

In cooperation with

Luther.

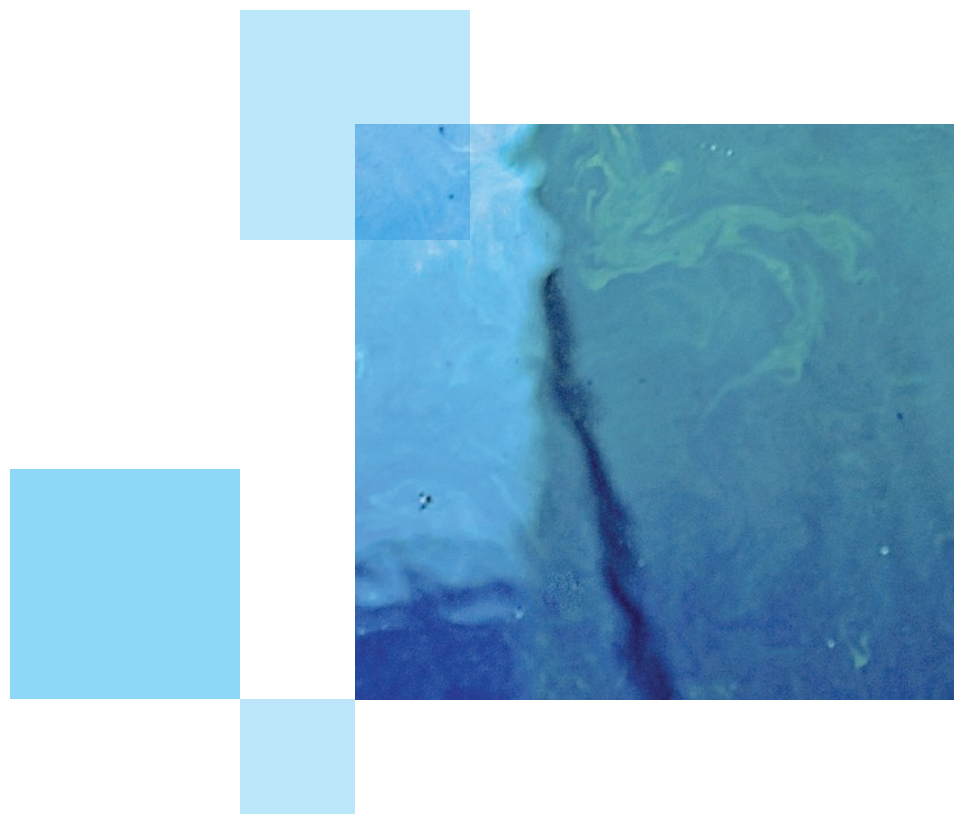
DACbeachcroft

An aerial photograph showing an oil spill on a sandy beach. The oil has spread across the sand, creating a large, irregular area of contamination. The oil's surface is highly reflective, creating a vibrant, iridescent sheen with colors ranging from deep blue and purple to bright green and yellow. The surrounding water is a dark, deep blue. The overall scene is one of environmental damage and pollution.

**Personal Data: the new oil
and its toxic legacy under the
General Data Protection Regulation**

Contents

Foreword	1
Executive summary	2
Key findings	3
In-depth analysis	4
The current European Data Protection landscape	4
Regulatory fines and sanctions	6
Compensation	9
The GDPR effect	10
Contributors	12



Foreword

We live in the age of Big Data. The ability to capture, analyse and utilise massive troves of data has increased exponentially thanks to technological advancements over the past twenty years.

Big Data is often characterized as the 'four Vs': Volume, Variety, Veracity and Velocity. A fifth 'V', Value, has arguably driven the Big Data phenomenon with the greatest speed. Companies that have been able to monetise data, particularly personal data, have achieved the greatest growth. It is no wonder that personal data has been described as the "new oil" and we are in the boom.

Modern companies must use personal data to innovate if they are to prosper, pushing the boundaries of what data is captured and how it is used. However, the commoditization and innovation surrounding personal data also places our fundamental rights to privacy in great danger. The potential for the loss or misuse of data has grown just as fast.

In recent years, judges, legislators and regulators across the EU have recognised the need to protect rights of privacy in the modern era and redress the balance in favour of the individual. This has resulted in a rise in compensation claims and regulatory sanctions against organisations that infringe privacy rights or suffer a data security breach.

Whilst there is currently a varied approach to compensation and regulatory sanctions across the EU, the General Data Protection Regulation attempts to harmonise the regime across member states and in some cases introduces entirely new rights, remedies and liabilities.

The effect of the GDPR on organisations that rely on personal data cannot be underestimated. To highlight the changes the new regime will have, we canvassed data protection and privacy experts across Europe to predict how the liability and sanctions landscape will change, and where the changes will be felt most. We are excited to share our findings in this report.

A theme of our findings was that sanctions and litigation will increase across Europe. It is clear that as we emerge out of the oil boom of the Big Data age, those organisations that are not prepared to deal with its toxic legacy will be hit hard.



