

Data class actions in Europe

and spotlights in Mexico,
Russia and the U.S.

Here's what you should know, and how you should
prepare to defend data class actions under the GDPR.



A recap on the basics

The General Data Protection Regulation 2016/679 (GDPR) provides means to enforce provisions related to personal data processing by you as a data controller or data processor. It introduces collective actions everywhere in European Member States; which can be brought by not-for-profit bodies dedicated to personal data protection.

An individual right of action before national courts against a controller or a processor

When data subjects – the people whose data is at issue – believe the processing of their data has infringed their rights, the GDPR kicks in. It enables data subjects to claim against a data controller or processor in national courts. Non-judicial or administrative remedies may also be available.

The GDPR gives data subjects a choice of forum, allowing them to bring their claim before different courts. There's also a pending lawsuit system. Here, courts have to suspend their proceedings or decline jurisdiction where identical proceedings are pending before another court.

Liability and a right to compensation

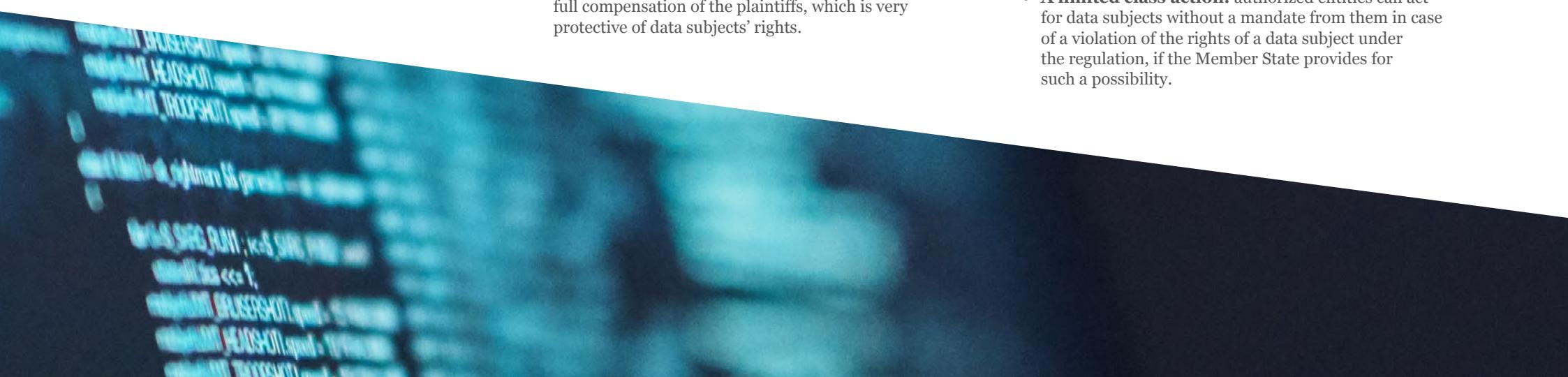
There's a strict liability regime on data controllers and processors. Also, when several controllers or processors are involved, they are jointly liable. To avoid liability, the defendant controller(s) or processor(s) must prove they weren't responsible for the event that harmed the data subjects. Bear in mind that data subjects can bring a claim without having to prove a controller's or processor's fault or negligence.

Data subjects can seek compensation before national courts for material or non-material damage that results from the infringement of their rights under the GDPR. The regulation also sets the principle of full compensation of the plaintiffs, which is very protective of data subjects' rights.

Claims consolidation mechanism

The GDPR creates three rights of action:

- **A representative joint action:** data subjects have the right to mandate an authorized entity to lodge a complaint for them (the data subjects) with a data protection authority or to exercise the right to judicial remedy.
- **A limited compensatory representative joint action:** data subjects have the right to mandate an authorized entity to exercise their right to receive compensation, if the law of the Member State enables it.
- **A limited class action:** authorized entities can act for data subjects without a mandate from them in case of a violation of the rights of a data subject under the regulation, if the Member State provides for such a possibility.



European data class actions: tell us who you really are

A European right to 28 (or so) national collective actions

The GDPR doesn't provide a consistent class action or even a procedural framework to launch an efficient representative joint action. Instead, it introduces a European right to collective actions. Although the GDPR says the data subject "shall have the right to" initiate actions, it doesn't provide the data subject with an actionable tool; it leaves this to Member States. In other words, the GDPR doesn't detail the procedural aspects of claims an association brings for data subjects, so reference to national procedural law should be made.

Consequently, there could soon be as many personal data collective action procedures as European countries, which would be contrary to the GDPR's objective of consistency. In fact, this started with Members States adopting new bills to implement the GDPR into their national laws, even though the GDPR directly applies.

Are pan-European and global class actions possible?

If you process personal data all around the world, you may legitimately wonder whether the GDPR could lead to multi-jurisdictional collective actions, including European and non-European data subjects.

Here, the first issue lies with the GDPR's scope: it isn't limited to European citizens or residents. Although not limitless, the territorial scope of the GDPR is broad, and this could lead to it applying beyond EU borders.

This mix of broad territorial scope and choice of forum could give birth to pan-European data protection collective actions. Under certain circumstances, these could include non-EU data subjects.

Nevertheless, the European data protection class action regime remains unclear at this stage. Some answers may come from the European Data Protection Board, whose mission is to issue guidelines, recommendations, and best practice procedures on the GDPR.

How EU representative actions interact with GDPR class actions

On 24 November 2020, the European Parliament endorsed the new European collective actions legislation, Directive (EU) 2020/1828 of the European Parliament and of the Council on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC. The Directive will enter into force on the 20th day following its publication in the Official Journal of the European Union. Member States will then have 24 months to transpose it into their national laws, and an additional six months to apply it. So we can expect the new procedures to be actually implemented from mid-2023 onward.

The new directive enables representative actions against infringements by traders of a variety of EU directives and regulations, including the GDPR. The Member States have latitude when implementing certain features of the directive. The next 24 months will therefore be decisive for the shape of the collective proceedings in the Member States and some jurisdictions may emerge as enabling these representative actions with fewer options than others. Given the possibility of cross-border representative actions, we may see some venues becoming (even) more popular for collective redress. While the new directive promises safeguards against abusive lawsuits it will be crucial that defendants' rights and fairness of procedure are going to be maintained in practice.

[Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee](#)

What does the directive on representative actions provide for?

“

Since consumers now operate in a wider and increasingly digitalised marketplace, achieving a high level of consumer protection requires that areas such as data protection [...] be covered by the Directive, in addition to general consumer law.

”

“

It is for the Member States to lay down rules, for instance, on admissibility, evidence or the means of appeal, applicable to representative actions.

”

Qualified entities from different Member States should be able to join forces within a single representative action in a single forum.

”

The directive aims to ensure equal consumer protection across the EU and set a minimum standard below which Member States must not fall.

These are its main features:

- Data protection is within the scope of the directive.
- Actions can be brought only by ‘qualified entities’ designated by an EU Member State.
- If designated for cross-border representative actions, a ‘qualified entity’ is allowed to bring actions in any EU Member State.
- Several ‘qualified entities’ from different EU Member States are allowed to jointly bring a single representative action in one EU Member State where the alleged infringement affects or is likely to affect consumers from different EU Member States.
- Qualified entities may choose to apply for an injunction or to seek compensation (redress measures).
- EU Member States can decide whether to establish an “opt-in” system or an “opt-out” system.
- An “opt-in” system is required for any consumer living outside the relevant EU Member State to join the action.
- Cross-border effects of final decisions.
- Introduction of the loser-pays principle.
- Third parties may fund representative actions.

Interaction with the data class actions created by the GDPR and the existing or future national mechanisms for collective redress

“

This Directive should not replace existing national procedural mechanisms for the protection of collective or individual consumer interests.

”

“

This Directive does not prevent Member States from adopting or retaining in force procedural means for the protection of the collective interests of consumers at national level. However, Member States shall ensure that at least one procedural mechanism that allows qualified entities to bring representative actions for the purpose of both injunctive measures and redress measures complies with this Directive.

