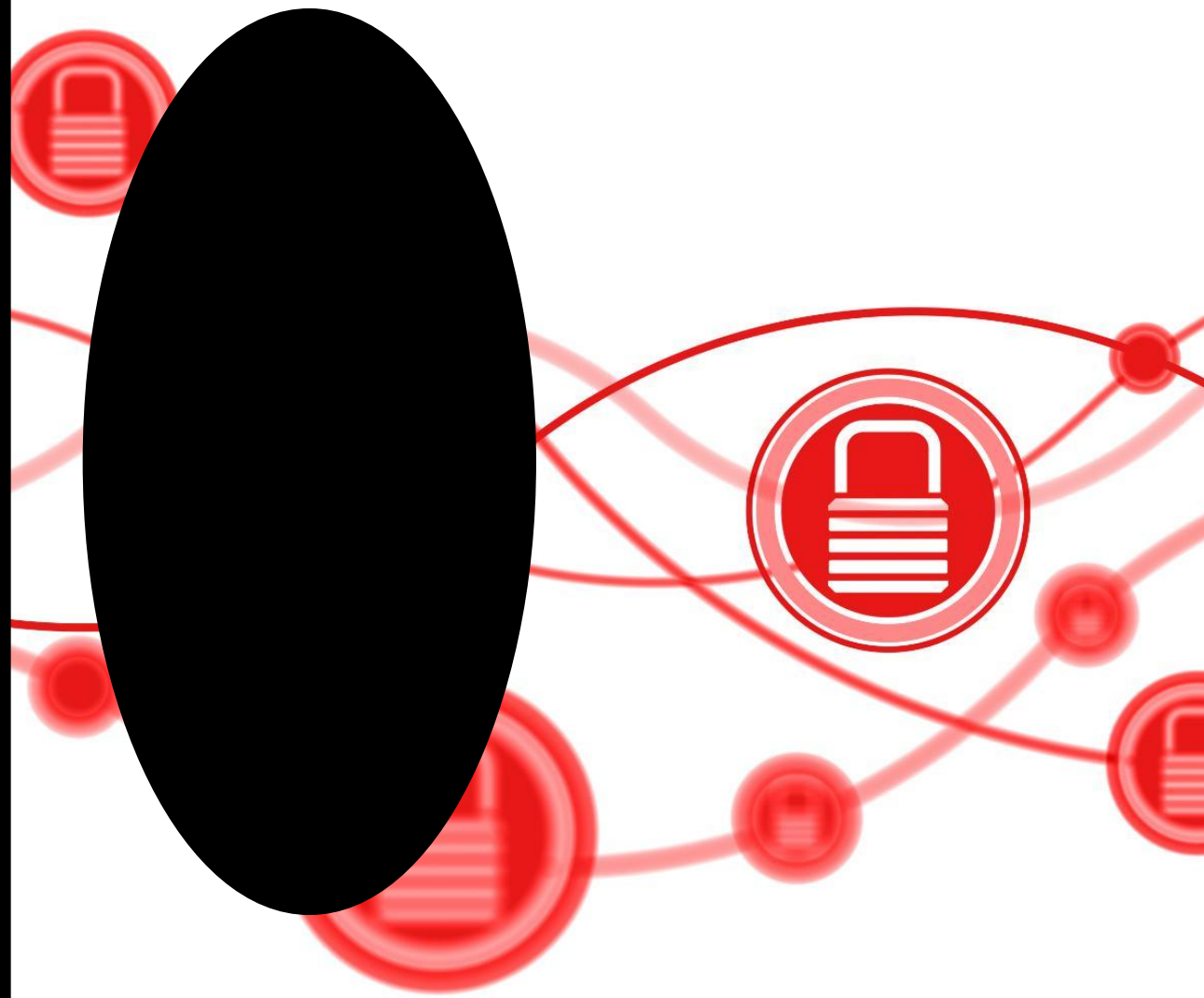
INTRODUCING THE DATA USE AND ACCESS ACT 2025 (DUAA) FOR LEGAL SERVICES

Enhancing legal data management and secure accessibility



INTRODUCTION TO DUAA

OVERVIEW OF DUAA

Purpose of DUAA

DUAA simplifies compliance and encourages responsible innovation while ensuring strong privacy protections in the UK.

