

Forcyd Insights

Data in class actions: know your case, understand your class

21 September 2026



Data in class actions: know your case, understand your class

MATHIEU VAN RAVENSTEIN | JULIAN GERAERDS

Class actions¹ continue to grow throughout Europe. Once regarded as an American concept, they are now a component of the European legal landscape, spanning competition, consumer, data protection, and product liability matters. Jurisdictions are introducing, or broadening, collective action and redress mechanisms, claimant entities are becoming more active, and litigation funding has become increasingly available². At the same time, we have seen the data (evidence) underlying these disputes multiply, generated in greater volumes and spread across more systems, devices and channels than ever before³. What defendants often underestimate is that a class action is a data problem before it is a legal one.

None of this is a passing trend. For almost twenty years, the EU worked to build a common framework for collective redress, and that framework is still hardening and evolving⁴. The practical effect is simple: more claims, larger classes and greater exposure, across more industries than before. That growth is mirrored by an increase in the amount of data that must be identified, analysed and reviewed⁵. The data underlying these disputes is scattered accordingly: across countries, systems and channels, from email and mobile⁶ to chat and cloud platforms⁷. Every piece of data leaves a trail, and in any litigation that trail is crucial. The hard part is no longer questioning whether the data exists. It is finding it, making sense of it and using it to your advantage.

This article shows through an example how devastating the consequences can be when data management in the liability phase and distribution phase fails. It then takes the defendant's perspective on the role of data and legal technology across both phases. Following the conclusion, this article closes with some practical tips.

Key Takeaways

- **Data is decisive.** It must be integrated across the whole lifecycle of a class action, from the moment a potential class action is on the horizon. An early read on the strength of the evidence, the likely size and shape of the class and the exposure lets a party set the direction of the case rather than chase the other side's moves.
- **Control and produce evidence.** Locating what exists, producing what must be disclosed, and being able to prove the absence of relevant material, rather than having that absence lead to adverse inferences against you, ensures control of the narrative.
- **Review incoming claims at scale.** Verifying who belongs in the class and what each member is actually owed is a challenge of both volume and method.

The cost of not knowing

The consequences of losing control of the data are not just procedural, nor theoretical. When an organisation understands neither its own record nor the population it must ultimately compensate, failures in liability can compound into failures in redress.

The Post Office Horizon IT scandal (UK)

In the United Kingdom, between 1999 and 2015, the state-owned Post Office Limited (**Post Office**) held thousands of its sub-postmasters liable for accounting shortfalls reported by “Horizon”, an IT system, and prosecuted⁸ hundreds of them for theft and false accounting. The shortfalls were, in very many cases, imaginary and the product of bugs, errors, and defects in Horizon itself.

Following this, 555 sub-postmasters brought a group action against the Post Office⁹, which produced two judgments that substantially upheld the claimants’ case. What followed included a settlement of £57.75 million days before the final judgment, overturned convictions through courts and by legislation¹⁰, a government-commissioned inquiry¹¹, and redress payments exceeding £1.4 billion¹², making this one of the most consequential miscarriages of justice in British legal history, and a case study relevant to both phases explored in this article.

The liability phase failed first. For years, the Post Office insisted Horizon was reliable while the evidence to the contrary sat in its own records, including an independent review the company itself had commissioned that found the system in some cases not fit for purpose¹³. The court described the defence as institutional obstinacy: bare assertions maintained against the weight of the defendant’s own material. The Post Office’s difficulties with its own data never ended. Years later, the statutory inquiry was still being disrupted by the late disclosure of documents¹⁴, with hearings postponed because of continuing disclosure failures. The Post Office failed to confront its own record during the litigation and could not produce it on time afterwards. It never controlled its case, so its case controlled it.

The distribution phase then failed on top of it. The redress schemes that followed the litigation were not a court-ordered distribution, but the operational challenge was closely analogous. The Post Office struggled to verify eligibility and assess claims at scale.