”

The Directive does not require Member States to scrap their existing mechanisms, they just have to establish the mechanism required by the Directive as well. However, doubts remain about how this European collective redress mechanism will interact with the data class actions created by the GDPR and the existing or future national mechanisms for collective redress.

U.S. perspective



Class actions are well established in the United States and have been a conspicuous part of the legal landscape for many years. While there's no single uniform law for data processing in the United States, class actions have become a feature of litigation around data processing, practices, and security. The U.S. experience offers a cautionary tale of what class actions may bring to Europe.

To establish standing to pursue their claims in federal court, individuals seeking to represent a class of consumers must show, at a minimum, that they suffered concrete injury. This injury must be actual or imminent, not hypothetical or conjectural. It must be fairly traceable to the defendants' conduct and able to be redressed by a court. The injury requirement has proved especially challenging for plaintiffs asserting claims related to the collection, use, or disclosure of data, or to a data breach. A number of courts have found that alleged intangible harm related to individuals' data does not rise to the level of a concrete injury sufficient to confer standing.

Apart from standing, individuals must show they have a viable cause of action. In the United States, there is no GDPR analogue; no federal law provides an express mechanism for redressing alleged harms arising out of the processing of data. Instead, a patchwork of federal and state laws governs such processing. These laws cover, among other things, protection of data, representations about the handling of data, and notifications should a data breach occur.

To proceed with claims on a class basis, litigants must also satisfy Federal Rule of Civil Procedure 23. In most cases this Rule creates an opt-out framework where all individuals within the class definition are considered part of the action unless they exclude themselves from the class. Litigants seeking "class certification" must show, among other things, that their claims are typical of other putative class members' claims. They must also show that there are common questions of law or fact across the putative class and that they will fairly and adequately represent the putative class.

These requirements have not deterred a wave of class action suits around data processing, including data breaches. Many of these actions have been dismissed as legally deficient or have been resolved by settlements. The settlements often include significant sums for the plaintiffs' lawyers, while providing limited cash benefits to individuals in the class. The intangible nature of alleged harms and the large size of the affected population make these settlements even more challenging. Data stolen in a cyberattack, for example, may not have been misused. It may likely not be misused in the future, and providing meaningful compensation to the data subjects can prove difficult.

Russian perspective

The main data protection law in Russia is the Federal Law of 27 July 2006 No. 152-FZ on Personal Data. Data class actions can be brought before the Russian courts only if data subjects' rights are violated according to Russian data privacy law, not the GDPR.



Russian data privacy law doesn't include the terms "data controller" or "data processor"; instead, it uses "data operator". It defines a data operator as a state or municipal authority, individual, or legal entity that processes personal data in any form on its own or jointly with other persons; that organizes and/or carries out the processing of personal data, and determines the purposes, content, and actions of personal data processing.

One data operator may instruct another to process particular personal data. In this case, the instructing data operator remains responsible for the personal data processing by the other data operator before relevant data subjects.

Data subjects can file civil claims with the court for compensation of damages caused and moral harm, as well as ending unlawful data processing if their rights are violated according to the Russian personal data legislation.

The claimant has to prove the amount of damages, as well as the breach of their rights and a link between the two. Compensation for moral harm has been historically quite low in Russia. As a result, data subjects favor filing complaints with the Russian data protection authority (Roskomnadzor) to protect their rights and end unlawful data processing, since this requires less time and effort.

Russian courts of general jurisdiction are authorized to consider the claims of data subjects against data operators. Currently, Russian law doesn't provide an opportunity to file a joint action in the civil proceedings. So, several data subjects may file a single claim only as co-plaintiffs. But the court may divide this claim into different cases involving different plaintiffs.

Amendments to the Russian Code on Civil Procedure devoted to class actions were adopted on 18 July 2019. These came into force on 1 October 2019. Since this date, filing joint actions is allowed in civil proceedings and will likely become more popular in Russia.

Issues to expect when you face data class actions in Europe

Forum shopping

The broad territorial scope of the GDPR, and the choice of forum it provides to data subjects, could give rise to forum shopping and multi-jurisdictional collective actions, including European and non-European data subjects.

The data subject may bring proceedings against you as a controller or processor before the courts of the Member State where you are established or the courts of the Member State where the data subject resides.

This choice of forum may lead data subjects to bring individual and class actions in a specific Member State to benefit from differences in national laws. Examples include injury in fact standard, compensatory actions, compensation of material, and non-material damages.

Burden of proof

Under the GDPR, you are responsible for making sure and showing that your processing activities comply with the provisions of the GDPR, as well as with the laws of the Member States that implement the regulation.

You must keep written records of your processing activities and make these records available to the supervisory authority on request. You must also record and document all personal data breaches, and these records must be disclosed on demand to the supervisory authority.

This is why it's vital that you keep records of all measures, actions, and elements likely to prove you comply with the GDPR. You must treat the GDPR's accountability mechanisms as part of your pre-litigation strategy, designed to create documents to show you applied appropriate technical and organizational measures.

Evidence gathering

The GDPR doesn't create a pre-litigation discovery process. Yet it sets out some provisions requiring you to disclose evidence proving you comply with the GDPR. This may enable data subjects to build their case before filing a claim.

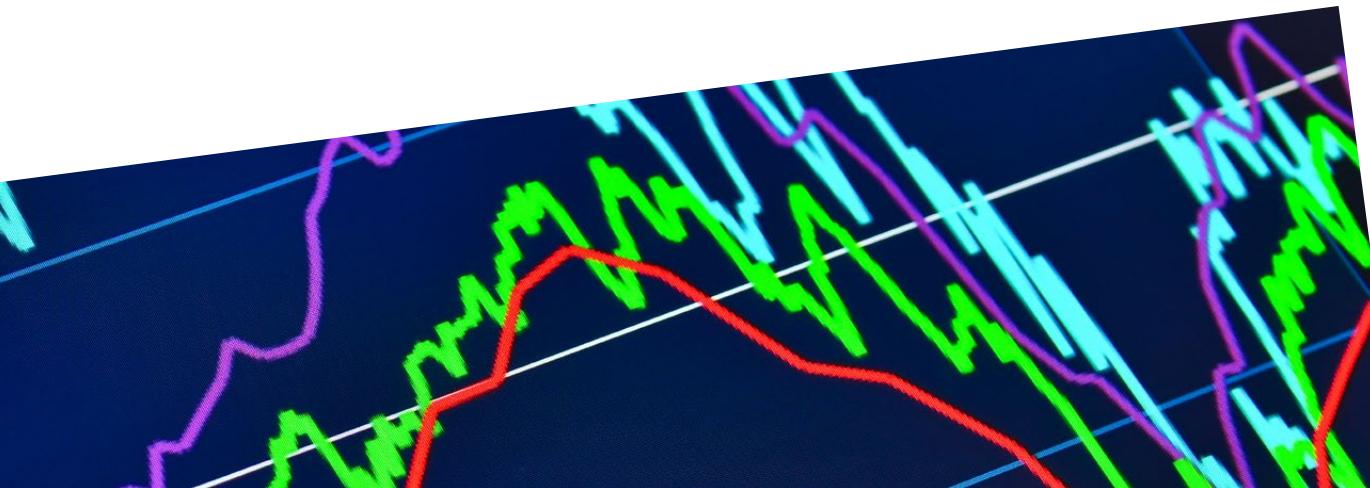
The GDPR provides data subjects with a comprehensive right to access their own personal data through a subject access request. You must respond within one month of the request and give the data subject a copy of all personal data the subject has made available to you.

The GDPR expands the mandatory categories of information that must be supplied in response to a subject access request.

You may refuse to respond to a subject access request if it is "manifestly unfounded or excessive" but you have to prove it is so.

You should be prepared for data subjects to exercise their right to lodge a complaint with a supervisory authority to access the findings of the administrative investigation. It's likely the data subjects will use this information during civil proceedings.

Due to this approach, data subjects can easily create a presumption of a data protection violation, then an even greater administrative burden is placed on you as controller or processor.



What you should do to prepare

The GDPR and the laws that implement it into Member States' national laws (where applicable) have raised the risks of actions seeking collective redress for data breaches or non-compliance with privacy requirements. Of that, there's no doubt.

