Country Report: The Netherlands[1]

Marta Reysner & Anna van Duin (APPLIED project)

1. Introduction and general overview

In the Netherlands, the processing of personal data is regulated by the General Data Protection Regulation (Regulation (EU) 2016/679) ("**GDPR**") and its Implementation Act. The general system of collective redress is provided in the Act on the Resolution of Mass Claims in Collective Action ("**WAMCA**", date of entry into force: 1 January 2020). Its development was triggered by the need to address the volume and complexity of mass claims, particularly those involving large groups of individuals affected by similar issues (for example in consumer law). The WAMCA represents the third significant advancement in the field of legal development, following WCA (1994) and WCAM (2005) which already allowed interest groups to seek a binding settlement or a declaratory judgment.

The Netherlands successfully implemented the EU Representative Actions Directive - "**RAD**" (with explicit reference to the GDPR in the Explanatory Memorandum). Nonetheless, because the Netherlands already had a generally available class action procedure in the WAMCA, there was no need to create new legislation to implement the Directive. The grounds of claim for collective actions are not limited to cases regarding or originating in EU law. Within a single regime which now applies under Article 3:305a of the Dutch Civil Code (*Burgerlijk Wetboek*, "**BW**"), collective redress is permitted for a wide range of claims regardless of the remedies being sought (e.g. declaratory judgment, injunction, damages) and applies in a considerable number of areas (e.g. consumer protection, competition law, environmental protection, data protection under the GDPR).

Since the introduction of the WAMCA, the number of collective redress actions has increased significantly. The collective redress system has been employed to address a diverse range of issues, including data privacy concerns, consumer rights violations, and financial disputes. The central registry of collective claims shows a steady rise in the number of filed and ongoing cases. The involvement of commercial litigation funders is one of the factors contributing to this. At the time of writing (9 August 2024) there are ten (10) pending WAMCA cases about (alleged) GDPR violations; there are crossovers with other areas of law, in particular consumer law[2] and telecommunications law; unjust enrichment is also used as a cause of action.

Nevertheless, significant obstacles remain, particularly in meeting criteria on representation and governance as well as securing adequate funding. The preliminary rounds, which assess the admissibility of claims, can be lengthy and complex. This can slow down the resolution of cases and impose significant burdens on claimant organizations. Furthermore, calculating damages,

---

1 A similar version of this report has been co-produced by Anna van Duin (together with Aart Jonkers and Kirsten Meiring, UvA) for the Digital Freedom Fund. The authors have participated in the DFF digiRISE project, funded by the European Union CERV action. To learn more about this project, please contact Alexandra Giannopoulou (alexandra@digitalfreedomfund.org).

2 There is also public enforcement of consumer law (unfair commercial practices) against e.g. TikTok by the Authority Consumer & Market.

especially for non-material harm, remains a complicated and unresolved issue; it also impacts the assessment of the possibility of bundling claims.

Section 2 of this report gives a brief description of the legal framework which applies to collective litigation also, or specifically, in the field of data protection law. It addresses three key issues: (i) opt-in regime, (ii) recognition as a qualified entity, and (iii) funding.

Section 3 identifies the main collective actors working in the field of data protection in the Netherlands, either specifically, or as an element of general consumer protection.

Section 4 gives a comprehensive overview of the collective private parties' litigation in the field.

2. Legal Framework

a. National implementation of Art. 80 GDPR

The explanatory memorandum to the Dutch Implementation Act of the RAD (*Implementatiewet richtlijn representatieve vorderingen voor consumenten*) underscores, firstly, that Member States may provide that the rights referred to in Articles 78 and 79 of the GDPR can be exercised without the data subject's mandate (cf. Article 80(2) and recital 142 of the GDPR). This includes the right to claim damages. Secondly, the GDPR is listed in Annex I of the RAD. As the explanatory memorandum states, this is, for the Netherlands, solely a clarification that collective damage claims are also possible for violations of the GDPR. Furthermore, the Dutch Implementation Act of the GDPR (*Uitvoeringswet Algemene verordening gegevensbescherming*) stipulates that the data subject can object against representation in collective and administrative proceedings (Article 37), which in practice would amount to an opt-out.