When the Post Office opened the Horizon Shortfall Scheme, it expected claims “of the order of a few hundred”. By 27 November 2020, it had received over 2,400 eligible claims. Guidance on consequential losses was not published until approximately four months after the scheme launched and two months before it was due to close. By 26 June 2026, the scheme had received over 14,000 claims, including eligible late claims, while more than £1.4 billion had been paid across the redress schemes to close to 13,000 claimants. Claims were still being processed¹⁵.

The Inquiry’s conclusion was stark: the Horizon Shortfall Scheme had not consistently delivered full and fair redress, particularly in more substantial claims. The gap between the claimant cohort anticipated and the claimant population that actually emerged became a distribution problem in its own right.

Phase I – Liability

The Post Office Horizon IT scandal illustrates that the consequences of poor data management may become most obvious during redress but often originate much earlier. Before a class can be compensated, liability must be established. This phase centres on one question: is the defendant responsible for the alleged harm? The answer is determined through evidence: the internal records of what happened, and what the defendant knew.

From a data perspective, two things matter during this phase and they run in sequence.

1. **Understand your own case.** Get a grip on what the facts actually are, where the weaknesses lie, and what the internal record will and will not support.
2. **Disclose what must be disclosed.** Increasingly, defendants must hand over the relevant parts of that same record to the other side.

This initial understanding is what a defence and strategy are built on. Getting the first part right before the second arrives is what separates a defendant that controls its position from one that reacts to it.

The disclosure shift

Traditionally, most of continental Europe did not have broad US-style discovery. Civil-law procedure generally puts the burden on each party to prove its own case. Often this comes with no overarching duty to hand the opponent all relevant documents, including unfavourable material. When production requirements exist, they are often narrow and document-specific rather than open-ended.

Disclosure in Europe is widening, and the clearest sign of it is the Product Liability Directive¹⁶ (PLD). Adopted in 2024, the revised Product Liability Directive must be transposed by 9 December 2026 and will apply to products placed on the market or put into service from that date. The PLD modernises a regime left largely untouched since the 1980s: it broadens the definition of a product and eases the claimant's burden to prove a defect. For a defendant, though, the changes are much more significant as the PLD brings disclosure into product liability litigation, in many Member States for the first time¹⁷. The European legislator aims to reduce the potential asymmetry of information between claimants and manufacturers¹⁸.

If a claim is plausible, a court can order the defendant to disclose the relevant evidence in its possession, bound by the principles of necessity and proportionality and with protection for trade secrets. It does not allow a fishing expedition. The obligation has teeth: if a defendant fails to produce what it has been ordered to, defectiveness is presumed, and it falls to the defendant to rebut it. A failure to produce is not treated as neutral, and "we could not find it" is rarely a defence. The inability to produce your own evidence risks being read as a statement about what that evidence would have shown.

This does more than add a procedural step; it creates real exposure. Because "relevant evidence" is not tightly defined, a disclosure order can reach material a company would never volunteer. Once that material is produced, control over it weakens. While confidentiality measures exist, they are court-managed, and do not give a company complete control over how sensitive information is handled once it has entered the litigation process.

Companies should treat disclosure as a risk to be managed from the moment the first claim is on the horizon, assessing early what their own documents reveal and preparing accordingly. Defendants must make sure they understand their own evidence long before anyone else asks to see it.

The PLD is the clearest example of broadening disclosure regimes, though not an isolated one. The EU has been writing disclosure into its regimes for over a decade. The Antitrust Damages Directive¹⁹ (ADD) brought it to competition claims in 2014. The Representative Actions Directive²⁰ (RAD) extends disclosure to representative actions brought by qualified entities across a wide range of fields²¹. Subject to the RAD's conditions, courts must be able to order disclosure of relevant evidence in the defendant's control.

National legislators are moving the same way, with the Netherlands broadening parties' access to each other's documents in its 2025 evidence reform²². The changes are also not restricted to a specific area of the law; the new regulations do not just apply to product liability. A defendant in European mass litigation should, therefore, expect that part of its internal record can be ordered into the open.