Amendments to Existing Laws

DUAA updates UK GDPR, Data Protection Act 2018, and Privacy and Electronic Communications Regulations (PECR) to refine data protection frameworks without full overhaul.

Key Changes for Legal Professionals

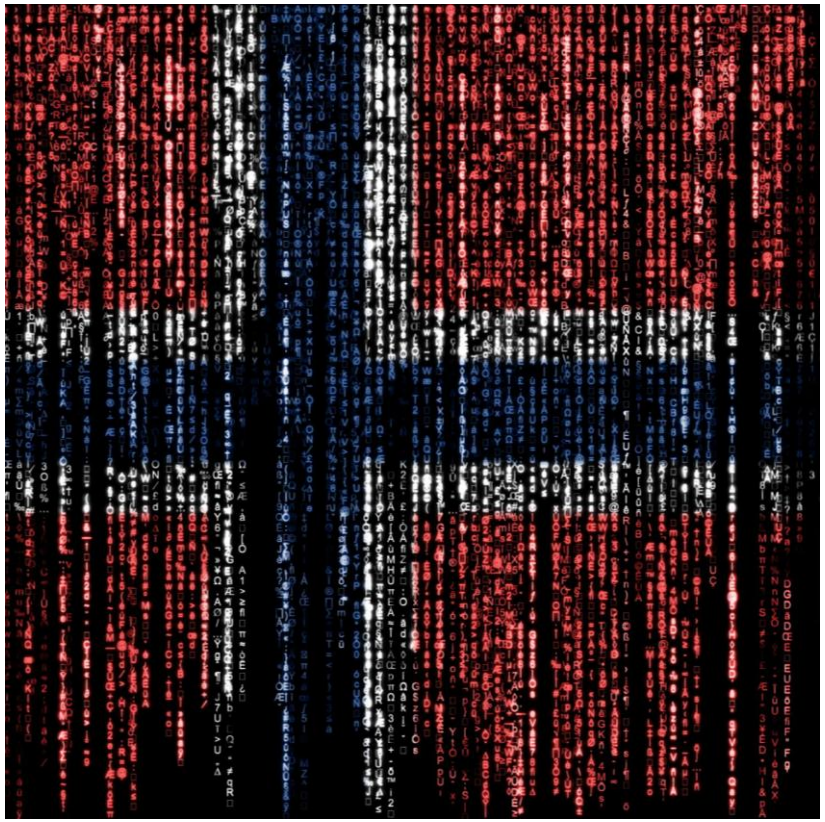
New lawful bases, modified access requests, and updated cookie and automated decision-making rules affect solicitors.

Importance of Early Preparation

Adapting early to DUAA is essential to avoid financial penalties and reputational risks in data compliance.

CONTEXT AND HISTORY

BACKGROUND AND LEGISLATIVE EVOLUTION



Foundations in UK GDPR

The DUAA builds on UK GDPR introduced in 2018 aligning with European data protection standards.

Post-Brexit Reforms

Post-Brexit, UK reforms aim to reduce complexity while maintaining EU adequacy for economic growth.

Modernization and Digital Transformation

DUAA modernizes data governance, balancing innovation with privacy rights across sectors.

Legal Implications for Firms

Understanding DUAA's evolution helps legal firms align with emerging compliance and regulatory trends.

KEY CHANGES COMPARED TO GDPR

MAJOR AMENDMENTS INTRODUCED BY DUAA

Recognised Legitimate Interests

DUAA establishes recognised legitimate interests as a lawful basis for specific processing without balancing tests.

Revised SAR Procedures

Subject Access Requests now allow reasonable and proportionate searches instead of exhaustive reviews.

Relaxed Cookie Consent

Cookie consent requirements are relaxed for non-intrusive analytics, while maintaining transparency obligations.

Expanded Automated Decision-Making

DUAA broadens automated decision-making scope with safeguards and mandatory human review mechanisms.

IMPLICATIONS FOR LEGAL FIRMS

COMPLIANCE CHALLENGES AND RISKS

Regulatory Compliance Requirements

Legal firms must update privacy policies and marketing practices to comply with DUAA's new regulations.

Subject Access Request Revisions

Handling Subject Access Requests must align with the 'reasonable and proportionate' standard under DUAA.

