STEPHENSON HARWOOD

DSARS: DROWNING IN REQUESTS

21 November 2026

KATIE HEWSON

Partner

Meet the Team

SPEAKERS



KATIE HEWSON

Partner

+44 20 7809 2374

+ katie.hewson@stephensonharwood.com

2027 Chambers Ranked in UK
Katie Hewson

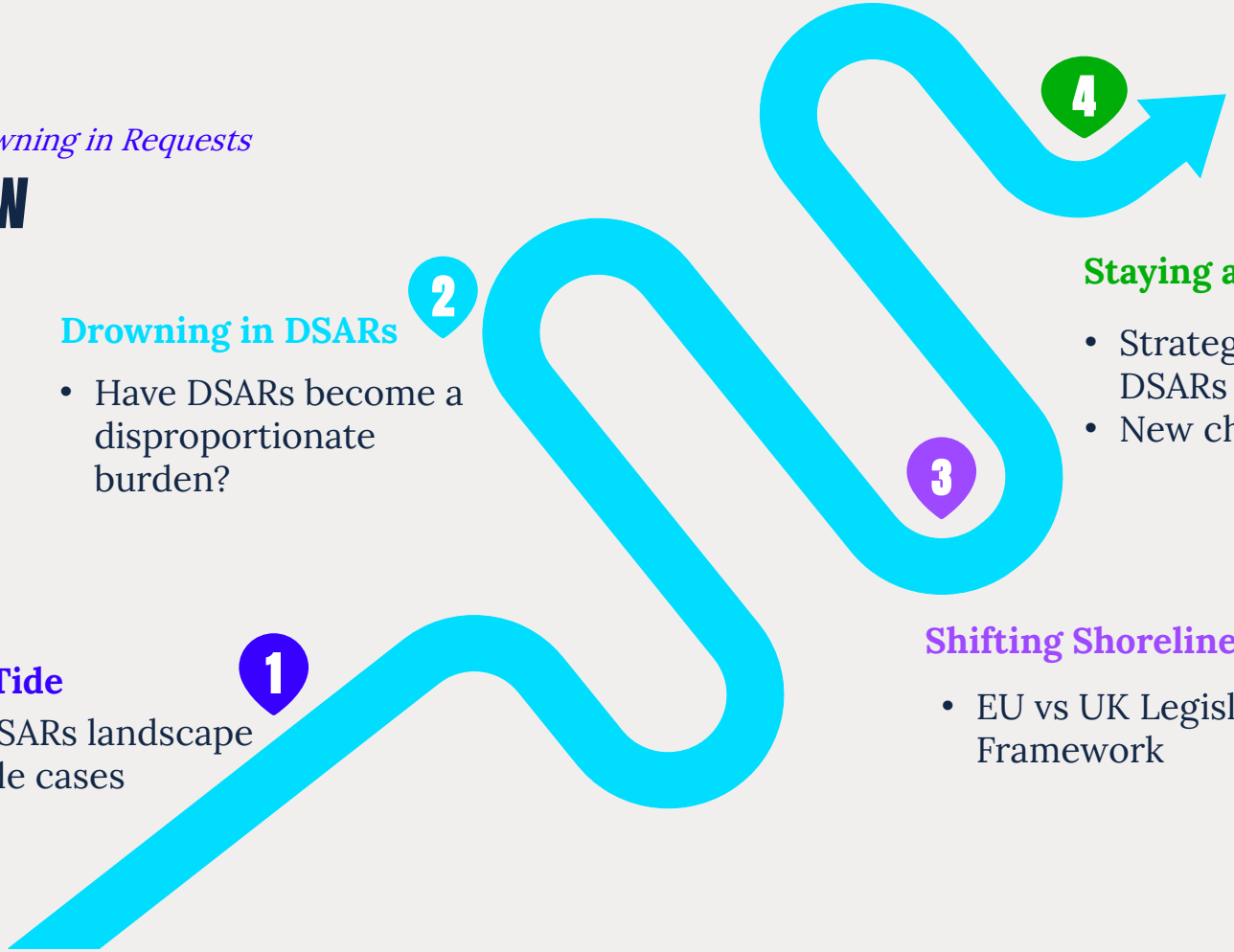
RECOMMENDED LAWYER
Legal500
UNITED KINGDOM
2026

© Stephenson Harwood LLP.

STEPHENSON HARWOOD

DSARS: Drowning in Requests

OVERVIEW



The Rising Tide

- Current DSARs landscape
- High profile cases

Drowning in DSARs

- Have DSARs become a disproportionate burden?

Shifting Shorelines

- EU vs UK Legislative Framework

Staying afloat

- Strategies for tackling DSARs
- New challenges

© Stephenson Harwood LLP.

STEPHENSON HARWOOD

The Rising Tide

CURRENT DSARS LANDSCAPE

Farage joins explosion in people using subject access requests

Haroon Siddique

SARs from employees have become standard in work disputes and are increasingly used by public figures



Nigel Farage claims his account at Coutts was closed because of his political values. Photograph: Reuters/Alamy

Nigel Farage's claim that his account at the prestigious bank Coutts was closed because of his political values has been bolstered by a report from the bank's reputational risk committee that he obtained via a subject access request (SAR), an increasingly common tool - some would say weapon - used by individuals in dispute with organisations.