Preparing properly

If disclosure can pull your evidence into the open, and silence works against you, the only sensible approach is to know your own record before anyone else does. That means not waiting until a claim is on the horizon to understand your information landscape, but putting yourself in a position to respond swiftly, on your own terms, when a claim does arise.

At the scale of a modern business, however, getting to that position is not straightforward. Relevant material sits across years of email, chat, documents, and system data, likely spread across the globe. There is often far more information than any team can realistically work through manually, let alone in the time a case allows.

What the review practically looks like

Legal technology exists to address this exact problem. In practice a review of the entire corpus helps to sort a large, unstructured body of data into what matters and what does not. Every document, within scope, is assessed for relevance to the issues, screened for privilege, and, if relevant, marked as a key document (one that supports your position or exposes a risk). Done well, this is what converts raw data into an understanding of the case while remaining efficient and proportionate. Done badly, or not at all, it leaves the defendant guessing about its own records.

Technology-assisted review, analytics and generative AI can sift a large corpus quickly, surface the documents that matter and group them by issue. This way human reviewers reach the important material first, cluster documents by issue so related threads are assessed together, and flag likely-privileged content so it is caught before it is disclosed. Models used properly across millions of files can provide a level of consistency that is difficult for large review teams to maintain, especially under time pressure.

Used well, AI can make a review faster and more consistent without sacrificing defensibility. Validation is what separates the two outcomes.

The newest capability goes a step further: generative AI can draw on the reviewed material to produce first drafts of the artefacts a case strategy is built on: chronologies of key events, summaries of the evidence per issue, and overviews of what each custodian knew and when. These are starting points for counsel rather than conclusions and should be treated with caution, but they compress the distance between a reviewed corpus and an informed strategy from weeks to days.

What matters most, however, is not the tool but the methodology behind it: a structured approach that builds a clear internal picture of the facts, the issues that drive the case, and the underlying evidence, all while maintaining defensibility.

What validation actually involves

Defensibility is the key. A review is only as good as your ability to defend the process behind it. That means using these tools in a controlled way, with outcomes validated against sampling, measured for accuracy, quality-checked, and documented at every step, so the process can be explained and defended in court²³.

In a technology-assisted review specifically, validation is typically achieved with a control set. A control set is a sample of documents coded by experienced lawyers, blind to the model, that serves as the ground truth the system is tested against. The model's output is then measured for recall (how much of what matters it found) and precision (how much of what it found matters), with targets set and agreed before the review starts, not after the results are in. Before anything is discarded, the discard pile itself is sampled, so there is evidence, not hope, that nothing decisive was left behind. Privilege calls get their own layer of human quality control. And every threshold, sample and decision is logged as the review runs, producing a record that can be handed to a court that asks how the set was produced.

The results of validation are a clear, tested view of your own evidence, and the confidence to disclose knowing exactly what you are handing over and why.

Information governance

However, all of this presumes one thing: that the records still exist and are available. Retention policies left on autopilot, chat messages that delete themselves, devices wiped when employees leave can all quietly impact the information available. A failure to preserve relevant records may expose a defendant to adverse inferences or other procedural consequences, depending on the rules.

The mitigation is unglamorous but well established. Retention policies should be deliberate rather than default. For example, deletion schedules should be set per data type against actual legal and business needs, applied consistently, and reviewed as systems change.

On top of that sit legal hold procedures. Organisations should have a tested process for suspending deletion once preservation obligations are triggered under the applicable law, often when litigation is reasonably contemplated or foreseeable, reaching the sources that matter in practice, including chat,

mobile devices, and the accounts of departing employees. Preservation also means keeping evidence intact in a forensically sound manner, with metadata preserved, so that for any given document it can still be proven when it was created, by whom and whether it changed.