But there are steps you can take to prepare. As a minimum, you should:

- ✓ Put in place a process to address in good time requests from data subjects.
- ✓ Anticipate that potential plaintiffs will shop around to find the "best" forum, or national courts, to launch data class actions, if you have multiple establishments and subsidiaries and process data across borders.
- ✓ Be able to prove – at any time – that your processing is in line with both the GDPR and the national laws that implement it. You should be able to show you use "appropriate technical and organizational measures" to do so. And you should keep records of all measures, actions, and elements.
- ✓ Design your data processing records with a pre-litigation strategy in mind.
- ✓ Include in your data processing records the measures you implemented for each data subject. To do this, you should establish a system to log individual processing operations so you can prove who had access to any given person's personal data and what actions were taken with it.
- ✓ Bear in mind that potential plaintiffs may use subject access requests and complaints to data protection authorities to help build a litigation case and, in particular, a data class action.

How we can help you

We can:

- Train your teams.
- Implement effective procedures to address requests or claims from data subjects or data protection authorities.
- Help you with investigations and proceedings led by data protection authorities.
- Act for you in data class actions and media crises in Europe and across the globe.

“

All the members of the Hogan Lovells team that I've worked with are outstanding... Their strengths are global reach and expertise in privacy.

”

Our team

Our integrated, cross-border team has developed practical solutions to pan-European and global issues.

We've advised many clients on complying with the GDPR, and we continue to help them anticipate and minimize the risks of data breach litigation. We're also advising on the first data-related investigations and litigations launched since the application of the GDPR. We have extensive experience in data-related investigations and class actions in the United States and beyond.



Christine Gateau
Partner, Paris
T +33 1 53 67 47 47
christine.gateau@hoganlovells.com



Matthias Schweiger
Partner, Munich
T +49 89 290 12 0
matthias.schweiger@hoganlovells.com



Marek Wroniak
Senior Counsel, Warsaw
T +48 22 529 29 00
marek.wroniak@hoganlovells.com



Patrice Navarro
Partner, Paris
T +33 1 53 67 47 47
patrice.navarro@hoganlovells.com



Martin Strauch
Counsel, Munich
T +49 89 290 12 0
martin.strauch@hoganlovells.com



Ewa Kacperek
Counsel, Warsaw
T +48 22 529 29 00
ewa.kacperek@hoganlovells.com



Pauline Faron
Senior Associate, Paris
T +33 1 53 67 47 47
pauline.faron@hoganlovells.com



Christian Di Mauro
Partner, Milan
T +39 027202521
christian.dimauro@hoganlovells.com



Gonzalo Gallego
Partner, Madrid
T +34 91 349 82 00
gonzalo.gallego@hoganlovells.com



Dr. Stefan Schuppert, LL.M. (Harvard)
Managing Partner for Germany, Munich
T +49 89 290 12 0
stefan.schuppert@hoganlovells.com



Massimiliano Masnada
Partner, Rome
T +39 06 6758 2342
massimiliano.masnada@hoganlovells.com



Jose Luis Huerta
Partner, Madrid
T +34 91 349 82 66
joseluis.huerta@hoganlovells.com



Martin Pflüger
Partner, Munich
T +49 89 290 12 0
martin.pflueger@hoganlovells.com



Joke Bodewits
Partner, Amsterdam
T +31 20 55 33 645
joke.bodewits@hoganlovells.com



Nicola Fulford
Partner, London
T +44 20 7296 298
nicola.fulford@hoganlovells.com



Detlef Hass
Partner, Munich
T +49 89 290 12 0
detlef.hass@hoganlovells.com



Manon Cordewener
Office Managing Partner, Amsterdam
T +31 20 55 33 691
manon.cordewener@hoganlovells.com



Ivan Shiu
Partner, London
T +44 20 7296 2834
ivan.shiu@hoganlovells.com

Our team



Eduardo Ustaran
Partner, London
T +44 20 7296 2000
eduardo.ustaran@hoganlovells.com



Natalia Gulyaeva
Office Managing Partner, Moscow
T +7 495 933 3025
natalia.gulyaeva@hoganlovells.com



Omar Guerrero
Office Managing Partner, Mexico
T +52 55 5091 0162
omar.guerrero@hoganlovells.com



Valerie Kenyon
Partner, London
T +44 20 7296 5521
valerie.kenyon@hoganlovells.com



Alexei Dudko
Partner, Moscow
T +7 495 933 3015
alexei.dudko@hoganlovells.com



Jorge Valdés King
Partner, Mexico
T +52 55 50 91 01 60
jorge.valdes@hoganlovells.com



Matthew Felwick
Partner, London
T +44 20 7296 2000
matthew.felwick@hoganlovells.com



Michelle Kisloff
Partner, Washington
T +1 202 637 6631
micelle.kisloff@hoganlovells.com



Mark Parsons
Partner, Hong Kong
T +852 2840 5033
mark.parsons@hoganlovells.com



Arwen Handley
Partner, London
T +44 20 7296 2810
arwen.handley@hoganlovells.com



Adam Cooke
Counsel, Washington
T +1 202 637 5479
adam.a.cooke@hoganlovells.com



Byron Phillips
Counsel, Hong Kong
T +852 2840 5960
byron.phillips@hoganlovells.com

01

Focus on...

Who can start and join data class actions?

Article 80 of the GDPR defines the type of legal entity that is entitled to exercise the data subject's rights on their behalf:

Not-for-profit bodies, organizations or associations whose statutory objectives are in the public interest, and which are active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data.

Standing and other procedural questions on admissibility of the action

The GDPR doesn't set the procedural framework of data class actions; instead, it leaves it to the Member States to provide an actionable tool. So, you must refer to the national laws that apply, if any, which set the national legal criteria to bring a data class action.

It is essential you check whether the entity leading the collective action has adequate standing, meets the national legal criteria, and complies with the procedural rules.



Spotlight on France

The [French Data Protection Act](#) provides that only three types of associations have the capacity to bring a data class action:

- Associations duly declared for at least five years, the corporate purpose of which is the protection of privacy and personal data.
- Consumer associations representative at national level and authorized under Article L. 811-1 of the French Consumer Code, when the data processing at stake affects consumers.
- Employees or civil servants trade unions representative under the French Labor Code, when the processing at stake affects the interests of individuals that the by-laws of these organizations entrust them to defend.

French law compels qualified associations to send a formal notice to data controllers at least four months before starting a lawsuit. This four-month period is designed to enable the parties to try to find an amicable solution. In that respect, it is provided that associations can take part in mediation processes. Associations cannot start a class action before the end of the four months.



Spotlight on Germany

Germany has two mechanisms to bring collective actions under the GDPR. Neither are class actions nor group actions but representative actions with the goal to enable collective relief or redress.

First, representative actions, which can only achieve cease-and-desist measures (*Unterlassungsklagen*). Second, another type of representative action with the goal of achieving a binding declaration on factual or legal prerequisites for consumer claims (*Musterfeststellungsklage*). The latter is unusual in that consumers can register their claims about the action and make the declaratory judgment binding for their own case.

The *Musterfeststellungsklage* doesn't provide for a ruling on compensation in money and therefore its scope would mainly be the assessment of whether there is a breach of the GDPR or the German *Bundesdatenschutzgesetz*. A declaratory judgment on a breach may lead to further actions for compensation in money by the consumers who registered the representative action, invoking the content and binding effect of the declaratory ruling. Of course, actions from unrelated consumers who claim an infringement of their rights are also possible. But these consumers cannot rely on the declaratory judgment by law.

Both representative actions must be brought by qualified entities, many of which are specialized consumer associations (*Verbraucherschutzverbände*). To have standing to bring a *Musterfeststellungsklage*, stricter requirements must be met by the qualified entity, for example their non-profit status. There are few requirements – and no costs – for consumers who want to register their claims, except some formalities.

So far this vehicle has not been used for a data class action and the current mechanism may become obsolete in the light of the Directive on representative actions for the protection of the collective interests of consumers.

The *Musterfeststellungsklage* doesn't provide for a ruling on compensation in money and therefore its scope would mainly be the assessment of whether there is a breach of the GDPR or the German *Bundesdatenschutzgesetz*.