Hans Allnutt
Partner

+44 (0) 20 7894 6925
hallnutt@dacbeachcroft.com



Rhiannon Webster
Partner

+44 (0) 20 7894 6577
rwebster@dacbeachcroft.com

Executive summary

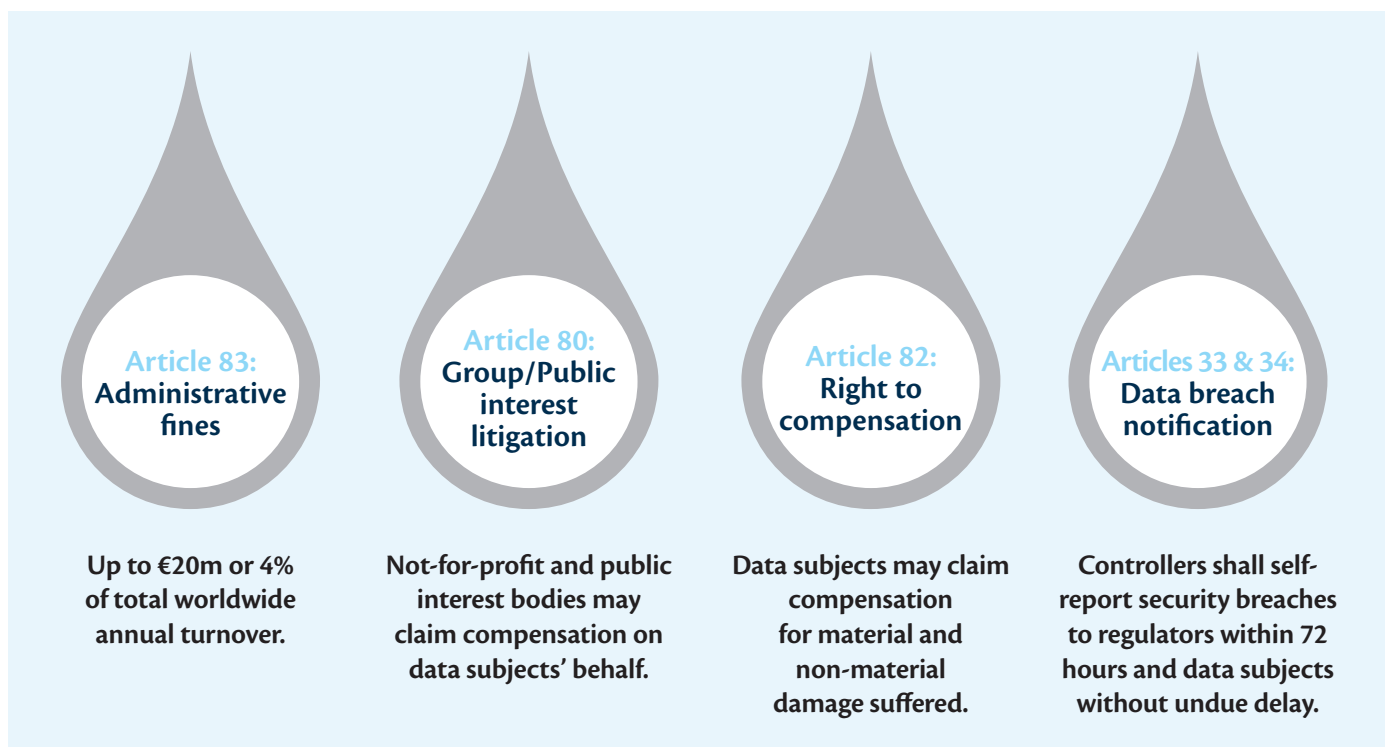
The GDPR represents a step change in privacy rights across Europe

The General Data Protection Regulation (GDPR) will apply from 25 May 2018. It reforms EU data protection law in an attempt to better realise the objectives of its predecessor Directive.

The GDPR introduces new provisions that will dramatically change the risks and potential liabilities facing data processors and controllers. Awareness of GDPR violations will increase due to regulatory rights of audit and the need for the self-reporting

of security breaches. The resulting administrative fines that may be levied by regulators (the higher of €20 million or 4% of total worldwide annual turnover) will also increase, as will compensation claims for material and non-material damage by affected individuals.

Notably, these risks will extend to non-EU organisations that offer goods or services to EU residents or monitor their behaviour. The GDPR's tentacles are truly international.



The GDPR will therefore change the liability model for data protection law across Europe and the world. Over the past year, DAC Beachcroft carried out a study across Europe in order to provide insights into where the liability risks lie, and where they will be greatest felt. Contributions were taken from renowned data protection experts in each EU member state (a full table of contributors can be found at page 12).

Our key findings are set out opposite, with in-depth analysis in the remainder of the report.

Key findings



Individuals' rights to claim compensation for data protection breaches will be new for many EU countries

The current approach to compensation is fragmented across Europe. Article 82 will represent a more significant legal change for some member states than others. In some member states local law already offers equivalent compensation rights as expected under the GDPR (for example, **Bulgaria, Cyprus, Czech Republic, Hungary, and Italy**) however our study identifies that for at least half of EU countries, article 82 will extend existing rights for compensation.