Phase II – Distribution

The distribution phase is what follows once liability is established or a settlement is agreed. In this phase the individual claimants come forward and say what they are owed. For the defendant, the question flips from what happened to who genuinely belongs in the class and what, if anything, each of them is actually owed.

Two things matter and, again, they run in sequence.

1. **Verification of class members.** Unfortunately, not everyone who files belongs in the class, and each claim must be verified against what the defendant already knows to be true.
2. **Valuation of damages.** The amount claimed and the amount owed are rarely identical. A thorough process should assess the damages based on the available evidence, the facts of each claim and the valuation framework.

The difficulty is scale. When claims arrive in the tens or hundreds of thousands, assessing them one by one is impossible and accepting them without review creates errors and unnecessary cost. At that volume, effective verification and valuation are essential to compensate eligible claimants accurately and consistently.

How claims can be validated, and what claimant-level data can be obtained, depends heavily on the applicable regime and jurisdiction. For example, claims acquired by assignment may require each underlying file, entitlement and loss to be assessed individually, while opt-out collective actions arising from common conduct may allow greater standardisation where individual circumstances and damages are sufficiently similar. Both require validation, but the necessary evidence, workflow and degree of individual review can differ substantially.

What the incoming data looks like

In the liability phase the evidence is your own and you know, roughly, where it lives, who created it and what systems retain it. In the distribution phase it arrives from outside, from claimants, and often at large scale. The information can take many forms, from claim forms and bank statements to receipts, medical records, and photographs. It may be submitted in every format, be incomplete or duplicated and, in some cases, fraudulent. All of it must be processed and validated consistently.

What makes the incoming flood manageable is the defendant's own data. Transaction histories, customer records, product registrations, delivery data: these are the reference against which every claim can be checked, to confirm that a claimant bought the product, held the account, or suffered the loss they describe. A defendant that has done the work of the liability phase already understands this data. That is the quiet payoff of the first half of this article: the corpus you mastered to defend the case is the same corpus that now lets you verify the class. The two phases are not separate data problems; they are two sides of the same coin. This is why integration matters. The process becomes significantly more efficient when claims can be reviewed directly against financial systems, ERP platforms and other internal data.

Verification and valuation in practice

In practice this is a review of every incoming claim against two questions: does this claimant belong in the class, and if so, what are they owed. Verification means extracting the facts asserted in each claim and matching them against the reference data: names against customer records, purchases against transaction logs, and dates against what the defendant knows to be true. It also means looking across the claims, not just at each individually, since duplicate claimants, recycled documents and clusters of near-identical submissions only become visible in the aggregate. Valuation then applies the compensation framework, whether set by settlement, judgment, or scheme rules, to each verified claim, so that materially equivalent claims are assessed consistently.

At scale, none of this can be done by hand alone. Technology now carries much of it. Models can read unstructured submissions and extract the relevant facts, matching can run automatically against the reference data, and clear cases can be triaged from contested ones so that human judgement is spent on the exceptions, borderline calls, and the claims requiring closer scrutiny. The shape is the same as the liability phase review. Technology carries the volume but people decide what matters.

Defensible process

Here too, the point that separates a serious process from a risky one is defensibility, but the audience has changed. In the liability phase you defend your process to a court. In the distribution phase you defend it to the class, to the court approving the outcome and, if it goes wrong, to the public. Every rejected claim is a decision that may have to be justified to the person it affects. Every accepted claim is money spent that may have to be justified to whoever funds the scheme. And inconsistency, materially equivalent claims being decided differently, is not a rounding error at this scale; repeated across thousands of claims, it becomes a question of fairness.

The requirements are the ones the liability phase already taught. Criteria must be applied consistently, decisions documented and quality-checked against sampling, and the process explained in full when someone asks how a claim was decided. Handled this way, distribution closes the case. Handled badly, as the Post Office example shows, it reopens it.