Spotlight on the Netherlands

On 1 January 2020, the new Collective Damages Actions (called the “WAMCA”) came into force in the Netherlands. The WAMCA introduces an option to claim monetary damages in a U.S.-style class action for any type of claim, including claims relating to violations of the GDPR. The WAMCA includes enhanced standing and admissibility requirements (e.g., governance, funding, representation, previous experience/track record) for collective action organizations, which will be assessed at an early stage of the proceedings (comparable to the United States’ motion to dismiss).

One of the admissibility requirements is that the action must have a sufficiently close connection with the Dutch jurisdiction – the so-called scope rule. For example:

- If most of the affected individuals for whom the collective action is initiated reside in the Netherlands.
- If the controller or processor is established in the Netherlands, provided that other circumstances also point to a connection with the Dutch legal sphere.
- If the processing that resulted in the violation of the GDPR took place in the Netherlands.



Spotlight on Spain

The [legislation](#) doesn't develop Article 80 of the GDPR, as it focuses on administrative proceedings before the Spanish Supervisory Authority. In Spain, consumers and users associations can defend the rights and interests of their members, the association itself, and the general interest of consumers and users before courts and judges. How they bring such actions, and the consequences arising from them, depend on whether the consumers and users form part of a group in which each can be perfectly or easily identified:

- Where they can be identified, these associations (as well as the entities legally formed to protect their interests, and the group itself) may protect and defend their collective interests.
- Where there is an undetermined plurality of consumers and users or it is difficult to determine them, the only ones who can defend these “vague” interests are the consumers and users associations legally deemed representative.



In Spain, consumers and users associations can defend the rights and interests of their members, the association itself, and the general interest of consumers and users before courts and judges.



Spotlight on the United Kingdom

The [UK Data Protection Act \(DPA\) 2018](#), which entered into force on 23 May 2018, states that a body or other organization that meets the conditions set out in Article 80 of the GDPR may be authorized to exercise the data subject's rights as set out in the GDPR. This includes the right to lodge a complaint against a supervisory authority, to obtain an effective judicial remedy, and to claim for compensation, including for both material or non-material damage. The DPA 2018 doesn't introduce any additional conditions that the body or other organization must meet to have this representative capacity.

The DPA 2018 includes a provision for the Secretary of State to introduce specific regulations to deal with collective proceedings brought by representative bodies under the GDPR and with, for example, the effect of judgments and orders, and an assessment of the amount of compensation to be paid. These regulations have not yet been introduced. For now, the DPA 2018 specifies that court proceedings for exercising the right to receive compensation brought by a representative body for a person should be brought "in accordance with the rules of the court". The expectation for now remains that GDPR-related class actions in the United Kingdom will also be brought under existing national procedural frameworks.

Under existing UK Civil Procedure Rules, there are a number of ways litigation can involve multiple claimants

These include:

- Claims by more than one claimant managed together under the courts' case management powers under the Civil Procedure Rules.
 - Group Litigation Orders (GLOs), where more than one claimant has a cause of action giving rise to "common or related issues of fact or law", and these cases are grouped and managed together.
 - Claims by representative claimants where more than one person has the "same interest" in a claim

What constitutes the same interest is a high bar: the UK High Court has held that the class must have a common interest or grievance and seek relief that is beneficial to all. The standard of commonality required for a GLO is considered less difficult to meet, as the interests do not need to be identical.

Neither mechanism specifies a maximum number of claimants that is required for the action to proceed, though each requires a minimum of two.

Note: in order to allow for the continuing application of the EU data protection regime in the UK after Brexit, the UK government has incorporated the GDPR into UK law as a newly titled “UK GDPR”. This UK GDPR operates alongside the UK’s Data Protection Act 2018. The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 made the necessary amendments required to allow these laws to operate within a “UK only” context. The majority of the amendments came into force at the end of the Brexit transition period.

For a full analysis of data privacy and Brexit please visit [Hogan Lovells Brexit Hub](#).



Spotlight on Russia

Since 1 October 2019, according to amendments to the Russian Civil Procedural Code, a group of citizens or organizations are entitled to file a joint action with the Russian court of general jurisdiction.

The following conditions shall be simultaneously met to consider a claim as joint action:

- There is a common defendant with respect to each member of the group of plaintiffs.
 - The subject of the dispute constitutes common or similar rights and legitimate interests of the members of the group.
 - The rights of members of the group and obligations of the defendant are based on similar circumstances.
 - All members of the group use the same remedy to protect their rights. The group shall consist of at least 20 members as of the date of filing of the court claim.

```
verse(); b = m(a, " "); -1 < b &&
, void 0); -1 < b && a.splice(b, 1);
&& a.splice(b, 1); return a; }
replace(RegExp(", ", "g"), " ");
{ for (var c = 0, d = 0;d < b.length;
c++; } return c; } function m(a,
d = 0;d < a.length;d++) { if (a[d] ==
c) { } } function s() { }
```



Spotlight on the United States

An individual consumer can bring a class action in the United States. No associations or organizations are necessary to assert claims on behalf of individual consumers.

To pursue claims on a class basis in federal court, the individual must show that they have standing to pursue the action. Standing requires, at a minimum, that the individual has suffered a concrete injury fairly traceable to the defendants' conduct and that this injury can be redressed by a court. In recent years, U.S. courts have issued many decisions – not all consistent – about what constitutes a concrete injury in cases involving data breaches and data practices.

The individual also must satisfy the procedural rules that govern class actions. To do so, they must show, among other things, that their claims are typical of other proposed class members' claims, that there are common questions of law or fact across the proposed class, and that they will fairly and adequately represent the proposed class.



Spotlight on Mexico

According to Mexico's Federal Code of Civil Procedure, the following persons or entities have standing to file a class action:

- Consumer Protection Agency.
- The representative of a class of at least 30 members.
- Association with the corporate purpose of filing such claims.
- Attorney General.

Note that the Mexican Data Protection Authority doesn't have standing to start a data class action.

While the Financial Services' Users Protection Agency and the Antitrust Agency have standing to file class actions, it is not clear if they have the authority over data related matters.



Spotlight on Hong Kong

In May 2012, the Law Reform Commission of Hong Kong (LRC) published its report on class actions. It recommends the introduction, under an incremental approach, of a class action regime, following which the Department of Justice of the Hong Kong Special Administrative Region established a cross-sector working group to study and consider the LRC's recommendations.

On 17 April 2019, the Department of Justice stated that it had (at that date) held 25 meetings since its inception while a subcommittee set up under the working group had met 30 times.

The working group's current position is that time is required for more in-depth analysis, including of the proposed definition of "consumer cases", certification criteria for a class action to be adopted by the Hong Kong courts, the design of the procedural rules, and other ancillary measures.

A draft public consultation document is being compiled, although there is no definitive timetable yet for consultation.

In the meantime, the only type of collective actions available to plaintiffs in Hong Kong is representative proceedings under Order 15 Rule 12 of the Rules of the High Court. Where numerous persons have the same interest (a "common interest and grievance" (Pan Atlantic Insurance Co. and Republic Insurance v Pine Top Insurance Co [1989] 1 Lloyd's Rep 568)) in any proceedings, the proceedings may be begun and, unless the court otherwise orders, continued, by or against any one or more of them as representing any or all of them.

Opt-in or opt-out

Class actions may either be initiated on an opt-in or an opt-out basis. In the opt-in system, individuals must proactively join the class. In contrast, the opt-out system means that all individuals within the class definition are considered part of the action unless they exclude themselves from the class.

The GDPR doesn't impose an opt-in or opt-out system. So, there are a variety of systems within the Member States that have implemented data class actions into their national laws. This issue is also relevant for the effects of a settlement during the class action.



Spotlight on France

The French legislator chose an opt-in mechanism. Once the decision ruling on liability is final, the court orders the defendant to implement the relevant publicity measures to inform the people who potentially suffered damage of this decision.

Each person looking to join the class to get compensation must either send a notice to the data controller or the association asking for compensation. In this notice, the person must justify that they meet the criteria to join the group. The data controller then compensates the person if they meet the criteria set by the judgment and according to the guidelines set by the judgment, especially the heads of loss, which can give rise to compensation.