With this, it seems clear that (although there is still some discussion whether) Article 80 GDPR does not stand in the way of collective actions for damages. This interpretation has been confirmed by the Amsterdam District Court in its 2023 judgment in the TikTok case (ECLI:NL:RBAMS:2023:6694). It also aligns with the recent 2024 appellate judgment in Oracle & Salesforce (ECLI:NL:GHAMS:2024:1651), where the Amsterdam Court of Appeal reaffirmed the possibility of collective actions under the GDPR while indicating that certain questions regarding the scope of Article 80 might warrant further clarification by the CJEU.[3]

b. National framework on collective redress

- **The WCA (1994)**

The earliest form of collective redress in the Netherlands, allowing organizations to initiate collective actions on behalf of groups of individuals. This law primarily provided for declaratory judgments and injunctive relief and did not facilitate claims for monetary compensation.

[3] A request for cassation appeal has been granted in this case, allowing the Supreme Court to provide much-needed (further) guidance on the admissibility requirements under the WAMCA.

- **The WCAM (2005)**

Introduced a mechanism for the collective settlement of mass damages, which could, upon court approval, become binding on all affected parties unless they opt-out.

- **The WAMCA (2020)**

See section 1. Admissibility criteria for claimant organizations can be found in both the BW and the Code of Civil Procedure ("**Rv**"); the case law is still evolving and on the GDPR, few cases have been adjudicated. The recent ruling in Orale & Salesforce serves as a pertinent example of how Dutch courts apply the stringent admissibility criteria in practice, particularly in the context of complex GDPR claims.

An interest organization with full legal capacity that, according to its articles of association, has the objective to protect specific interests, may bring a claim to protect similar interests, meaning that the rights of action of the (sub)groups involved are suitable for bundling (Article 3:305a sub 1 BW). The claimant organization must be sufficiently representative in terms of constituency and amount of the claims represented (Article 3:305a sub 2 BW). The claimant organization must meet certain governance requirements, including the existence of a supervisory body and the availability of sufficient funds (Article 3:305 a sub 2 (c) BW) as well as having sufficient experience and expertise. The claimant organization is only admissible if it has no profit motive, and the legal action brought has a sufficiently close connection with the Dutch legal sphere (the 'scope rule' of Article 3:305a sub 3 (a) and (b) BW). Before bringing an action, the claimant organization should consult with the defendant (Article 3:305a sub 3 (c) BW). The district courts are responsible for determining the admissibility of collective claims during preliminary hearings. This process ensures that only well-founded and representative claims proceed to trial. Dutch case law places great emphasis on the strict adherence to admissibility criteria.

When the WAMCA was drafted, lawmakers recognized that the strict requirements outlined in Article 3:305a BW could be excessively burdensome for interest groups pursuing legal action with an idealistic objective. Consequently, a new paragraph 6 was added, granting judges discretionary power to provide a partial exemption, so that they may be required 'only' to comply with the representativeness requirement, maintain a non-profit motive and adhere to the scope rule. Furthermore, the legal action cannot seek monetary damages under this lighter regime. In February 2023, a motion was passed which called for the exploration of the extent to which further requirements for representativeness should be set for interest groups with an idealistic purpose (Parliamentary documents II 2022/23, 36169, nr. 37), but no changes have been made so far.
The court will only consider the merits of the claim if it is sufficiently plausible that collective action is more efficient and effective than bringing an individual action and that the claim is not evidently without merit (Article 1018c sub 5 (b) and (c) Rv). If multiple claimant organizations are engaged in proceedings about the same events and concerning similar facts and legal questions, the court will designate one of them as the exclusive advocate (Article 1018e Rv); the court will consider several factors, including the size of the organizations' constituencies, the financial interest they represent and the nature of the activities they undertake. Once the exclusive advocate has been appointed, stakeholders will be able to exercise their first opt-out option; if a collective settlement is reached, there is a second opt-out round for stakeholders who do not wish to be bound by it (Article 1018f sub 1 and Article 1018h sub 5 Rv).

Third party litigation funding ("**TPLF**") is allowed under the Dutch collective action regime, subject to conditions. The litigation funder should not have substantial influence over the

procedure and the success fee should not be excessive. In other words, it has to be established whether the foundation is sufficiently independent in relation to the litigation funder (and the lawyers working for it) and thus whether the interests of the persons it represents are adequately safeguarded (see Section 2a, Section 4).