Privacy considerations

Such a process may involve handling medical records, financial data, or other sensitive data, and making decisions that materially affect individuals. This demands access controls, data minimisation, meaningful human review of adverse outcomes, a route to challenge decisions, and an auditable record of how each decision was reached. Some of these safeguards are already reflected in law. Where a decision is based solely on automated processing and produces legal or similarly significant effects, restrictions from the General Data Protection Regulation²⁴ (GDPR) apply, subject to limited exceptions. The Artificial Intelligence Act²⁵ (AI Act) adds a further layer of governance for AI systems within its scope, with obligations applying in phases.

In distribution, consistency is not a technical virtue. Assessing ten thousand, or even hundreds of thousands, of claims in a fair manner means applying the same criteria to materially equivalent claims.

Conclusion

A class action is a data problem before it is a legal one. In the liability phase, the case is decided by how well a defendant knows its own record, under disclosure regimes that can increasingly attach adverse consequences to failures to disclose relevant evidence. In the distribution phase, it is decided by how well a defendant can verify and value the claims of thousands of claimants against that same record. While the data flips direction, the discipline does not.

That continuity is the practical lesson. The corpus a defendant masters to fight liability is the same, or at least the basis of the reference against which it later verifies its class. The processes that make a review defensible, including documented decisions, consistent criteria and sampling-based quality checks, are also what make a distribution survive scrutiny. Work done early compounds, whereas work deferred must be completed later under a court's deadline rather than the defendant's own timeline.

None of this is hypothetical. The Post Office example illustrates failures analogous to both phases within a single broader scandal: it would not confront its own record when liability was contested and did not understand the scale and composition of the population eligible for redress. The consequences are still unfolding.

For organisations with any realistic exposure to class actions, the conclusion is uncomfortable but simple. The trend lines all point one way: more claims, broader disclosure, larger classes, and more data underneath all of it. Whether the data strengthens the defence or undermines it is decided before proceedings begin.

Data is decisive in class actions, from the liability phase to distribution. Organisations with proper data governance, that map their data early, validate their tools rigorously, and design defensible processes will be best positioned to control their cases, not chase them.

Practical Tips

Class actions are won or lost on data. Below are concrete steps to ensure your organisation is prepared for both the liability and distribution phases.

Before a dispute

1. **Map your data landscape now.** Identify systems, custodians, and jurisdictions where data resides. A data map built under pressure is a data map built to fail.
2. **Get retention and legal hold in order.** Check auto-deletion policies (especially for ephemeral data like chats) and ensure holds can be enforced the moment a dispute is foreseeable.

When a claim is on the horizon

3. **Conduct an *Early Case Assessment* (ECA).** Use internal data to size the class, assess exposure, and identify gaps. Use these insights to steer strategy from day one. Don't let the opponent define the narrative.

Running the process

4. **Prioritise defensibility over novelty in technology.** Validate tools with sampling, track accuracy metrics, and document every step. A workflow that can't be explained to a court isn't a workflow but a liability.
5. **Use humans for judgement, machines for scale.** Automate ranking, clustering, and matching, but reserve human review for exceptions, borderline cases, and adverse decisions. Always record who decided what.
6. **Document in real time.** Log decisions, criteria, versions, and QC checks as they happen.

When distributing

7. **Clean and deduplicate reference data before claims arrive.** Matchable customer and transaction records are the backbone of scalable verification. Starting this after the portal opens guarantees delays.
8. **Design for the honest but messy claimant.** Most incomplete submissions are legitimate. Build in correction and resubmission workflows. Run fraud detection across the dataset to target outliers without alienating the class.
9. **Finalise the compensation framework before processing claims.** Pre-defined criteria, evidence thresholds, and valuation rules ensure consistency at scale. Ad-hoc rules create ad-hoc injustice.