Spotlight on Germany

The German *Unterlassungsklage* is a purely representative action for only a cease-and-desist judgment, and there is neither an opt-in nor an opt-out possibility. It is independent of the rights of individuals. There may only be an indication for individual actions regarding the facts assessed in the *Unterlassungsklage*. There is no binding effect, however.

The *Musterfeststellungsklage* is an opt-in regime.

Settlement agreements approved by the court generally bind registered applicants. Other than the action itself, settlements can also provide for compensation.

In contrast, consumers who are not interested in being affected by the settlement agreement are given the opportunity to withdraw from it. The relevant declaration must be made within one month and must be addressed to the competent court. While a withdrawal doesn't affect the consumer's valid registration for the class action, the closed settlement agreement becomes ineffective as soon as more than 30 percent of the registered consumers declare their withdrawal. Because the registration is untouched by a consumer's withdrawal, it results in the limitation of time remaining suspended regarding this individual claim. Eventually, a withdrawing consumer has to file a separate action to pursue their legal interests.



Spotlight on the Netherlands

For the Collective Damages Action (the "WAMCA"), the Dutch legislator chose an opt-out mechanism because, among other reasons, this will create closure for the defendant. It will prevent new collective actions being brought on the same facts and regarding the same legal issues once a collective action has finished.

Initially, the Dutch legislator had international ambitions, and the draft legislation did not limit the size of the opt-out class. If the scope rule was met, the class could consist of international class members. After heavy criticism, the Dutch legislator amended the draft act to limit the class to Dutch class members only, giving foreign class members the opportunity to opt-in. No rule without an exception: on request by one of the parties, the court may also apply the opt-out regime to foreign class members who are "easily identifiable".



Spotlight on Spain

The procedure relies on the advertising duties of the relevant party that brings class actions so that the affected people are aware of the proceeding. Following the distinction above:

- Where consumers and users are identifiable, the consumers and users association must inform each concerned consumer and user.
- Where there is undetermined plurality of consumers and users, a public and general announcement will be carried out, and after a maximum of two months of suspension, the proceeding will continue.

The final ruling will affect all consumers and users whose interests are being claimed. Where a consumer or user opts in and intervenes in the proceeding, the final ruling will expressly give an answer to their claims. There's no opt-out mechanism.

The procedure relies on the advertising duties of the relevant party that brings class actions so that the affected people are aware of the proceeding.



Spotlight on the United Kingdom

The UK legislators chose not to introduce the opt-out mechanism envisaged by Article 80(2) of the GDPR, which would have allowed bodies or organizations to exercise some or all of the data subject's rights under the GDPR without authority from the data subject. However, and following pressure from campaigners when the draft UK legislation was debated, the UK Data Protection Act (DPA) 2018 does require the UK government to review and report on the merits of enabling bodies or other organizations to have this power, by November 2020. Accordingly, the Department for Digital Culture, Media and Sport ran a consultation calling for views from August to October 2020. The results of this government consultation are currently awaited. Until such time as any changes are proposed, the DPA 2018 allows for the representation of data subjects only with their authority.

This is broadly consistent with existing mechanisms for class actions available in the United Kingdom. The Group Litigation Order is a pure opt-in mechanism, requiring the existence of two or more identifiable claimants who have issued their own separate claims. Representative actions may be brought as opt-out proceedings where a representative can establish that additional class members who may not have provided their authority satisfy the "same interest" test. However, this is a high hurdle and UK courts have been historically reluctant to admit representative actions when they are brought in an opt-out manner, though this may be set to shift following recent data privacy decisions. In [Lloyd v Google \[2019\] EWCA Civ 1599](#), a claim brought under the United Kingdom's pre-GDPR data protection regime, the Court of Appeal held that on the facts of the case the same interest test could be satisfied across an alleged class membership of 4.4 million individuals, and there was no requirement for the members to have opted in to the action. The defendant was granted permission to appeal to the Supreme Court and the resulting judgment, expected in the first half of 2021, is anticipated to provide welcome clarity on the availability and appropriateness of opt-out style representative actions as a response to mass data breaches in the United Kingdom.

Meanwhile, encouraged by the Court of Appeal's decision, claimant solicitors have been quick to initiate new representative actions. In *Atkinson v Equifax Ltd* in which the Hogan Lovells Data Class Action team represented Equifax, the complaint on behalf of a purported class of 15 million individuals concerned perceived data breaches occurring as a result of large-scale cyber-attacks. The claim was subsequently withdrawn as a representative action. More recently in November 2020, a UK consumer privacy activists' claim against Oracle and Salesforce alleging their misuse of user data has been reportedly stayed pending the outcome of the Supreme Court's decision in *Lloyd*.

For completeness, the United Kingdom does have a true national procedural opt-out mechanism for class actions but this is currently limited to antitrust infringements brought before the Competition Appeals Tribunal.



Spotlight on Russia

Once the court accepts the claim for consideration, the person who handles the case for the class must make information about the claim publicly available. New plaintiffs may join the class before the court starts the hearing of arguments.



Spotlight on the United States

Federal courts in the United States follow an opt-out system for most data class actions. All individuals who fall within the definition of the class are members of, and included in, the class unless they exclude themselves. Notice is provided to class members, which explains the nature of the action, the ability of individuals to opt out of the class, and the effect of not opting out of the class. While opt-out class actions increase litigation exposure for companies, in the settlement context, they provide a mechanism of achieving global peace.

Who can join and when?

The GDPR is silent on this issue. The answer depends on the law of the Member State.



Spotlight on Mexico

Mexico adopted an opt-in system. Members of the class can join the data class action at any point during the procedure. Also, they can join the action within 18 months after the final decision is issued, or 18 months after a settlement agreement is reached. Members only need to express their intention to join the class action to the representative of the class by any means.



Spotlight on Germany

In case of a *Musterfeststellungsklage*, individuals who are consumers cannot become a party to the action. But they can join their legal relationship to the action by registering their claim against the defendant via the litigation register set up by the Federal Office of Justice. Registration suspends the limitation period for the consumer and makes the judgment binding in a follow-up action by the individual against the same defendant. Registration also brings the individual within the scope of a potential court-approved settlement. Where the individual had brought an action against the same defendant, this action will be stayed once they register to the *Musterfeststellungsklage*.

Individuals can register their claims from the first publication of the *Musterfeststellungsklage* in the litigation register until the end of the first day before the first hearing. The registration can be withdrawn until the end of the first day of the oral hearing.

Non-consumers cannot register claims with the litigation register. But a plaintiff who is not a consumer can move for a stay of proceedings where the decision in their legal dispute depends on the subject matter of a *Musterfeststellungsklage*. In case the court, seized by the non-consumer, anticipates that its ruling depends on the *Musterfeststellungsklage*, it can grant a stay of proceedings until the *Musterfeststellungsklage* has been dealt with and terminated.



Spotlight on France

Based on provisions of the French Data Protection Act, only individuals, not legal persons, may join the class.



Spotlight on Italy

The Italian class action reform was supposed to come into force in April 2020. However, also due to the Covid-19 pandemic, its entry into force has been postponed to 19 May 2021. Such reform has a new, interesting regime as to who can join and when.

First, in the reformed class action rules, there's no reference to "consumers and users", as in the current class action rules. This makes the new class action mechanism able to protect a wider range of rights beyond compensation for damages suffered by consumers from, for example, unfair competition, unfair commercial practices, consumer contracts, and so on.

Second, the class action reform provides a double opt-in window. The Italian class action is a two-tier procedure. First, the court decides whether the action is admissible, and then, only if it is, rules on the merits of the claim. Under the new class action law, claimants who opt-in may join the class either after the first decision admitting the class action or after the court has handed down the decision on the merits.

In this scenario, businesses are exposed to higher risks. Not only does the new law offer a wider spectrum of possible claims, but it allows claimants to join a class action even after a favorable decision is issued on the merits of the plaintiff's claim.



Spotlight on the Netherlands

In the Netherlands, a collective (damages) action organization can represent the interests of both private individuals and legal entities.