Gregg Wallace drops personal data claim against BBC



Care home director found guilty of ignoring request for personal information

Date **4 September 2025**

Type **News**

The director of a care home in Bridlington, Yorkshire, has been fined for refusing to respond to a request for a resident's personal information – known as a subject access request (SAR).

In April 2023, a woman requested personal information about her father from Bridlington Lodge Care Home.

Jason Blake, 56, was found to have blocked, erased, or concealed records held by Bridlington Lodge Care Home between 12 April and 12 May 2023 to prevent this information being disclosed.

© Stephenson Harwood LLP.

STEPHENSON HARWOOD

Drowning in DSARs

HAVE THEY BECOME A DISPROPORTIONATE BURDEN?

Used in ways the legislators didn't intend?

DSARS OFTEN USED BY DATA SUBJECTS:



+ To help uncover personal data that could be used for potential or existing claims.



+ To put pressure on controllers to settle claims, particularly in UK.



+ In employment, in conjunction with, or instead of, a grievance.



+ In a way that "feels" unfounded – breadth, lack of clarification, anger.



+ Using GenAI or similar tools that don't always help target data of interest.



+ As a nuisance element to waste controller time and resources.

© Stephenson Harwood LLP.

Drowning in DSARs

OR ARE INDIVIDUALS JUST EXERCISING THEIR LEGAL RIGHTS?

An important right of access for data subjects

BENEFITS OF DSARS:



+ Enable data subjects to make up for deficient notices & challenge bad practices.



+ Why shouldn't DSARs be used to support a claim? Particularly in certain jurisdictions.



+ Burden can be fault of controller's retention or usage policies (or lack thereof).



+ Balance of power still with controller.



+ GenAI and tech tools now available to support controllers.



+ Perhaps DSARs are the symptom, not the cause?

© Stephenson Harwood LLP.

Drowning in DSARs

LET'S PLAY DSAR BINGO!

GenAI	WhatsApp	"All"
To an individual	"Relates"	+WP
Campaign	1m+	MP / Police

© Stephenson Harwood LLP.

Hidden Currents

BEWARE....



AI TOOLS

+ HR systems
+ Online interviews
+ Recording meetings



VERSION CONTROL

+ Multiple iterations
+ Final version



BYOD

+ Personal devices
+ WhatsApp for business



CCTV

+ Where is it stored?
+ Retention



ELECTRONIC NOTE TAKING DEVICES

+ Are they approved devices
+ Where stored?

© Stephenson Harwood LLP.

Shifting Shorelines

EU VS UK LEGISLATIVE FRAMEWORK



EU DIGITAL OMNIBUS

- *"... the right of access, which is from the outset favourable to data subjects, should not be abused in the sense that the data subjects abuse them for purposes other than the protection of their data"*
- Proposals allow refusal for manifestly unfounded / excessive. "Reasonable grounds" for excessive.
  - Intent of causing damage or harm to controller.
  - Offer to withdraw in return for compensation.



- **C-526/24 (BRILLEN ROTTLER GMBH & CO. KG V TC)**

CJEU ruled in March 2026 that even a first DSAR can be refused as "excessive" under Article 12(5) GDPR when it is pursued with an abusive intention.



UK DATA (USE AND ACCESS) ACT 2025

- DUAA codified "reasonable and proportionate" search.
- Impact of DUAA complaints process on DSARs?
- However, a high bar, underlined by *Ashley v HMRC [2025] EWHC 134 (KB)*, which criticised:
  - Narrow approach to what is personal data.
  - Restricting searches to one department only.
  - Decontextualised extractions.
  - Number of hours alone does not make searches disproportionate.
  - Speculative balancing of disclosure vs prejudice.

© Stephenson Harwood LLP.

Staying Afloat

STRATEGIES FOR TACKLING DSARS

"MANIFESTLY UNFOUNDED" AND PRIVILEGED CORRESPONDENCE

COORDINATION WITH DISPUTE RESOLUTION STRATEGY - TIMING AND PRIVILEGE

SETTLEMENT AGREEMENT LANGUAGE AND PROFESSIONAL OBLIGATIONS

© Stephenson Harwood LLP.

Staying Afloat

STRATEGIES FOR TACKLING DSARS



Retention - data mapping and actually applying policies.



Scoping upfront – critical step in making a DSAR reasonable and proportionate.



Standardising approach and workflows, aligned to usage policies.



Accountability - recording decisions, ready to justify to regulator or data subject.



Technology – AI options to narrow down search results; potentially even highlight responsive personal data. Safeguards?

© Stephenson Harwood LLP.

STEPHENSON HARWOOD

Q+A

© Stephenson Harwood LLP. Any reference to Stephenson Harwood in this document means Stephenson Harwood LLP and/or its affiliated undertakings. Full details can be found at Legal Notices | Stephenson Harwood. Information contained in this document is current as at the date of first publication and is for general information only. It is not intended to provide legal advice.