUDITS

Conduct marketing compliance audits: consent logs, suppression lists, cookie configurations.

COOKIE CONSENT

Review cookie consent mechanisms against ICO guidance.

LAWFUL BASIS

Document lawful basis for each marketing channel.

EASIER USE OF COOKIES

LEGISLATIVE INTENTION

Simplify low-risk analytics tracking while maintaining transparency.

WHAT IS CHANGING?

- Certain analytics and functional cookies may be set without prior consent if clear opt-outs exist.

EXAMPLES

- Public Sector: Council exempts session analytics cookies with opt-out notice.
- Commercial: Retailer exempts traffic measurement cookies from consent.
- Non-Profit: Charity differentiates essential cookies from marketing cookies.

EASIER USE OF COOKIES

PRACTITIONERS ACTIONS

AUDITS

Conduct cookie classification audits.

COOKIE BANNERS

Update cookie banners for opt-out compliance.

ICO GUIDANCE

Monitor ICO privacy-preserving advertising guidance.

RELAXED CONSENT REQUIREMENTS FOR CERTAIN COOKIES

The DUAA amends the Privacy and Electronic Communications Regulations (PECR) to remove the need for explicit user consent for specific types of non-essential or low-risk cookies. These include cookies used for:

- Statistical purposes (e.g., gathering usage data to improve services)
- Website appearance or performance
- Security and fraud detection
- Emergency assistance functions

The Information Commissioner's Office (ICO) may also relax enforcement for low-risk advertising cookies — such as those used for basic targeting—though consent is still required for more intrusive tracking. This is currently being consulted on and may lead to new guidance or secondary legislation.

TRANSPARENCY & OPT-OUT REQUIREMENTS

While some cookies are exempt from consent, organisations must still:

- Provide clear transparency about their use.
- Offer opt-out mechanisms, allowing users to refuse or disable these cookies.

STREAMLINING COOKIE RULES - SIMPLIFICATION

These reforms aim to simplify the regulatory landscape by making cookie rules more targeted and risk-based, eliminating the one-size-fits-all approach and easing compliance burdens for low-impact use cases.

SOFT OPT-IN FOR CHARITIES

LEGISLATIVE INTENTION

Enable simplified supporter communications where prior engagement exists.

WHAT IS CHANGING?

- PECR is being amended so that charities can use a soft opt-in exemption for direct electronic marketing (emails, texts, etc.).
- Charities can send marketing to existing supporters unless they opt out.

EXAMPLES

- Non-Profit: Charity sends appeals to previous donors under soft opt-in rules.

FURTHER INFORMATION

UNDER THIS SOFT OPT-IN FOR CHARITIES:

- The communication must be for the sole purpose of furthering charitable purposes.
- The contact details must be acquired when someone expresses an interest in the charity or provides support to further them (e.g. by donation, volunteering, etc).
- That the person must have been given a simple way to opt out at the time their details are collected, and each subsequent communication must also provide an opt-out.

? DOES IT ONLY APPLY TO “NEW” SUPPORTERS?

- It won’t apply retrospectively: you can’t automatically apply the soft opt-in exemption to people whose contact details you collected before the new rules take effect.
- It will apply for supporters recruited after the rules take effect (once the relevant secondary legislation is implemented).
- There might be limited cases where existing “active” supporters could qualify, depending on the nature of the relationship, how their data was collected, whether they were given opt-out choices at collection, etc.

KEY CAVEATS AND THINGS TO WATCH OUT FOR

THE “NEW SUPPORTER” IDEA ISN’T THE WHOLE STORY

- Even for new supporters, the exact point at which their data was collected matters.
- If they haven’t “expressed interest” or “offered support”, the soft opt-in won’t apply.
- Must ensure opt-out is offered at collection and in every message.
- Just because someone was active or supportive in the past doesn’t automatically mean they meet the “expression of interest/support under the required conditions” test.
- The legal basis of how their data was obtained matters for whether soft opt-in is valid.
- The soft opt-in is only available to organisations that are charities under the statutory definition. So non-profits not formally defined as charities can’t use it.

CONCLUSION

- Soft opt-in conditions are relevant to new supporters, but with some possibility that certain existing relationships/data might qualify, depending on how they were set up.
- It’s not a simple “only new supporters, no exceptions”, but it is heavily titled that was to avoid retrospective misuse.