Spotlight on Spain

Where consumers and users are identifiable, they may join at any time after being notified. Where they are part of an undermined group, they may join only by responding to the announcement in due time.



Spotlight on Russia

To join a joint action, a person or organization must apply in writing to the person handling the action, if they would like to join an action that has not been filed with the court. Or if a joint action has been filed, they must apply to the court.



Spotlight on the United Kingdom

Data subjects are defined within the GDPR as identifiable natural persons; the UK DPA 2018 follows this definition. Accordingly, the collective proceedings envisioned by the UK regime are limited to individuals, not legal persons.

Claims proceeding on the basis of a Group Litigation Order (GLO) require each claimant to start individual proceedings. On direction of the court, a group register is established onto which claims issued by individual claimants can be entered. This register is generally required to be made public to efficiently identify and manage all relevant claims. The court may specify a deadline after which no claim may be added to the group register without permission. A party joining the group register will be bound by any judgment or order made on the issues of fact or law common to the group unless the court rules otherwise. Claimants may also apply to be removed from the register, in which case they will not be bound by the judgment.

A representative action may be commenced by one or more persons as representatives of any others who have the “same interest” in the claim. As the representative action proceeds on an “opt-out” basis, the parties represented do not need to be joined as parties to the action or even identified on an individual basis at the outset of the action. However, at all stages of the proceedings it must be possible to say of any particular person whether or not they would qualify for membership of the represented class by virtue of having the “same interest”. Unless the court expressly orders otherwise, any judgment or order made will be binding upon all represented persons.

One of the first data privacy dispute heard by the English courts using a collective action mechanism (a GLO) was *Various claimants v Wm Morrisons Supermarket PLC [2017] EWHC 3113 (QB)*. This was brought under the previous data protection regime in the United Kingdom, the Data Protection Act 1998. In that claim, over 9,000 employees (the claimants in the action) were successful in arguing before the High Court that Morrisons should be held vicariously liable for its employee’s misuse of data. This was despite the supermarket having taken preventative measures to prevent the data misuse, and despite the rogue employee’s intention to harm his employer. Although the Court of Appeal followed the lower court’s decision, in April 2020 the Supreme Court disagreed: holding in a landmark judgment that Morrisons should not be held liable for damages following the deliberate act of a rogue employee, where the disclosures made were not within the “field of activities” assigned to that employee. However, the Supreme Court did go on to indicate that employers may, in principle, still be vicariously liable for breaches of data protection legislation where their employees are data controllers in their own right, which makes the decision only of limited comfort for companies that experience a data security breach.

02

Focus on...

Combination of regulatory inquiries and data class actions

Coordination of court proceedings with other enforcement actions

Data class action proceedings before national courts can be initiated in parallel to, or just after, a complaint lodged with data protection authorities, investigations initiated by data protection authorities, or both.

The GDPR provides for a system of suspension of proceedings in case of concurrent actions launched before courts in several Member States. In contrast, it doesn't provide for a formal mechanism of coordination of the court proceedings with a concurrent action launched before a data protection authority.

Where a class action was initiated and based on the sanction potentially issued by a data protection authority, it may be possible to request the national court seized of the class action to order a stay of proceedings until the sanction decision is final. The chances of getting a stay of proceedings in this case would depend on the national laws and case law that apply. Also, plaintiffs may object to the request for a stay of proceedings, arguing that the data protection authority, the most competent body to assess potential non-compliances with the GDPR, has identified non-compliances.

Do not underestimate the consequences of the decisions issued by data protection authorities

Some elements requested and produced in administrative investigations may be reproduced or mentioned in the decision issued by the data protection authority. These elements may then be used by plaintiffs in the scope of a data class action. So, you should expect the findings of administrative investigations to work as a pre-litigation discovery process favorable to plaintiffs.

Plaintiffs may base their data class action on the decision issued by the data protection authority of another Member State. This is likely since the GDPR is implemented, and should be applied, evenly in the Member States.

Also, several data class actions in various countries may be based on a single decision handed down by a national data protection authority.

Consequently, a decision by a national data protection authority may have devastating and cross-border effects outside the Member State. This is because plaintiffs elsewhere may base their data class action on this decision.

A coherent and harmonized interpretation of the GDPR is of utmost importance. In this respect, the European Data Protection Board plays an important role by issuing guidelines, recommendations, and best practices.

Another important tool to prevent potential abuses or deviations of a national data protection authority is the cooperation mechanism, even though it may prove underdeveloped and not sufficiently effective in practice.

Keep in mind: when you receive an inquiry from a data protection authority, it's important that you respond and defend as quickly and effectively as you would in proceedings before courts, such as antitrust proceedings. The inquiry may have cross-border consequences.





Spotlight on Germany

Germany has two mechanisms to bring collective actions under the GDPR. Neither are class actions nor group actions but representative actions with the goal to enable collective relief or redress. First, representative actions for cease-and-desist measures (*Unterlassungsklagen*), which can only achieve cease-and-desist measures. Second, another type of representative action with the goal of achieving a binding declaration on factual or legal prerequisites for consumer claims (*Musterfeststellungsklage*).

German civil procedure doesn't allow a court to suspend actions based on data breaches in case of concurrent inquiries of data protection authorities, at least not without the consent of both parties. This is because findings of the data protection authorities have no legally binding effect on the courts. But in regard to *Unterlassungsklagen*, courts are required to consult national data protection authorities before reaching their decisions. This is supposed to ensure coherency between the data protection authorities' findings and the courts' rulings. As a result, claimants might not bring the data class actions before the end of the data protection authorities' inquiries.

Article 15 of the GDPR provides the data subject with a broad right to access. This right to access can collide with confidentiality agreements and privileges, for example attorney-client privilege. Article 15 doesn't explicitly stipulate an exception for privileged information, in contrast to Article 14 §5d). But §203 of the German Penal Code, which, among other things, penalizes the violation of private secrets by an attorney, also applies to Article 15 of the GDPR. It renders the right of access of the data subject inapplicable whenever privileged information is concerned.



Spotlight on the United States

Data class actions are independent of, and proceed in parallel with, government enforcement actions at federal and state levels. No formal system exists for coordination.

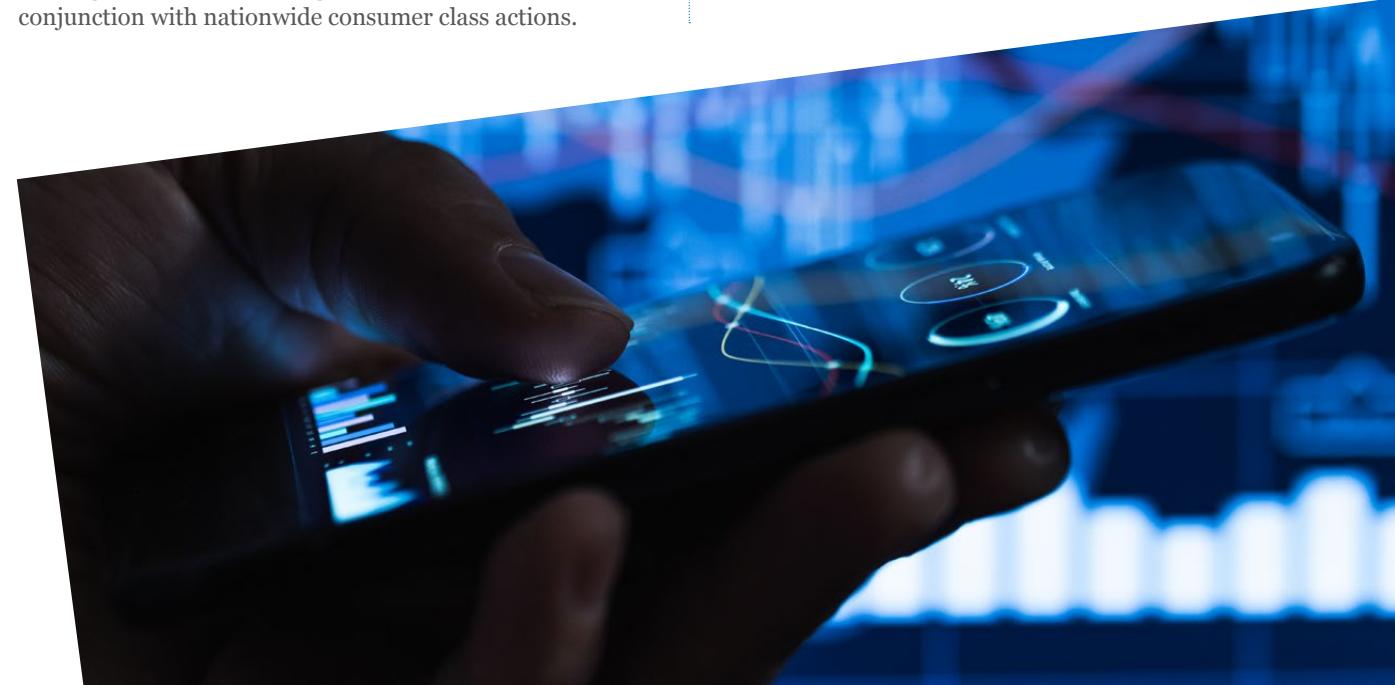
Because class actions and regulatory enforcement proceed independently, findings in one action can have a broader impact. Adverse findings of a government investigation, for example, can prompt the filing of a class action suit or can be used by plaintiffs in an existing class action suit. Resolution of one action through settlement or judgment also could affect the viability or scope of an overlapping, parallel action. A settlement reached in a government proceeding that provides redress to consumers, for example, may limit a class action seeking relief for the same consumers.