The acceptable percentage of the compensation to be received for the benefit of a litigation funder will depend on the amount of compensation to be awarded and the number of individuals who are expected to claim it. A percentage of 25% has been mentioned as accepted in the case law, but more important is the expected outcome for both the stakeholders and the litigation funders when executing a collective settlement or a settlement agreement. It is justifiable for litigation funders to receive appropriate compensation given the risks they take, but this must be reasonably proportionate to the amount they have financed. In other words, what is acceptable as a percentage depends on the circumstances of the case. See also the Amsterdam District Court judgment in TikTok, in which case the court suggested the funder should in any case not receive more than five times the investment it made. It is unclear whether this takes account of inflation and the risk-free rate of return (time value of money), which is highly relevant because pay-out often takes place after many years. The fivefold ceiling is not a general rule.

There is no experience with how to handle the compensation that claim foundations can receive on behalf of their engaged litigation funders in the situation where there is more than one representative organization, of which – in the case of admissibility – at least one will be designated as the exclusive representative, and possibly non-designated representatives will remain as litigants.

- **Implementation of the RAD**

The RAD has been implemented in the Netherlands primarily through the existing WAMCA framework. The WAMCA is also meant for – but not limited to – consumers, and meets most of the requirements of the RAD. Only where the RAD has additional rules for claims falling within its scope, an adjustment of the WAMCA was necessary. There are just a few special rules that required a relatively limited adjustment of Dutch law.

Compared to the previous regime, the scope has not changed significantly. One notable change is the prohibition of the application of an opt-out regime to consumer claimants residing outside of the Netherlands (Article 1018f(6) Rv). The WAMCA generally does allow an opt-out regime for foreign claimants, albeit not by default and subject to court approval (Article 1018f(5) Rv).

Another difference is that the RAD works with a list of qualified representative organizations, whereas the WAMCA only works with general (though rather strict) admissibility criteria per case. The Directive's requirements for organizations are almost the same as the requirements for an organization in the WAMCA. Therefore, the Netherlands can also apply the WAMCA's organizational requirements to Dutch organizations that want to be on the list. However, the Directive does impose a few additional requirements that have now been implemented, including provisions for transparent communication about collective claims. Another change is that the Netherlands now has to accept standing of foreign organizations that are on the RAD's list, and cannot subject them to the WAMCA requirements.

A further modification through implementation of the RAD is that the rules on third party litigation funding are somewhat more detailed than the pre-existing regime under the WAMCA. The law implementing the RAD made one small change, implemented in Article 3:305a(2)(f) BW,

which stipulates that, for consumers claims, litigation funding is not allowed by a party that is a competitor of the funder.

3. Main Actors

Compared to other countries, there are many actors in the Netherlands driving collective data protection litigation, including consumer advocacy organisations, non-governmental organizations focused on privacy rights, and specialized law firms. These groups often (allege they) represent large numbers of individuals who have been affected by data breaches or unlawful data proceedings. Additionally, specialized litigation vehicles, such as (ad-hoc) claims foundations, are increasingly playing a role in facilitating collective actions. These efforts are supported by a growing interest from litigation funders who finance these actions. The involvement of this wide mix of actors makes the Netherlands a notably active jurisdiction for collective private enforcement of the GDPR, reflected in the relatively high number of cases pursued in this area.

The Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*) oversees compliance with privacy laws. However, there seems to be no direct connection or no clear link between public enforcement of the GDPR and collective actions.

4. Legal Proceedings

The objective of this last section is to provide an overview of pending and adjudicated data protection CPE proceedings as per 31 August 2024.

The judiciary maintains a central registry of collective claims. The main purpose of this digital environment is to provide lawyers, stakeholders and interested parties with information on collective claims that have been filed. The register contains details of the parties involved, the nature of the claims and the current status of each case, enabling interested parties to determine whether they also wish to file a collective claim for the same event(s).