INDICATIVE TIMELINE FOR SOFT OPT IN

Soft Opt-In Timeline (Charities under DUAA)

Milestone	Estimated / Commented Timing	Notes / Conditions
Royal Assent of DUAA	19 June 2025	The Act becomes law. GOV.UK +3
Passage of Section enabling soft opt-in (s. 114 PECR amendment)	June 2025 (with Act)	The soft opt-in "exemption" for charities is embedded in DUAA (amends PECR) in s. 114. GOV.UK +4
Commencement via secondary legislation	~ **December 2025** (estimated)	Legal commentary suggests the soft opt-in rule could come into effect around December 2025. Russell-Cooke
No retrospective application	Upon commencement	The soft opt-in cannot apply to contacts collected before the rule takes effect; only to supporters recruited after it's in force (though there is uncertainty regarding "existing active supporters" in limited circumstances). Mondaq +2
Preparatory / transitional period	mid-2025 to commencement	Charities are advised to prepare systems (recording preferences, review processes, opt-out options) before the rule is live. Fundraising Regulator +4

SUMMARY TABLE

CHANGE	DETAILS
Consent exemptions	No consent needed for statistical, performance, security, fraud-related, or emergency cookies.
Enforcement relaxations	ICO may ease enforcement for low-risk advertising cookies, under consultation.
Fines increased	PECR breaches now subject to fines up to £17.5 m or 4% of global turnover.
Stronger enforcement powers	ICO gains new powers for investigations and audits around cookie practices.
Transparency obligations	Must still inform users clearly and allow opt-outs—even for exempt cookies.

CHARITY SOFT OPT-IN CHECKLIST

- [ ] **Eligibility - Are they a registered UK charity? Do communications directly further charitable purposes (not commercial)?**
- [ ] **Collection of Details - Did contact come from supporter action (e.g. donation, volunteering, event sign-up)?. Were they told upfront that their details may be used for marketing?**
- [ ] **Opt-Out - Was clear opt-out offered at sign-up? Does every message include an easy unsubscribe?**
- [ ] **Timing & Scope - Was data collected after DUAA rules OR did original collection already meet opt-out/transparency standards? Are details only used for the same/similar charitable purposes?**
- [ ] **Records - Is there evidence of how/when details were obtained and if/when someone opted out?.**
- [ ] **Governance - Is the privacy notice up to date? Are staff/volunteers trained? Is supporter data regularly audited?**

DIGITAL ID SERVICES

LEGISLATIVE INTENTION

Enable secure, government-accredited digital identity verification to reduce fraud and streamline onboarding.

WHAT IS CHANGING?

- Creation of a legal framework for certified Digital ID providers.
- Digital ID may substitute physical verification for employment, tenancy, and financial services.

EXAMPLES

- Public Sector: Local authority replaces manual ID checks for housing benefits.
- Commercial: Challenger bank integrates Digital ID for account opening.
- Non-Profit: Refugee support charity uses Digital ID for beneficiary verification.

DIGITAL ID SERVICES

PRACTITIONERS ACTIONS

DPIAs

Perform DPIAs before onboarding any Digital ID solution.

PRIVACY NOTICES

Update Privacy Notices to reflect new data flows.

MONITOR

Monitor official lists of accredited providers.

DATA SUBJECT ACCESS REQUESTS (DSARS)

LEGISLATIVE INTENTION

Reduce disputes by clarifying timelines, exemptions, and pause rights.

WHAT IS CHANGING?

- Clock starts after ID verification.
- Clock pauses if further information is required from requester.
- Mandatory written reasons for refusals.

EXAMPLES

- Public Sector: NHS Trust pauses timelines awaiting data scope clarification.
- Commercial: Fintech tracks DSAR timeline pauses in its CRM.
- Non-Profit: Research charity creates refusal rationale templates for complex cases.

DATA SUBJECT ACCESS REQUESTS (DSARS)

PRACTITIONERS ACTIONS

DSAR TEMPLATES

Update DSAR templates with pause and refusal justifications.

AUDIT TRAILS

Maintain audit trails for requests, pauses, and refusals.

HANDLING EXEMPTIONS

Train staff on handling exemptions such as legal privilege.

RECOGNISED LEGITIMATE INTERESTS

LEGISLATIVE INTENTION

Simplify processing for low-risk, public interest activities without full balancing tests.