About the Authors

Mathieu van Ravenstein

Partner at FORCYD



Mathieu has over 20 years of experience in legal and policy advice and eDiscovery. He has worked with global corporations, law firms and international institutions advising on many high-profile and complex investigations and disputes as well as on litigation in areas such as corporate fraud, money laundering, competition law and international trade.

vanravenstein@forcyd.com
+31(0)6 458 727 46

Julian Geraerds

Cyber & eDiscovery Expert at FORCYD



Julian is an expert in legal technology and digital investigations. He is experienced in complex, large-scale matters relating to litigation, regulatory compliance, internal investigations and arbitration. He works with large corporations and leading law firms, focusing on high-stakes issues such as competition, anti-corruption and bribery, and data breaches.

geraerds@forcyd.com
+31 (0)6 398 111 71

The authors would like to thank Michelle Hagoort, Liwia Jarczewska, and Marie Munten, who contributed to this piece.

¹ For the purposes of this article, the term “class action” is used as a shorthand for the full range of collective redress mechanisms, including bundled and assigned claims, both in opt-in and in opt-out regimes. While these differ significantly as a matter of law, from a data and legal technology perspective the challenges largely converge.

² CMS, European Class Action Report 2025 (August 2025), <https://cms.law/en/gbr/publication/cms-european-class-action-report-2025>.

³ See e.g. IDC, Data Age 2025: The Digitization of the World from Edge to Core (November 2018), <https://www.seagate.com/files/www-content/our-story/trends/files/dataage-idc-report-final.pdf>.

⁴ See, in particular, the Commission’s EU Consumer Policy Strategy 2007-2013 of 31 May 2007 COM(2007) 99, <https://eur-lex.europa.eu/EN/legal-content/summary/eu-consumer-policy-strategy-2007-2013.html>, the Commission Green Paper on Consumer Collective Redress, COM(2008) 794 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52008DC0794>, and the Commission Recommendation 2013/396/EU of 11 June 2013 on common principles for injunctive and compensatory collective redress mechanisms in the Member States [2013] OJ L 201/60, <http://data.europa.eu/eli/reco/2013/396/oj>.

⁵ See e.g. Disclosure in the Business and Property Courts, Lecture by Sir Julian Flaux, the Chancellor of the High Court, on 17 January 2023, in particular paragraphs 2 and 6, https://www.judiciary.uk/wp-content/uploads/2023/01/Disclosure-Lecture-2023_.pdf.