Consumers are also informed about ongoing collective redress actions through public notices published in widely accessible media such as newspapers, online platforms and official websites. Opt-in collective actions require consumers to actively register to participate. This can usually be done through an online portal or by submitting a form provided by the plaintiff organization. The RAD also facilitates the participation of consumers from other EU Member States in cross-border collective actions. The number of consumers opting in plays a crucial role in demonstrating the representativeness of the claimant organization. A higher number of participants can strengthen the mandate of the organization and support the legitimacy of the collective action.

Pending cases

Of the currently pending WAMCA cases about the GDPR, five cases concern litigation against big-tech companies for the unlawful commercial use of data (advertising, surveillance of users, predicting behaviour):

Meta: summons of Data Privacy Stichting (1-3-2024)	
Date of Initiation of the Claim	2024

Summary	Data Privacy Stichting claims that Meta has violated several privacy laws. The core of the case consists of two parts. Firstly, between 2010 and 2020 Meta unlawfully processed personal data of Dutch Facebook users without a valid legal ground for advertising purposes (as confirmed in a previous ruling by the Dutch Court in 2023). Secondly, Meta allegedly transferred personal data of Dutch Facebook and Instagram users to the U.S., where it became subject to surveillance by U.S. intelligence agencies. After filing two lawsuits in cooperation with Consumentenbond for the unlawful use of personal data and the transfer of data outside Europe, the Data Provacy Stichting has filed a new lawsuit, seeking damages.
Claimant	Data Privacy Stichting (with the support of Consumentenbond)
Defendant	Meta
Funder	Lieff Cabraser Heimann & Bernstein, LLP. According to the information available at the Data Privacy Stichting website, Lieff Cabraser Heimann & Bernstein bears the full financial risk of the action and will be eligible to receive a litigation funding fee up to 18% of the net proceeds, plus expenses, subject to Court approval and provided that the Foundation obtains compensation for the Aggrieved Parties.
Remedies Sought	Injunction to stop processing special personal data without legal basis and a conditional injunction to destroy or at least return personal data; material and material damages, amounting to €750 per Facebook user for privacy violations and €500 for the unlawful data transfers.
Status/Outcome	TBA

Meta: summons of Stichting Onderzoek Marktinformatie (3-11-2023)	
Date of Initiation of the Claim	2023
Summary	Meta has allegedly violated several privacy laws, including those pertaining to data leaks, targeted advertising, and the transfer of user data to the US. These actions also constitute an unfair trade practice. With regard to targeted advertising, the summons also addresses the following issues: unjust enrichment, undue payment and group liability.
Claimant	Stichting Onderzoek Marktinformatie (SOMI)
Defendant	Meta
Funder	All the funds required for the Meta case have been provided by Reunion Ventures B.V. – a company owned by the chairman of SOMI, Mr Franke – under an agreement last updated in December 2022. Reunion has made the donation without seeking any form of compensation, with the objective of utilising the funds to facilitate the social change that SOMI was established to achieve.
Remedies Sought	Injunction to stop processing special personal data without legal basis and a conditional injunction to destroy or at least return personal data: Immaterial and material damages amounting to €500 per Facebook user for data privacy infringement and €1000 per Facebook user for data leak

Status/Outcome	TBA

Google: summons of Stichting Privacybelangen and Stichting Massaschade & Consument (12-9-2023)	
Date of Initiation of the Claim	2023
Summary	• Stichting Bescherming Privacybelangen: Collecting and processing personal data without consent. Transfer of personal data to third parties, including governments outside Europe. In addition, Google uses so-called "dark patterns": design techniques that manipulate users into taking actions that negatively impact their privacy, such as unknowingly providing access to certain personal information. • Stichting Massaschade & Consument: Allegedly unlawful collection and processing of personal data from Android users;
Claimant	• Stichting Bescherming Privacybelangen, cooperation with Consumentenbond • Stichting Massaschade & Consument
Defendant	Google Inc.
Funder	• Stichting Bescherming Privacybelangen: Lieff Cabraser Heimann & Bernstein. • Stichting Massaschade & Consument: Eaton Hall Funding LLC.
Type of Action	
Remedies Sought	• Stichting Bescherming Privacybelangen: Immaterial damages, material damages (estimated at Google's profits); various injunctions and prohibitions, including a ban on tracking internet usage via third-party cookies and a prohibition on using location data for advertising purposes • Stichting Massaschade & Consument: prohibitions and injunctions, under the penalty of a fine ("onder verbeurte van een dwangsom"), claim for material and immaterial damages;
Status/Outcome	TBA