The possibility of representative litigation by consumer and non-government organisations is new to almost all EU countries

The large majority of the member states do not currently have mechanisms for representation of data subjects by non-government organisations, as provided under article 80. There are a handful of exceptions in EU countries that have similar types of representative litigation already in place (for example, **France, Germany, Hungary**). However, for the majority the type of representation proposed in article 80 will be entirely novel.



Fines and compensation currently vary hugely between countries

Our study revealed a significant disparity in the level of fines currently issued by supervisory authorities across the member states. To date, the largest fines on record have been issued in **Germany** (1,460,000 to LIDL in 2008), **Italy** (€1,000,000 to Google in 2013), **Spain** (€1,200,000 to Facebook in 2017) and the **United Kingdom** (£400,000 to TalkTalk in 2016). Most countries report much lower record fines, for example in **Latvia** (€4,248), **Slovakia** (€8,000) and **Poland** (€47,000). In other member states there was no record of any fines being issued, either by the relevant Data Protection Authority or by the courts (i.e. **Luxembourg**).



There will be an increase in data protection compensation litigation under GDPR

Opinion was relatively split over whether data protection and privacy litigation had increased over the last five years, which is perhaps unsurprising given the different legal regimes. However, the majority of respondents thought that compensation claims would increase under the GDPR. A number of reasons were given for this, including the effect of breach notification under articles 80 and 82, increased data subject rights and awareness, and the increased value of sanctions.

In-depth analysis

The current European Data Protection landscape

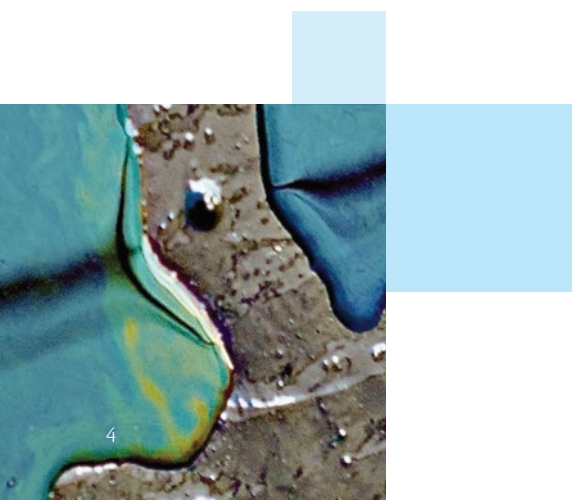
A central objective of the GDPR is the harmonisation of EU data protection law, which is currently fragmented in a number of areas. The GDPR's predecessor, Directive 95/46/EC (the 'Directive'), allowed EU countries to incorporate its provisions into their own national laws and at different times. The Directive also contained a number of derogations that allowed member states to adopt divergent approaches to particular issues.

As a result, the current state of EU data protection law under the Directive is far from consistent. The GDPR acknowledges as much in recital 9, stating that *"The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the implementation of data protection across the Union, legal uncertainty or a widespread public perception that there are significant risks to the protection of natural persons"*.

Aside from the implementation of the Directive, respondents to the study pointed to a range of other privacy related laws that have developed in recent years. Therefore, while data protection law has continued to grow and change since the Directive, it has not always done so through primary legislation.

These legislative developments, combined with the various developments in common law, have resulted in an EU privacy framework that varies markedly from member state to member state. It is arguable that the GDPR's harmonisation objective faces the greatest challenge from those jurisdictions where it represents the greatest change or where existing laws have been in place for the longest. However, if harmonisation is not achieved, then the EU runs the risk of a multitiered approach and the prospect of forum shopping by organisations seeking leniency.

EU states' implementation of the Directive



Findings: the current landscape



The Directive has been implemented by all member states, although often with additional or supplemental regulation and judicial precedent

All the respondents to the study confirm that the Directive had been implemented in the relevant member state, although many included additional details that demonstrate the level of fragmentation within the EU. In **Austria**, for example, the Austrian Data Protection Act is based on the Directive, but includes additional details and requirements that exceed the requirements contained in the Directive. In **Ireland** the Data Protection Acts 1988-2003 have been supplemented by the Office of the Data Protection Commissioner with nonbinding guidance notes and codes of practice.



Many member states have other laws that address data protection and privacy

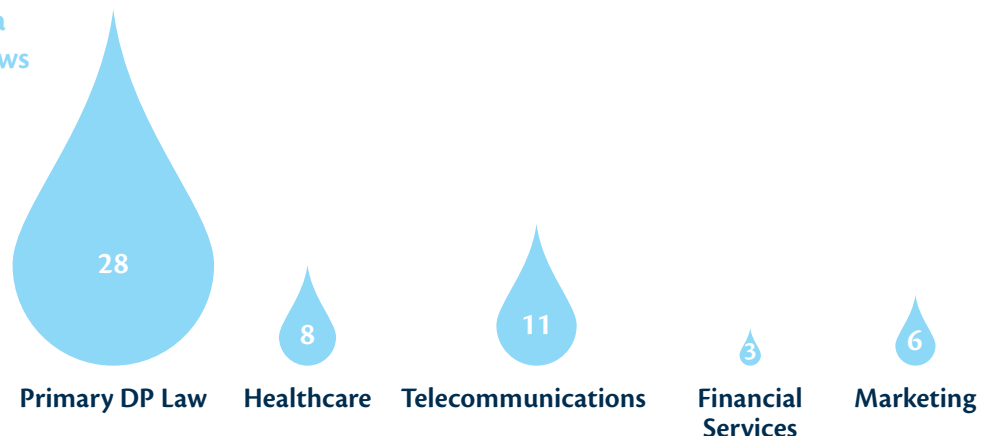
As well as their primary data protection legislation, most respondents referred to other legislative instruments that also played a role in regulating data protection and privacy. For example, in **Croatia**, besides the Act on Protection of Personal Data, data protection regulation can be found in a number of legislative instruments including the Constitution of the Republic of Croatia, the Act on Data Confidentiality, the Employment Act and the Criminal Code. Respondents also referred to other causes of action in tort and equity which further supplemented these laws, including the tort of misuse of private information and breach of confidence.