- ⁶ See e.g. The Sedona Conference, Commentary on Discovery of Mobile Device Data, 26 Sedona Conf. J. 735 (2025), https://www.thesedonaconference.org/sites/default/files/publications/Commentary_On_Discovery_of_Mobile_Devices_Data_Post_Public_Comment_Version_1.pdf.
- ⁷ See e.g. The Sedona Conference, Commentary on Discovery of Collaboration Platforms Data, 26 Sedona Conf. J. 627 (2025), https://www.thesedonaconference.org/publication/Commentary_on_Discovery_of_Collaboration_Platforms_Data.
- ⁸ Most cases were privately prosecuted by the Post Office itself. However, a number of cases were prosecuted by other bodies, including the Crown Prosecution Service, the Public Prosecution Service for Northern Ireland, and the Crown Office and Procurator Fiscal Service.
- ⁹ Bates & Others v Post Office Ltd (No 3: Common Issues) [2019] EWHC 606 (QB) and (No 6: Horizon Issues) [2019] EWHC 3408 (QB), <https://www.bailii.org/ew/cases/EWHC/QB/2019/3408.html>.
- ¹⁰ Post Office (Horizon System) Offences Act 2024, https://www.legislation.gov.uk/ukpga/2024/14/pdfs/ukpga_20240014_en.pdf.
- ¹¹ See Retired High Court judge to lead Post Office Horizon IT Inquiry, a UK Government press release published 29 September 2020, <https://www.gov.uk/government/news/retired-high-court-judge-to-lead-post-office-horizon-it-inquiry>.
- ¹² Department for Business and Trade, Post Office Horizon financial redress data as of 31 January 2026, <https://www.gov.uk/government/publications/post-office-horizon-financial-redress-and-legal-costs-data-for-2026/post-office-horizon-financial-redress-data-as-of-31-january-2026>.
- ¹³ Second Sight Support Services Ltd, Initial Complaint Review and Mediation Scheme: Briefing Report Part Two (21 August 2014), paras 18.6 to 18.12, Post Office Horizon IT Inquiry document POL00226961, <https://www.postofficehorizoninquiry.org.uk/sites/default/files/2025-06/POL00226961.pdf>.
- ¹⁴ Post Office Horizon IT Inquiry, *Final Report, Volume 1: Human Impact and Redress* (HC 1119, 8 July 2025), paras 4.18, 4.22 and 4.28, <https://www.postofficehorizoninquiry.org.uk/volume-1-post-office-horizon-it-inquiries-final-report>.
- ¹⁵ Department for Business and Trade, Post Office Horizon financial redress data as of 26 June 2026, <https://www.gov.uk/government/publications/post-office-horizon-financial-redress-and-legal-costs-data-for-2026/post-office-horizon-financial-redress-data-as-of-26-june-2026>.
- ¹⁶ Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC [2024] OJ L, 2024/2853, consolidated text of 18 November 2024, <http://data.europa.eu/eli/dir/2024/2853/2024-11-18>.
- ¹⁷ BEUC, Comparative Legal Study on Procedural Rules and Their Impact on Collective Redress in the EU (BEUC-X-2025-026, 2025), https://www.beuc.eu/sites/default/files/publications/BEUC-X-2025-026_Study_Procedural_Rules_Impact_on_Collective_Redress_in_EU.pdf.
- ¹⁸ Recital (42) of the PLD.
- ¹⁹ Directive 2014/104/EU of the European Parliament and of the Council of 26 November 2014 on certain rules governing actions for damages under national law for infringements of the competition law provisions of the Member States and of the European Union [2014] OJ L 349/1, <http://data.europa.eu/eli/dir/2014/104/oj>.
- ²⁰ Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC [2020] OJ L 409/1, consolidated text of 12 September 2025, <http://data.europa.eu/eli/dir/2020/1828/2025-09-12>.
- ²¹ Directive (EU) 2020/1828, Articles 2 and 18, and Annex I. The Directive applies to representative actions concerning infringements of the EU laws listed in Annex I that harm or may harm the collective interests of consumers. Annex I covers a wide range of fields, including data protection, financial services, travel, energy and telecommunications, consolidated text of 12 September 2025, <http://data.europa.eu/eli/dir/2020/1828/2025-09-12>.
- ²² Wet van 6 maart 2024 tot wijziging van het Wetboek van Burgerlijke Rechtsvordering en enige andere wetten in verband met de vereenvoudiging en modernisering van het bewijsrecht (Wet vereenvoudiging en modernisering bewijsrecht), Stb. 2024, 62, <https://zoek.officielebekendmakingen.nl/stb-2024-62.html> (Dutch).
- ²³ See, by way of example, Practice Direction 57AD, paras 9.6–9.7 and Appendix 1, paras 1.3 and 1.15, <https://www.justice.gov.uk/courts/procedure-rules/civil/rules/part-57a-business-and-property-courts/practice-direction-57ad-disclosure-in-the-business-and-property-courts>; *Pyrrho Investments Ltd v MWB Property Ltd* [2016] EWHC 256 (Ch), paras 31–35, <https://www.bailii.org/ew/cases/EWHC/Ch/2016/256.html>.
- ²⁴ Article 22 of Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L 119/1, <http://data.europa.eu/eli/reg/2016/679/oj>.
- ²⁵ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence [2024] OJ L, 2024/1689, <http://data.europa.eu/eli/reg/2024/1689/oj>.

FORCYD

Forcyd offers high-end eDiscovery, Document Review, and Cyber Forensics, advisory and solutions. We help clients get ahead of their most complex issues related to fraud, litigation and data breaches. Solutions range from data breach assessments and GDPR reporting to, end-to-end management of complex mass-volume litigation, and information requests (supported by eDiscovery tooling).