Twitter: summons of Stichting Data Bescherming Nederland (14-9-2023)	
Date of Initiation of the Claim	2023
Summary	Defendants used free apps on mobile phones and tablets to collect and then share personal data with third parties. The collection and sharing of personal data with third parties took place for advertising purposes.
Claimant	Stichting Data Bescherming Nederland
Defendant	• X Corp. • Twitter Inc. • Twitter International Unlimited Company

	• Twitter Netherlands B.V.
Funder	Orchard Global
Type of Action	
Remedies Sought	• Immaterial damages • Material damages (primary: costs incurred and/or the lost benefit resulting from the defendants' actions, secondary: remittance of profits made by the defendants) • Judicial order to pay the amount by which the defendants have unjustly enriched themselves • Judicial order for the destruction, inspection and notification of third parties, with the imposition of a penalty in the event of non-compliance
Status/Outcome	TBA

TikTok: appeal summons of Stichting Take Back your Privacy, Stichting Massaschade & Consument and Stichting Onderzoek Marktinformatie against two (interim) judgments of the Amsterdam District Court (3-6-2021)	
Date of Initiation of the Claim	2021
Summary	Data use of minor children without consent. In all three the summons: alleged violations of the GDPR, EU Charter, TW (Telecommunicatiewet), consumer law, the obligations of video platform services, and references to unjust enrichment.
Claimant	• Stichting Onderzoek Marktinformatie • Stichting Take Back Your Privacy • Stichting Massaschade & Consument
Defendant	TikTok
Funder	• Stichting Onderzoek Marktinformatie: All the financial resources required for the TikTok initiative have been provided by Reunion Ventures B.V. under an agreement that was last updated in December 2022 • Stichting Take Back Your Privacy: BPGL Funding I Limited, based in Jersey, is the funder of the TikTok campaign • Stichting Massaschade & Consument: The lawsuit is funded entirely by IVO Capital and its Cayman Islands-based fund Consumer Privacy Litigation Funding (42) L.P.
Remedies Sought	• Stichting Onderzoek Marktinformatie: The destruction of conditions, the erasure of personal data, orders protecting minors, and immaterial damages • Stichting Take Back Your Privacy: The destruction of conditions, the erasure of personal data, orders protecting minors, and (im)material damages

	• Stichting Massaschade & Consument: Annulment of unreasonably onerous terms, prohibitions and orders protecting minors under the penalty of a fine, and (im)material damages
Status/Outcome	Rechtbank Amsterdam 25 October 2023 (ECLI:NL:RBAMS:2023:6694) held STBYP and SMC to be admissible in their claims. STBYP as exclusive representative for minor TikTok users and SMC for adult users (judgment of 10 January 2024).

Amazon: summons of Stichting Data Bescherming Nederland (18-10-2023)	
Date of Initiation of the Claim	2023
Summary	Amazon collects a significant amount of data from customers who create accounts on their platform. This data is used by Amazon to build a detailed personal profile of users in order to show personalised ads. Furthermore, the company shares this personal data with third parties. Finally, Amazon tracks internet behaviour.
Claimant	Stichting Data Bescherming Nederland
Defendant	Amazon
Funder	Marsh Funding, LLC, a group company of Longford Capital.
Remedies Sought	Claim for damages; injunctions for, inter alia, the cessation of the breaches and the implementation of a privacy policy.
Status/Outcome	TBA

Two cases specifically concern litigation against online data management platforms (DMPs):

Stichting Data Bescherming Nederland v. Adobe Inc. en Adobe Systems Software Irl. Ltd. (13-12-2023)	
Date of Initiation of the Claim	2023
Summary	Unlawful data collection from internet users by Adobe, which is processed into profiles and offered to third parties, who use it to offer personalized content (mainly online advertisements).
Claimant	Stichting Data Bescherming Nederland
Defendant	• Adobe Inc. • Adobe Systems Software Irl. Ltd.
Funder	Marsh Funding, LLC, a group company of Longford Capital.
Remedies Sought	• An injunction for the protection of the data subjects, including the destruction of the unlawfully collected data and the cessation of the breaches of privacy; immaterial and material damages.
Status/Outcome	TBA