Some member states have sector specific laws that are relevant to data protection

Respondents to the study also identified a range of relevant sector specific instruments that address data protection concerns. These included instruments relevant to financial services (for example, the **United Kingdom's** FCA Principles for Businesses), healthcare (for example, **Slovenia's** Patient Rights Act), telecommunications (for example, **Austria's** Austrian Telecommunications Act 2003) and marketing and consumer rights (for example, **Sweden's** Swedish Marketing Act).

Relevant data protection laws



Regulatory fines and sanctions



An area of significant fragmentation under the Directive is regulatory enforcement powers and the level and frequency of sanctions handed down for breaches of data protection laws.

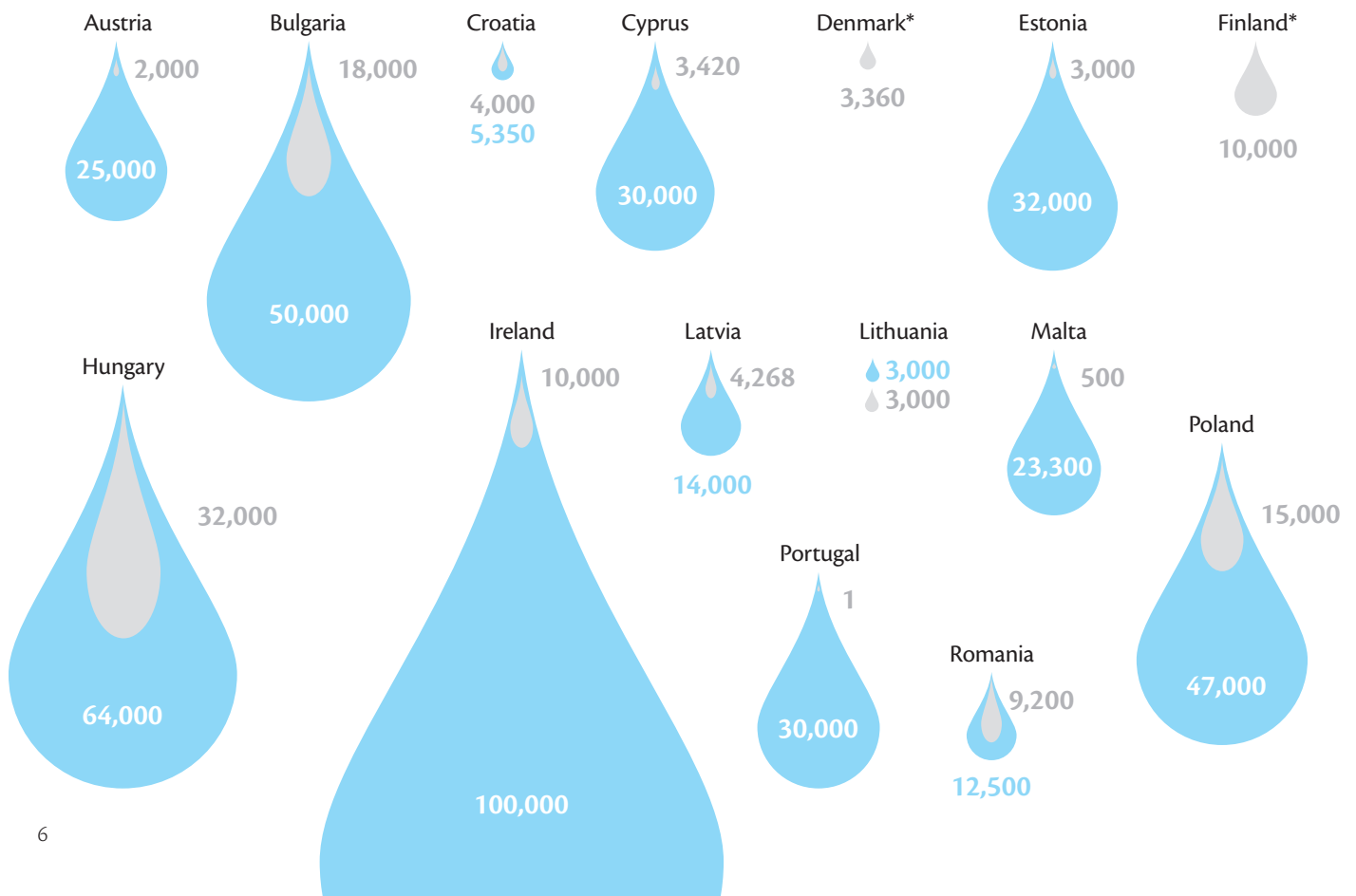
Whilst the Directive empowered EU countries to lay down sanctions to be imposed following infringements of the provisions, not all member states provided for financial penalties when first enacting their national legislation. In the UK, the ICO was only able to award monetary penalties from May 2010. Guidance is provided by both the Article 29 Working Party and the judgments of the European Court of Justice, but the level and frequency of financial penalties ultimately remained the purview of each member state, resulting in a range of approaches. Critics claim that current sanctions are an ineffective deterrent for large corporations.