Despite independent tracks, in the settlement context, there may be opportunities to coordinate class action and regulatory resolutions. For example, a company recently resolved several federal and state regulatory investigations related to a significant data breach in conjunction with nationwide consumer class actions.



Spotlight on Mexico

Data class actions are independent of any administrative proceeding started before or by the data protection authority, so both procedures could be conducted in parallel. A resolution issued by the data protection authority finding the controller or processor responsible for breaching its data protection obligations is not necessary to start a data class action. But lack of such decision may affect the court psyche.



03

Focus on...

Monetary compensation vs. injunction in data class actions

Compensation for damages

Under the GDPR, data subjects have the right to recover both material and non-material damages. So, in the event of liability, all damages caused by the data protection infringement have to be compensated. This extended liability is remarkably different from the current legal situation under many Member States' data protection laws.

The GDPR doesn't set out any criteria to assess the recoverable damage and leaves this to the national laws that apply. So, Member States use their own national standards to determine whether hypothetical, future, or even anxiety damage may be compensable, for example.

Compensatory actions vs. injunctive actions

Some Member States have created injunctive data class actions only, with no possibility for individual or collective compensation. In contrast, others have introduced compensatory data class actions.

Given the diversity of procedural rules in Member States and the GDPR's broad territorial scope, we can expect plaintiffs to conduct forum-shopping to find the best national courts for launching data class actions. In particular, your being headquartered in a country where compensatory class actions do not exist is no longer a protection. Collective actions can be brought in other Member States to seek damages under local procedural rules.



Spotlight on France

The data class action may be used to end an infringement of the provisions governing the protection of personal data. The law used to expressly specify that this class action could not give rise to compensation in the form of damages. Yet this changed with the enactment of the bill implementing the GDPR into French law, which created a compensatory data class action for damages that occurred after 24 May 2018. Both types of French data class actions are subject to the same regime, which can be found in Law no. 2026-1547 of 18 November 2016 on 21st-century justice. This sets out a general framework for class actions and specific provisions for class actions aimed at compensating a damage. Both are regulated by the same provision of the revised French Data Protection Law.

In addition to this double-sided class action scheme, the revised French Data Protection Law implements Article 80 of the GDPR. It enables data subjects to mandate associations to exercise their rights and/or bring a complaint before the French Data Protection Authority or court proceedings before the relevant court. The right to compensation provided by Article 82 of the GDPR is included in the scope of mandates data subjects can grant to associations.

In a nutshell, French law now allows all types of actions contemplated in the GDPR: both representative collective actions and class actions, with a possibility in each case to claim damages. As a result, associations may choose whichever procedural regime they find most convenient.

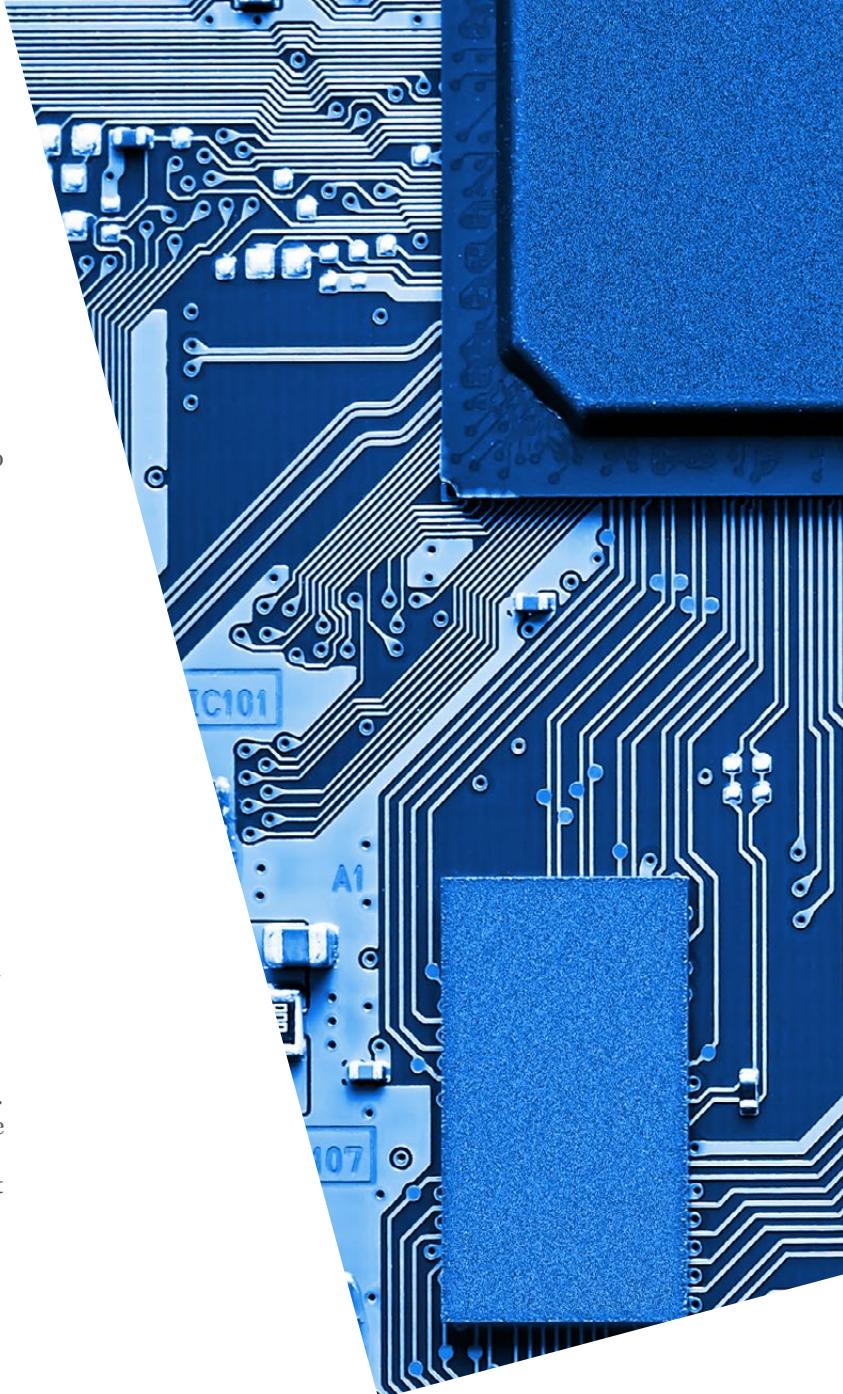


Spotlight on Germany

Germany allows for injunctions (cease-and-desist measures) in case of data breaches. They cannot be enforced by a class or group action but by representative action. The representative action must be brought by registered qualified entities.