The Privacy Collective tegen Oracle en Salesforce (28-3-2022)	
Date of Initiation of the Claim	2022
Summary	The Privacy Collective posits that Oracle and Salesforce create and maintain highly detailed profiles of internet users, including through the collection of data through cookies placed without valid consent. These profiles are then exploited for advertising targeting, in violation of privacy legislation.
Claimant	The Privacy Collective
Defendant	• Oracle • Salesforce
Funder	Innsworth Capital Limited
Remedies Sought	• Damages • Costs (litigation and extrajudicial costs) to be imposed upon Oracle and Salesforce. • Deletion of data • Provision of clear and accessible information to users about data collection • Cessation of unlawful conduct.
Status/Outcome	Amsterdam Court of Appeal 18 June 2024 (ECLI:NL:GHAMS:2024:1651) declared the claims of TPC to be admissible.

Two cases concern data leaks of personal health data:

***Stichting ICAM tegen de Staat der Nederlanden* (28-3-2023)**	
Date of Initiation of the Claim	2023
Summary	The ICAM Foundation represents the interests of over 6.5 million individuals whose highly sensitive personal data has been exposed to theft. This data concerns personal information collected and used by GGDs in connection with the fight against the coronavirus;
Claimant	Stichting Initatieven Collectieve Acties Massaschade (ICAM)
Defendant	• Staat der Nederlanden The other defendants include Dutch public health foundations, municipalities, security regions and public health services of several Dutch regions, constituting a total of 34 defendants. Some of these entities have been declared inadmissible by the court in an interlocutory ruling.
Funder	Liesker Procesfinanciering
Remedies Sought	• Injunction for the termination of the breach and the implementation of enhanced security measures • Immaterial damages

	• Material damages
Status/Outcome	TBA

Cliënten and beroepsbeoefenaren in de GGZ tegen Nederlandse Zorgautoriteit (19-7-2023)	
Date of Initiation of the Claim	2023
Summary	The objective of this procedure is to terminate the obligation of healthcare providers to submit data on the categorisation of care demands to the Dutch Healthcare Authority (NZa). This concerns highly sensitive data pertaining to approximately 800,000 Dutch citizens receiving mental health care ('GGZ').
Claimant	Multiple collective interest groups involved: • Stichting LOC Waardevolle Zorg • Stichting KDVP • Stichting Platform Bescherming Burgerrechten. The plaintiffs in the case have formed a coalition under the name "Confidence in the mental health sector."
Defendant	Nederlandse Zorgautoriteit
Funder	The necessary funds have been obtained through the use of a crowd-funding initiative.
Remedies Sought	No damages claimed; only declarations for rights and requests for injunctions/prohibitions.
Status/Outcome	Rechtbank Midden-Nederland 17 July 2024 (ECLI:NL:RBMNE:2024:4106) held the claim to be admissible.

And, most recently, one case against an anti-virus and security software provider:

Stichting CUIC tegen AvastSoftware sro cs. (17-8-2024)	
Date of Initiation of the Claim	2024
Summary	The claim filed by CUIC concerns alleged violations of privacy laws through the unlawful collection and commercialisation of user data by Avast Software and its subsidiaries via its antivirus software. The (partly sensitive) user data was unlawfully sold to third parties.
Claimant	Stichting CUIC – Privacy Foundation for Collective Redress
Defendant	· Avast Software S.R.O. · Avast LTD. · Avast Holding B.V. · Avast Software B.V. · AVG ECommerce CY B.V.
Type of Action	

Remedies Sought	• Compensation for (im)material damages • Injuctions for the cessation of unlawful data collection and commercialisation and the deletion of the unlawfully collected data. • Requirement to disclose which data was collected, how it was used and with whom it was shared.
Status/Outcome	TBA

Adjudicated cases

A few cases concerning the GDPR have already been adjudicated (under the WAMCA and/or the previous regime):