The GDPR will change this position dramatically. First, the level of fines will increase significantly for most member states: up to €20m or 4% of annual worldwide turnover, whichever is the highest. Second, it will clarify that each member state's supervisory authority is able to issue such fines. Third, harmonisation should, in theory, be enforced by the European Data Protection Board, which will supervise the application of sanctions across all member states.

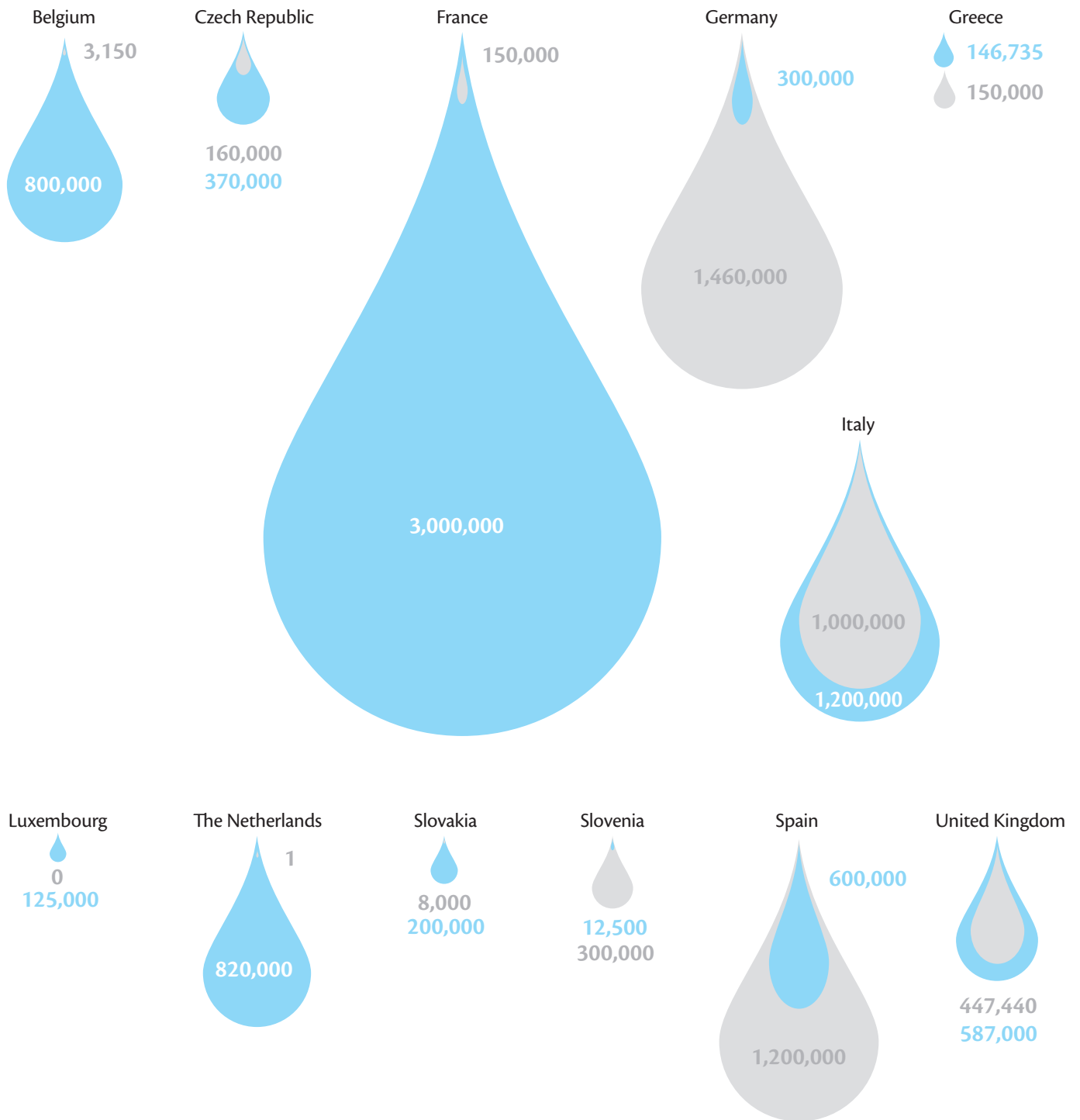
It is clear from our study that harmonisation will be challenging given the different experiences of the supervising authorities across Europe with some jurisdictions having no prior experience of issuing fines and others having already implementing approaches similar to those envisaged under the GDPR. If harmonisation is not achieved under the GDPR, at least in the early years, there is a risk that this could lead to data heavy organisations taking a strategic decision to relocate their central administration or main processing activities to more lenient jurisdictions.