Some of these qualified entities also have standing to bring a representative action with the goal of achieving a binding declaration on factual or legal prerequisites for consumer claims (*Musterfeststellungsklage*). The *Musterfeststellungsklage*, however, doesn't provide for a ruling on compensation in money and therefore its scope would mainly be the assessment of whether there is a breach of the GDPR or the German *Bundesdatenschutzgesetz*. The declaration may pertain to factual or legal elements. A declaratory judgment on a breach may lead to further actions for monetary compensation by the consumers who registered for the representative action, invoking the content and binding effect of the declaratory ruling.

In short, German law currently doesn't allow all types of actions contemplated in the GDPR: there is no possibility to enforce damages claims by way of class or group action. As a result, qualified entities with standing to sue may for now only bring a *Musterfeststellungsklage* for a declaratory ruling on prerequisites of civil claims of consumers. To date consumer claims for compensation because of infringement of rights under the GDPR – which already have become a reality in Germany – are not brought by collective action. The implementation of the Directive on representative actions for the protection of the collective interest of consumers will change this situation.





Spotlight on the Netherlands

In the Netherlands, injunctive relief for breaches of the GDPR can be obtained in a representative collective action. Here, a representative entity, a Dutch Vereniging or Stichting, initiates proceedings to protect similar interests of injured parties (being private individuals, legal entities, or both).

In addition, with the introduction of the new Collective Damages Action (the “WAMCA”), it is now possible to claim monetary damages in a U.S.-style class action for any type of claim. This includes for damages suffered as a result of violation of the GDPR. Claimants in the new Collective Damages Action will be (a) representative entity or entities, who can file a claim on behalf of consumers or business. The action can either result in a judgment in which the court will award damages or in a collective settlement held to be binding by the court, both on an opt-out basis. The class will in principle be limited to Dutch members only, albeit the Court can decide that the opt-out regime will also apply to foreign class members provided they are “easily identifiable”. In addition, foreign class members can voluntarily opt-in.

This new and unique class action mechanism is likely to increase the attractiveness of the Netherlands as a forum for personal data class actions.



Spotlight on Poland

If infringement of the provisions on personal data amounts to a tort, the claims available under the Act of 17 December 2009 for group proceedings consist of both compensation and injunctive relief. In practice, though, seeking compensation in group proceedings is often difficult. This is mainly due to difficulties in establishing and unifying the amount of compensation claimed by individual members of the group.

As yet, there are no associations representing individuals in class actions related to the infringement of the provisions governing the protection of personal data in Poland. Also, there have been no group proceedings to date.



Spotlight on Spain

Civil Procedure laws, which regulate this kind of action in the absence of specific rules under the Spanish Data Protection Act, allow consumers and users associations or groups to pursue both injunctive and compensatory actions.

However, claimants not looking for compensation generally go to the Spanish Data Protection Authority so that an administrative sanctioning proceeding is opened.

That said, it's important to note that, in practice, it is common for consumer associations to file claims with the Spanish Data Protection Authority.



Spotlight on the United Kingdom

The [UK Data Protection Act \(DPA\) 2018](#), which entered into force on 23 May 2018, implements Article 80 of the GDPR. It enables data subjects to authorize a body or other organization to exercise their rights to lodge a complaint against a supervisory authority, and to an effective judicial remedy. This includes exercise of the data subject's rights to compensation for material or non-material damages.

The UK legislators additionally sought to clarify the interpretation of “non-material damages” for the purposes of breaches of the GDPR. The DPA 2018 specifies that non-material damage includes distress.

The UK courts have previously analyzed the interpretation of non-material damages in data-related class actions. The existing decisions that arose under pre-GDPR UK data protection regimes will remain relevant to future claims under the GDPR. In particular, in *Vidal-Hall v Google* [2015] EWCA Civ 311 the Court of Appeal held that claimants affected by sufficiently serious data breaches may recover damages for distress and anxiety even in the absence of their having sustained any financial loss. As such this decision foreshadowed the principle of damages now set out in the DPA 2018. Meanwhile, in *Lloyd v Google* [2019] EWCA Civ 1599 the Court of Appeal held that where the breach in question is sufficiently serious, claimants may recover damages for loss of control over their data without proving financial loss or distress. The Supreme Court’s ruling on this case (expected in the first half of 2021) should provide further clarity on these matters.

In the absence of specific rules to the contrary, there should be no limit to the type of relief available for proceedings linked to contravention of the GDPR apart from those under UK law generally. Existing civil procedure in the United Kingdom allows claimants to seek both damages and injunctive relief as remedies where appropriate. Injunctions may additionally be sought as a form of interim relief.

Note: in order to allow for the continuing application of the EU data protection regime in the UK after Brexit, the UK government intends to incorporate the GDPR into UK law as a newly titled “UK GDPR”. This UK GDPR will operate alongside the UK’s existing Data Protection Act 2018, and the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 make the necessary amendments required to allow these laws to operate within a “UK only” context. The majority of the amendments are stipulated to come into force at the end of the Brexit transition period (currently anticipated to be 11pm on 31 December 2020).

For a full analysis of data privacy and Brexit, please visit [Hogan Lovells Brexit Hub](#).



Spotlight on Russia

In a joint action, plaintiffs may claim monetary compensation and/or ask for termination of misuses. But all the plaintiffs must use the same remedy. The plaintiffs choose the method to calculate and prove the alleged damages and/or moral harm. All the evidence and explanations are considered by the court, which decides on the final amount of the compensation.

In its ruling, the court must provide a separate conclusion for each member of the group of plaintiffs.

Russian courts rarely grant preliminary injunctions, and in joint actions the chances are also low.



Spotlight on the United States

Consumers can pursue both monetary and injunctive relief. Federal Rule of Civil Procedure 23, which governs class actions in federal courts, enables recovery of both in a single action. Plaintiffs litigating data class actions often pursue monetary and injunctive relief at the same time, and many resolutions have included both forms of relief.



Spotlight on Mexico

The class has the right to seek compensation for material and non-material damages, as well as injunctive remedies. It depends on the type of class action filed. Diffuse class actions (where the class is not determined, and the class is the holder of the right) give place only to injunctive remedies. Strict class actions (where the class is determined or can be determined, and the class is the holder of the right) give place to injunctive remedies and monetary compensations for material and non-material damages.

Homogeneous individual class actions (individuals that share common circumstance are the holders of the right) give place to injunctive remedies and seek the specific performance of a contract or its rescission.

For strict class actions and individual class actions, single members of the class must file an ancillary proceeding to quantify its compensation.



Alicante	Milan
Amsterdam	Minneapolis
Baltimore	Monterrey
Beijing	Moscow
Birmingham	Munich
Boston	New York
Brussels	Northern Virginia
Budapest*	Paris
Colorado Springs	Perth
Denver	Philadelphia
Dubai	Riyadh*
Dublin	Rome
Dusseldorf	San Francisco
Frankfurt	Sao Paulo
Hamburg	Shanghai
Hanoi	Shanghai FTZ*
Ho Chi Minh City	Silicon Valley
Hong Kong	Singapore
Houston	Sydney
Jakarta*	Tokyo
Johannesburg	Ulaanbaatar*
London	Warsaw
Los Angeles	Washington, D.C.
Louisville	Zagreb*
Luxembourg	
Madrid	
Mexico City	* Our associated offices
Miami	Legal Services Centre: Berlin

www.hoganlovells.com

"Hogan Lovells" or the "firm" is an international legal practice that includes Hogan Lovells International LLP, Hogan Lovells US LLP and their affiliated businesses.

The word "partner" is used to describe a partner or member of Hogan Lovells International LLP, Hogan Lovells US LLP or any of their affiliated entities or any employee or consultant with equivalent standing. Certain individuals, who are designated as partners, but who are not members of Hogan Lovells International LLP, do not hold qualifications equivalent to members.

For more information about Hogan Lovells, the partners and their qualifications, see www.hoganlovells.com.

Where case studies are included, results achieved do not guarantee similar outcomes for other clients. Attorney advertising. Images of people may feature current or former lawyers and employees at Hogan Lovells or models not connected with the firm.

© Hogan Lovells 2021. All rights reserved. 1356273_0321