AI and Automated Decisions Oversight

AI-driven tools require transparency and human oversight to prevent legal and ethical risks.

Consequences of Non-Compliance

Failure to comply can cause severe fines and damage client trust and professional reputation.

PROCESSES AND PROCEDURES TO REVIEW

OPERATIONAL ADJUSTMENTS FOR COMPLIANCE

Data Governance Review

Firms must update privacy notices and cookie policies to reflect new lawful processing bases and consent requirements.

Compliance of Marketing Practices

Direct marketing strategies should align with PECR standards to ensure lawful communication with clients.

Data Sharing and Transfers

Data sharing agreements must comply with updated international adequacy provisions for secure transfers.

Transparency in Automated Decisions

Automated decision workflows need transparency and options for human intervention to protect individuals.

ROLE OF DPO OR SENIOR RESPONSIBLE INDIVIDUAL

LEADERSHIP IN COMPLIANCE MANAGEMENT

Critical Role of DPO

The Data Protection Officer oversees compliance and updates policies according to changing legislation.

Training and Monitoring

DPO trains staff on compliance obligations and monitors ongoing adherence to regulations.

Ethical AI Oversight

DPO advises on ethical and legal implications of automated decisions and AI tools within the organization.

Strategic Compliance Leadership

DPO provides strategic and operational guidance to maintain accountability and transparency.

IMPACT ON CYBER ESSENTIALS

ALIGNMENT WITH SECURITY STANDARDS

Secure Data Handling Importance

DUAA emphasizes secure data handling aligned with any Cyber Essentials certification requirements for legal practices.

Core Security Measures

Both frameworks require supported and patched software, robust access controls, and regular security audits.

Risk of Non-Compliance

Failing to maintain security can breach DUAA and Cyber Essentials, risking penalties and reputational damage.

Integrated Cybersecurity Strategy

Legal firms should align DUAA compliance with cybersecurity strategies to ensure data protection and confidentiality.

HOW JDI-UK CAN HELP

PROFESSIONAL SERVICES FOR COMPLIANCE

JDI-UK
GDPR SERVICES

Consultancy and Compliance Audits

JDI-UK interprets legislative requirements and conducts audits to identify compliance risks for legal firms.

Policy Updates and Staff Training

We help update policies, revise workflows, and train staff to ensure understanding of compliance responsibilities.

Managed Compliance Services

For hands-off firms, JDI-UK manages compliance documentation and ongoing monitoring comprehensively.

Cyber Essentials Certification Support

JDI-UK assists firms in achieving Cyber Essentials certification to comply with Legal Aid Agency requirements, as well as strengthening data protection and cybersecurity for all customers.

REAL-LIFE EXAMPLES

REAL-LIFE EXAMPLES OF HOW DUAA MIGHT AFFECT LEGAL COMPANIES

1. Data Sharing with Authorities

Under DUAA, solicitors can rely on “recognised legitimate interests” for certain disclosures without a formal balancing test.
Example: A conveyancing firm may share suspicious transaction data with the **National Crime Agency** during a money laundering investigation without needing additional consent.

2. Handling Subject Access Requests (SARs)

DUAA introduces the concept of “reasonable and proportionate” searches for SARs.
Example: If a former client requests their data, the firm only needs to check case files, invoices, and correspondence—not every archived record. Failure to apply this standard could lead to complaints and ICO enforcement.

3. Automated Decision-Making in Client Services

DUAA relaxes restrictions on automated decision-making but requires safeguards.
Example: A firm using AI tools for initial case triage must provide transparency and allow human review. Ignoring these safeguards could result in discrimination claims or regulatory penalties.

REAL-LIFE EXAMPLES OF HOW DUAA MIGHT AFFECT LEGAL COMPANIES

4. Digital Identity Verification

DUAA promotes secure digital verification services for remote onboarding.

Example: A solicitor firm offering online client onboarding must implement compliant identity checks. Using outdated or insecure systems could breach DUAA and GDPR obligations.

5. Marketing and Cookie Compliance

DUAA eases cookie consent for analytics but maintains transparency requirements.

Example: A law firm running a website analytics tool without updating its cookie banner risks non-compliance and fines under PECR rules.