Maximum DP fines against those awarded by jurisdiction

 Largest recorded fine (€)
 Maximum potential fine (€)
 *No maximum fine



Alternative scale used on this page to represent larger figures above €100,000



Sweden: fines are determined due to the economic circumstances of the organisation rather than a fixed figure (no fines have been issued to date).

Germany, Greece, Slovenia and Spain: the largest recorded fines stated above were an aggregate of multiple fines applied to a single organisation.

Findings: fines and sanctions



There is a large disparity in the highest fines issued to date in different member states

Our study revealed a significant disparity in the level of fines issued by member states. To date, the largest fines on record have been issued in **Germany** (€1,460,000 to LIDL in 2008), **Italy** (€1,000,000 to Google in 2013), **Spain** (€1,200,000 to Facebook in 2017) and the **United Kingdom** (£400,000 to TalkTalk in 2016). Most countries report much lower record fines, for example in **Latvia** (€4,248), **Slovakia** (€8,000) and **Malta** (€500). In other member states there was no record of any fines being issued, either by the relevant Data Protection Authority or by the Courts (e.g. **Luxembourg**).



Some Data Protection Authorities do not have the power to issue fines and penalties

In a number of member states Data Protection Authorities are not empowered to hand down fines themselves, but rather have to apply to the Court for financial penalties. This was found to be the case in a handful of member states such as **Belgium, Denmark** and **Ireland**.



Not all member states publish information on fines and penalties

Assessing the relative level of fines in each member state was complicated by the fact that a number did not publish information on fines and penalties. In **Austria**, for example, information is limited because the decisions of the Austrian Regional Administrative Authorities, where most data protection matters are considered in the first instance, are not published. Responses from **Croatia** and **Estonia** also reported that some of the relevant decisions were not publicly available.



In some cases, member states are already adopting the GDPR's formulation of fines for a certain percentile of turnover

Both **Romania** (albeit under the Romanian e-Privacy Law) and the **Netherlands** have maximum fines which are limited to either a fixed sum, or a percentage of the organisation's annual turnover. Interestingly, in the Netherlands this cap is currently set at 10% of the organisation's global annual turnover.



Fines were reported for a range of reasons

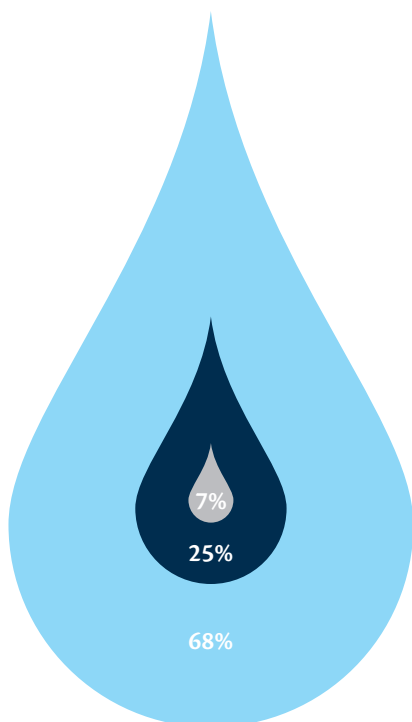
The responses to our study gave examples of fines issued for a range of reasons, both at the low and high end of the scale. These included unauthorised video surveillance (**Austria**), misuse of patient information (**Belgium**), insufficient data security (**Czech Republic**), inappropriate use of data for direct marketing (**Denmark**), storage of cookies (**France**) and unlawful use of traffic data (**Portugal**).

Compensation

As well as regulatory fines and sanctions, there has been an increasing trend in claims for compensation following security breaches and data protection violations. Across Europe, there is greater recognition of the damage such breaches can cause to individuals. This shift has been prominent in the United Kingdom, where the courts have acknowledged broader rights of compensation in cases such as *Gulati v MGN Ltd* [2015] EWHC 1482 (Ch) and *Vidal-Hall v Google Inc* [2015] EWCA Civ 311.

However, while there has been progress in some quarters, our study has shown that the approach to compensation remains varied across the EU. Developments like those made by the Courts in *Gulati* and *Vidal-Hall* do not further unify the EU approach, but drag member states further away from each other. For those member states that do provide compensation, the level and frequency of compensation awards varies significantly. This is not dissimilar to the variation in fines reported by the study respondents.

Current compensation regimes in member states



No compensation - 2/28

Compensation for material damage - 7/28

Compensation for material and non-material damage - 19/28

Findings: compensation



There are currently a range of approaches to compensation within member states

Member states are divided on the issue on compensation. A large majority of the respondents stated that the member state in question provided some form of right to compensation. However the nature and scope of that compensation varied significantly, particularly when it came to what type of damage the compensation could be claimed for, and who the compensation could be claimed from. A number of respondents stated that compensation could not currently be claimed for non-material damage, although there appears to have been a general movement in favour of recognising compensation for such damage.