WHAT IS CHANGING?

- Certain purposes (e.g., fraud prevention, safeguarding, crime mapping) automatically exempt from legitimate-interest balancing tests.

EXAMPLES

- Public Sector: Police use crime data mapping without additional balancing tests.
- Commercial: Health provider uses fraud detection systems under recognised interests.
- Non-Profit: Charity analyses donor data to prevent financial abuse.

RECOGNISED LEGITIMATE INTERESTS

PRACTITIONERS ACTIONS

IDENTIFY

Identify processes now falling under recognised legitimate interests.

ROPA

Update Records of Processing Activities (ROPA) to reflect simplified grounds.

AUTOMATED DECISON MAKING (ADM)

LEGISLATIVE INTENTION

Balance AI innovation with human oversight and appeal rights.

WHAT IS CHANGING?

- Article 22 restrictions remain for special category data.
- All ADM systems require appeal and review mechanisms.

EXAMPLES

- Public Sector: Benefits authority introduces manual review for AI-driven eligibility rejections.
- Commercial: Credit firm allows human review of automated loan declines.
- Non-Profit: Youth support platform reviews AI-based referral prioritisation.

AUTOMATED DECISON MAKING (ADM)

PRACTITIONERS ACTIONS

ADM WORKFLOWS

Map all ADM workflows organisation-wide.

HUMAN-IN-THE-LOOP

Implement human-in-the-loop review steps for sensitive decisions.

PRIVACY NOTICES

Update Privacy Notices with ADM contestation rights.

DIGITAL SMART DATA SCHEMES

LEGISLATIVE INTENTION

Extend Open Banking principles to energy, telecoms, insurance, and healthcare.

WHAT IS CHANGING?

- Framework for sectoral Smart Data Schemes using standardised APIs.

EXAMPLES

- Public Sector: Local council shares energy usage data for social tariffs.
- Commercial: Insurtech startup integrates Smart Data APIs for risk scoring.
- Non-Profit: Health charity joins Smart Data Schemes for anonymised analytics.

DIGITAL SMART DATA SCHEMES

PRACTITIONERS ACTIONS

DATA SHARING AGREEMENTS

Prepare Data Sharing Agreements (DSAs) and API protocols.

DPIAS

Conduct DPIAs before onboarding into schemes.

MONITOR REGULATIONS

Monitor sector-specific regulations

RELAXED “RIGHT TO BE INFORMED”

LEGISLATIVE INTENTION

Allow indirect notice where direct notice is disproportionate or impossible.

WHAT IS CHANGING?

- Documented proportionality assessments replace direct notification obligations for mass datasets.

EXAMPLES

- Public Sector: Council publishes research notice rather than contacting millions of individuals.
- Commercial: Telecom operator publishes privacy notices for anonymised big data projects.
- Non-Profit: Heritage charity posts legacy data notices on website.

RELAXED “RIGHT TO BE INFORMED”

PRACTITIONERS ACTIONS

COMPLIANCE RECORDS

Maintain proportionality justifications in compliance records.

PRIVACY NOTICES

Publish privacy notices online for transparency.

DIRECT MARKETING & LEGITIMATE INTERESTS

LEGISLATIVE INTENTION

Clarify when legitimate interests suffice for direct marketing under GDPR vs PECR.

WHAT IS CHANGING?

- Legitimate interests acceptable unless PECR explicitly requires consent.

EXAMPLES

- Public Sector: Library service markets events via legitimate interests basis.
- Commercial: SaaS firm uses legitimate interests for newsletters but honours opt-outs.
- Non-Profit: Alumni office adopts legitimate interests for event invites with unsubscribe links.

DIRECT MARKETING & LEGITIMATE INTERESTS

PRACTITIONERS ACTIONS

MAP MARKETING CHANNELS

Map all marketing channels against GDPR vs PECR consent needs.

PRIVACY NOTICES

Update Privacy Notices with lawful bases for marketing.

SCIENTIFIC RESEARCH

LEGISLATIVE INTENTION

Encourage data reuse for commercial and non-commercial research with safeguards.

WHAT IS CHANGING?

- Definition of research now explicitly covers commercial R&D.
- Data reuse permitted under consent or strong safeguards (e.g., pseudonymisation).

EXAMPLES

- Public Sector: NHS reuses patient data for AI health studies.
- Commercial: Pharma firm reuses pseudonymised trial data for follow-up studies.
- Non-Profit: University charity uses anonymised datasets for secondary research.