Collectieve vordering tegen Oracle Nederland B.V., SFDC Netherlands B.V., Oracle Corporation, Oracle America, Inc. en Salesforce.com, Inc. (17-8-2020)	
Date of Initiation of the Claim	2020
Summary	The case concerns the alleged violation of Dutch internet users' privacy. TPC claims that Oracle and Salesforce place cookies and collect personal data through their Data Management Platforms (DMPs), building detailed user profiles that are used for targeted advertising without the users' consent. Additionally, TPC claims that the privacy of Dutch internet users was violated due to a data breach at Oracle. TPC argues that these practices violate the GDPR and Dutch Telecommunications Act.
Claimant	The Privacy Collective (TPC)
Defendant	• Oracle Nederland B.V.; • SFDC Netherlands B.V.; • Oracle Corporation; Oracle America, Inc.; • Salesforce.com, Inc.
Type of Action	
Remedies Sought	• Declaratory judgment; • Prohibition against violating AVG/GDPR; • Damages.
Status/Outcome	The district court ruled that the plaintiff's claims were inadmissible due to a lack of sufficient representation. District Court Amsterdam 29 December 2021, ECLI:NL:RBAMS:2021:7647

Stichting Expertisebureau Online Kindermisbruik tegen Hammy Media Ltd and Stop Online Shaming en Expertisebureau Online Kindermisbruik tegen vagina.nl (27-2-2020)	
Date of Initiation of the Claim	2020
Summary	Involves two foundations taking legal action against the operator of a website that allows users to upload and share adult content, including images and videos. The foundations claim that some of the material published on

	the website includes sexually explicit or intimate videos of individuals filmed without their consent, thus violating their privacy rights. Claimants argue a breach of Dutch and European privacy laws, including Article 8 ECHR and the GDPR.
Claimant	• Stichting Stop Online Shaming; • Stichting Expertisebureau Online Kindermisbruik
Defendant	Operator of "vagina.nl" (Anonymous in the published judgment)
Type of Action	
Remedies Sought	• Declaratory judgment; • Order to remove the footage from the website and to provide a report from an independent ICT-expert appointed by the court to prove this; • Prohibition to upload, disclose or possess any footage.
Status/Outcome	The district court ruled that the defendants must be able to demonstrate that individuals who can be recognized in the images or footage published on the websites have given their consent. District Court Amsterdam 16 February 2022, ECLI:NL:RBAMS:2022:557 and 12 April 2023, ECLI:NL:RBAMS:2023:2192

Stichting Privacy First tegen de Staat der Nederlanden (5-1-2021)	
Date of Initiation of the Claim	2021
Summary	Stichting Privacy First filed a lawsuit against the Dutch State regarding the UBO (Ultimate Beneficial Owners) register. The UBO register requires companies to disclose personal information about their beneficial owners. Some of this information is accessible to the public, thus raising privacy concerns. Privacy First sought to have the UBO register suspended. They argued that the registration and public disclosure of this information violated fundamental privacy rights ander European law, including the ECHR, EUCFR and GDPR.
Claimant	Stichting Privacy First
Defendant	Staat der Nederlanden
Type of Action	
Remedies Sought	• Obligation to suspend the UBO register; • Declare inapplicable the right of any person to inspect data in the UBO register.
Status/Outcome	The district court rejected the claim regarding the UBO-register. The Hague District Court 18 Marc 2021, ECLI:NL:RBDHA:2021:2457

Collectieve vordering tegen Stichting Slachtoffers Iatrogene Nalatigheid Nederland (zwartelijstartsen.com) (11-11-2020)	
Date of Initiation of the Claim	2020

Summary	This case concerns a digital blacklist, listing nearly 900 medical professionals, often with their photos, accusing them of medical crimes or negligence. A Dutch foundation, Stichting Stop Online Shaming, claimed that the blacklist was unlawful, violating the privacy rights of healthcare professionals and breaching the GDPR.
Claimant	Stichting Stop Online Shaming
Defendant	Stichting Slachtoffers Iatrogene Nalatigheid-Nederland
Type of Action	
Remedies Sought	• Prohibition to make public statements, including names, photos or other personal information of doctors; • Prohibition to use the domain name 'zwartelijstartsen.nl' and 'zwartelijstartsen.com'; • Injuction to hand the domain names over to claimant and to request Google to remove all references to said domain names;
Status/Outcome	The district court ruled that the website's practice of blacklisting doctors was unlawful and violated the GDPR. District Court Midden-Nederland 8 January 2021, ECLI:NL:RBMNE:2021:23