There is also a large disparity in the level of compensation awarded

As with fines, the level of compensation varies from member state to member state. Of those member states that do provide compensation, most of the awards fell within a band of €10,000 or below. However, some awards were significantly higher. For example, in **Italy** awards had been made of €90,000 and €25,000.



Data protection legislation is not necessarily the only avenue for obtaining compensation

Most respondents to the study reported a number of alternative avenues for obtaining compensation. For example, through developing tortious causes of action (**United Kingdom**), unfair trade practices legislation (**Belgium**), and general and special provisions for damage under various civil codes (**Slovakia**). It may be that the availability of alternative, more familiar causes of action has discouraged data subjects from seeking redress through data protection legislation. This may change given the high profile of the GDPR and the increased focus on data subject rights.

The GDPR effect

The GDPR will have a profound effect on EU data protection law. Harmonisation means that most member states' data protection laws will change, most likely in ways that will expose data controllers and processors to increased risks of litigation under articles 80 and 82.

Under article 80, data subjects have the right to appoint certain non-profit bodies to lodge a complaint on their behalf, and exercise their right to compensation. Whilst it remains to be seen exactly how this will be put into practice in each member state, it does raise the possibility of group litigation.

Article 82 empowers data subjects to claim compensation for material and non-material damage resulting from an infringement of the GDPR, from both controllers and processors. While this represents the status quo in some member states, for a number of member states this either extends or introduces the right to compensation for breaches of data protection legislation.

Considering the effect of the GDPR in isolation, it appears that the new regime will encourage data subjects to seek to enforce their rights and claim compensation for breaches of the relevant principles and obligations.

However, the right to compensation cannot be considered in a vacuum. The prevalence of claims will be affected by the litigation culture and regime of the relevant member state, as well as their approach to costs and litigation funding. No matter how complimentary the regulatory environment and the rules around liability, litigation must be accessible if claims are to be made.

It is clear, however, from our study that the GDPR will trigger a wave of increased litigation and compensation claims across most of Europe. Unsurprisingly, this change may be most pronounced in jurisdictions where the litigation cost regime is more favourable to claimants.

Findings: GDPR effect



The extent to which article 82 introduces a new right to compensation is mixed

As discussed above, the current approach to compensation is fragmented and article 82 will represent a much larger shift for some member states than others. However, it appears from the respondents that article 82 will be an extension of the right to compensation for half of the affected member states. In some member states local data protection law already offers data subjects the compensation rights provided under the GDPR (for example, **Bulgaria, Cyprus, Czech Republic, Hungary, and Italy**). In other member states article 82 will broaden the right to compensation, either introducing liability for processors (for example, **Malta, Greece**), or by extending liability to non-material damage, as well as material damage (for example, **Poland, Sweden, and Austria**). In the most extreme cases, article 82 will introduce a right to compensation where none previously existed (for example, **Luxembourg**).

How the GDPR will change compensation rights



Number of Member States affected

Change – extends to non-material damage – 2

Change – application to processors – 5

Change – extends to non-material damage and processors – 7

No change – 14

Findings: GDPR effect continued



Introduction of group litigation under article 80 is new to almost every member state

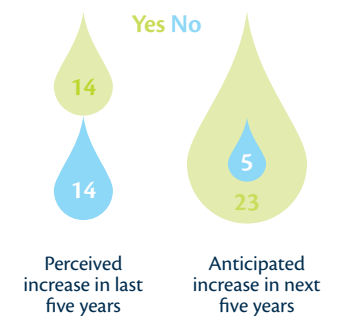
By contrast, while the current position regarding compensation varies from state to state, the large majority of the member states do not currently have a group litigation mechanism as provided under article 80. With the exception of a few states that allow group litigation in some circumstances (for example **Germany**, **Hungary** and **Lithuania**), article 80 represents a sea change for data protection litigation in the majority of the member states.



Respondents were mixed as to whether data protection litigation had increased over the last five years but were convinced it would increase under the GDPR

Opinion was relatively split over whether data protection and privacy litigation had increased over the last five years, which is perhaps unsurprising given the different legal regimes. However, the majority of respondents thought that compensation claims would increase under the GDPR. A number of reasons were given for this, including the effect of breach notification under articles 80 and 82, increased data subject rights and awareness, and the increased value of sanctions.

Perceived and anticipated increases in litigation



Where respondents thought that litigation would not increase, costs was the predominant factor

Only a minority of respondents thought that data protection litigation would not increase as a result of the GDPR. The most common reason given for this was the cost of litigation. In the vast majority of cases, litigants are able to recover their costs if successful. Therefore, the litigation cost regime of each member state will be an influencing factor of whether claims will be brought.

Cost is a factor in litigation



“No-win-no fee” in data protection cases remains in its infancy

“No-win-no fee” in data protection cases remains in its infancy. The majority of respondents reported that “no-win-no-fee” regimes were not available in the member state in question. Given the GDPR’s introduction of a group litigation model under article 80, the cost barrier to litigation may reduce. However, for the meantime it appears that most data subjects in the EU will not be able to take advantage of such arrangements.