SCIENTIFIC RESEARCH

PRACTITIONERS ACTIONS

TEMPLATES AND FORMS

Update research ethics templates and consent forms.

DATA MINIMISATION

Maintain data minimisation and anonymisation practices.

SOFT OPT-IN FOR CHARITIES

PRACTITIONERS ACTIONS

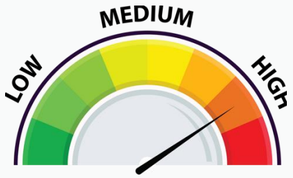
POLICIES

Review donor communications policies.

CLEAR OPT-OUT

Add clear opt-out links to all supporter messages.

PROTECTING CHILDREN ONLINE



LEGISLATIVE INTENTION

Enforce child-centric design and online protections under the Children's Code.

WHAT IS CHANGING?

- Child-accessible services must integrate age verification and data minimisation by design.

EXAMPLES

- Public Sector: Youth services site adopts strict age verification.
- Commercial: Gaming platform limits data profiling for under-16s.
- Non-Profit: Children's helpline anonymises user interactions by default.

PROTECTING CHILDREN ONLINE

PRACTITIONERS ACTIONS

REVIEWS

Conduct Children’s Code compliance reviews.

AGE GATES

Add age gates, parental consent, and child-friendly privacy notices.

COMPATIBLE PROCESSING

LEGISLATIVE INTENTION

Streamline secondary data use by designating pre-approved compatible purposes.

WHAT IS CHANGING?

- No fresh compatibility assessment for listed purposes like public health planning.

EXAMPLES

- Public Sector: Department reuses data for public health crisis planning.
- Commercial: Retailer analyses purchase data for trend insights.
- Non-Profit: Charity reuses anonymised data for grant applications.

COMPATIBLE PROCESSING

PRACTITIONERS ACTIONS

MONITOR LISTS

Monitor government lists of compatible uses.

ROPA

Document reuse in ROPA and privacy notices.

A NEW INFORMATION COMMISSION

LEGISLATIVE INTENTION

Transform the ICO into a CEO-led regulator for more responsive governance.

WHAT IS CHANGING?

- New Information Commission operational by 2027 with modern enforcement powers.

EXAMPLES

- Public Sector: Government department plans for new regulatory reporting templates.
- Commercial: DPOs track consultation outputs for policy updates.
- Non-Profit: Charities adapt governance for new audit requirements.

A NEW INFORMATION COMMISSION

PRACTITIONERS ACTIONS

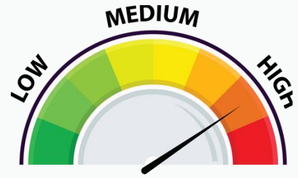
CODES OF PRACTICE

Monitor new Codes of Practice and regulatory consultations.

COMPLIANCE FRAMEWORKS

Update compliance frameworks to anticipate increased oversight.

PRACTITONER CHECKLISTS



HIGH RISK AREAS

IMMEDIATE ACTION REQUIRED

- Marketing fines: audit all campaigns, consent logs, suppression lists
- Automated Decision-Making: add human review, update privacy notices
- Child Protections: implement age verification, default privacy settings

PRACTITONER CHECKLISTS

MEDIUM-RISK AREAS

REVIEW AND IMPLEMENT

- DSAR timelines: add pause procedures, refusal justifications
- Digital ID & Smart Data schemes: conduct DPIAs, update onboarding workflows
- Direct marketing lawful bases: map GDPR vs PECR obligations
- Scientific research reuse: update consent templates, ethics approvals

PRACTITONER CHECKLISTS

LOW-RISK AREAS

MONITOR AND ADJUST

- Recognised legitimate interests: update ROPA entries
- Cookie exemptions: classify and label low-risk cookies
- Relaxed notification rules: document proportionality assessments
- Compatible processing purposes: track government updates
- Charity soft opt-ins: implement unsubscribe workflows

ANY QUESTIONS?

DPAS
DATA PRIVACY
ADVISORY SERVICE

GET IN TOUCH

info@dataprivacyadvisory.com

+44 20 3301 3384

www.dataprivacyadvisory.com

FOLLOW US

@dataprivacyadvisor

Data Privacy Advisory Service

DPAS®