Availability of no-win-no-fee arrangements



Contributors

DORDA

Austria

DORDA Rechtsanwälte

Axel Anderl

✉ axel.anderl@dorda.at

☎ +43 1 533 47 95 23



Belgium

Philippe Laurent

✉ philippe.laurent@mvvp.be

☎ +32 2 285 01 00



Bulgaria

Yana Madina

✉ y.madina@zmlf.com; zmlf@zmlf.com

☎ + 359 (0) 2 944 86 20



Croatia

Marija Gregoric

✉ marija.gregoric@babic-partners.hr

☎ +385 (0) 1 3821 124



Cyprus

Panayiotis Demetriades

✉ p.demetriades@demetriadesllc.com

☎ +35722666436



Czech Republic

Eva Nováková, Partner

✉ Eva.Novakova@jsk.cz

☎ +420 226 227 618



Denmark

Lasse A. Søndergaard Christensen

✉ lsc@gorrissenfederspiel.com

☎ +45 86 20 74 20



Estonia

Pirkko-Liis Harkmaa

✉ pirkko-liis.harkmaa@cobalt.legal

Ave Piik

✉ ave.piik@cobalt.legal

Aleksander Tsuiman

✉ aleksander.tsuiman@cobalt.legal

☎ +372 665 1888



Finland

Sakari Halonen

✉ sakari.halonen@twobirds.com

Milla Keller

✉ milla.keller@twobirds.com



France

Thierry Dor

✉ dor@gide.com

☎ +33 1 40 75 28 46



Germany

Dr Stefanie Hellmich

✉ stefanie.hellmich@luther-lawfirm.com

☎ +49 69 27229 24118



Greece

Vicky Chatzara

✉ v.chatzara@rokas.com

☎ +30 210 3616816



Hungary

Dr. Tamás Gödölle

✉ tamas.godolle@bogsch.hu

☎ +36 1 318 1945



Ireland

Aidan Healy

✉ ahealy@dacbeachcroft.com

☎ +353 123 19669

Rowena McCormack

✉ rmccormack@dacbeachcroft.com

☎ +353 1 231 9628



Italy

Aldo Feliciani

✉ a.feliciani@studiobonora.it

☎ +39 02 76013210



Latvia

Edvijs Zandars, Ilga Valjko

✉ edvijs.zandars@ellex.lv


☎ +371 67814848

SORAINEN

Lithuania

Renata Berzanskiene

 renata.berzanskiene@sorainen.com


 +370 52 649 321

LGAVOCATS — Luxembourg —

Luxembourg

Hervé Wolff

 hw@lgavocats.lu

 +356 44 37 37 65

GANADO ADVOCATES

Malta

David Borg Carbott

 dbcarbott@ganadoadvocates.com

 +356 21 235 406

Philip Mifsud

 pmifsud@ganadoadvocates.com

 +356 21 235 406

DENTONS

Netherlands

Mark Elshof

 marc.elshof@boekel.com

 +31 20 795 36 09


Bird & Bird


Poland

Izabela Kowalczyk-Pakula

 izabela.kowalczyk-pakula@twobirds.com

Maria Guzewska

 maria.guzewska@twobirds.com


 +48 22 583 79 00



Portugal

Marco Alexandre Saias

 marco.saias@pra.pt


 +351 213 714 940

TUCA ZBARCEA ASOCIATII

Romania


Catalin Baiculescu

 catalin.baiculescu@tuca.ro

 + (40-21) 204 76 34

Sergiu Cretu

 sergiu.cretu@tuca.ro

 + (40-21) 204 88 90

Bird & Bird

Slovak Republic

Mgr. Bibiana Mozoľová & JUDr. Radovan Repa

 bratislava@twobirds.com


 +421 232 332 800



Slovenia


Nataša Pipan Nahtigal

 natasa.pipan@selih.si

 +386 1 300 76 50


Tamara Petrović

 tamara.petrovic@selih.si

 +386 1 300 76 50

Nika Bosnič

 nika.bosnic@selih.si


 +386 1 300 76 50



Sweden

Mattias Lindberg

 mattias.lindberg@affarsadvokaternasverige.se

 +46 708 13 05 18



Spain

Irene Robledo de Castro

 irobledodecastro@dacbeachcroft.com

 +34 91 781 63 00



United Kingdom

Hans Allnutt

 hallnutt@dacbeachcroft.com

 +44 20 7894 6925


Rhiannon Webster

 rwebster@dacbeachcroft.com

 +44 20 7894 6577

Joseph Fitzgerald

 jfitzgerald@dacbeachcroft.com

 +44 20 7894 6875



In the event of a cyber incident or data breach, contact our Cyber & Data Risk team.

 +44 (0) 800 302 9215

 DataRisk@dacbeachcroft.com

www.dacbeachcroft.com

 Follow us: [@dacbeachcroft](https://twitter.com/dacbeachcroft)

 Join the discussion on LinkedIn: <https://www.linkedin.com/company/dac-beachcroft-llp>

The DAC Beachcroft LLP Personal Data: the new oil and its toxic legacy under the General Data Protection Regulation report is provided for information only and no liability is accepted for errors of fact or opinion it may contain. Professional advice should always be obtained before applying the information to particular circumstances. The copyright in this report is retained by DAC Beachcroft LLP. © DAC Beachcroft 2017