Report

Five Years of GDPR

From Revolution to Evolution: The GDPR's Impact on Data Protection and What Lies Ahead

RelianceCyber

Contents

Five Years of GDPR

Introduction

25 May 2023 marks the fifth anniversary since the General Data Protection Regulation (GDPR) became enforceable. The GDPR has transformed the landscape for data protection law, introducing a raft of new obligations for organisations using personal data, increasing individuals' data rights, and introducing stricter requirements for accountability.

The result was a best-in-class framework which has been emulated globally and continues to lead the way in ensuring that data is processed in keeping with the highest standards of security, transparency and lawfulness.

Much has changed since GDPR's formal introduction – multiple record fines, businesses working hard to understand their requirements, clarifications from EU organisations, Brexit, the development of increasingly.

sophisticated Artificial Intelligence (AI) technologies and many more challenges and developments – all of which has made GDPR only more relevant to the modern workplace

In our series of articles, we are looking back at the last 5 years of the GDPR and forward to what the future might hold.

Our team has examined the GDPR from a number of angles: from delving into the data to understanding why some Data Protection Authorities issue more fines and what they are looking for; to summarising the battle between tech firms and regulators; to analysing what the role of the Data Protection Officer might evolve into; and, finally, to examining the future of UK-EU cooperation in data protection and what the impacts of the post-Brexit world might be.

There is a view in some circles that GDPR is a nuisance, that it creates unrealistic burdens and is a barrier to businesses operating successfully. Nothing can be further from the truth. The GDPR should be seen as an incredibly positive development for individual rights and freedoms that raises the ethical and administrative bar.

Any organisation should want to treat their clients' and employees' data with respect, keep these parties informed to build trusting relationships, and to ensure that any sensitive information is suitably protected.

Having a framework that holds businesses to account and pushes them to do better and act more transparently, therefore, can only be a net benefit to us all.

If you would like to discuss any of the issues raised in this brochure, or any of your own requirements concerning data protection and data privacy, please contact one of our experts.

Get in touch

"Having a framework that holds businesses to account and pushes them to do better and act more transparently, can only be a net benefit to us all."

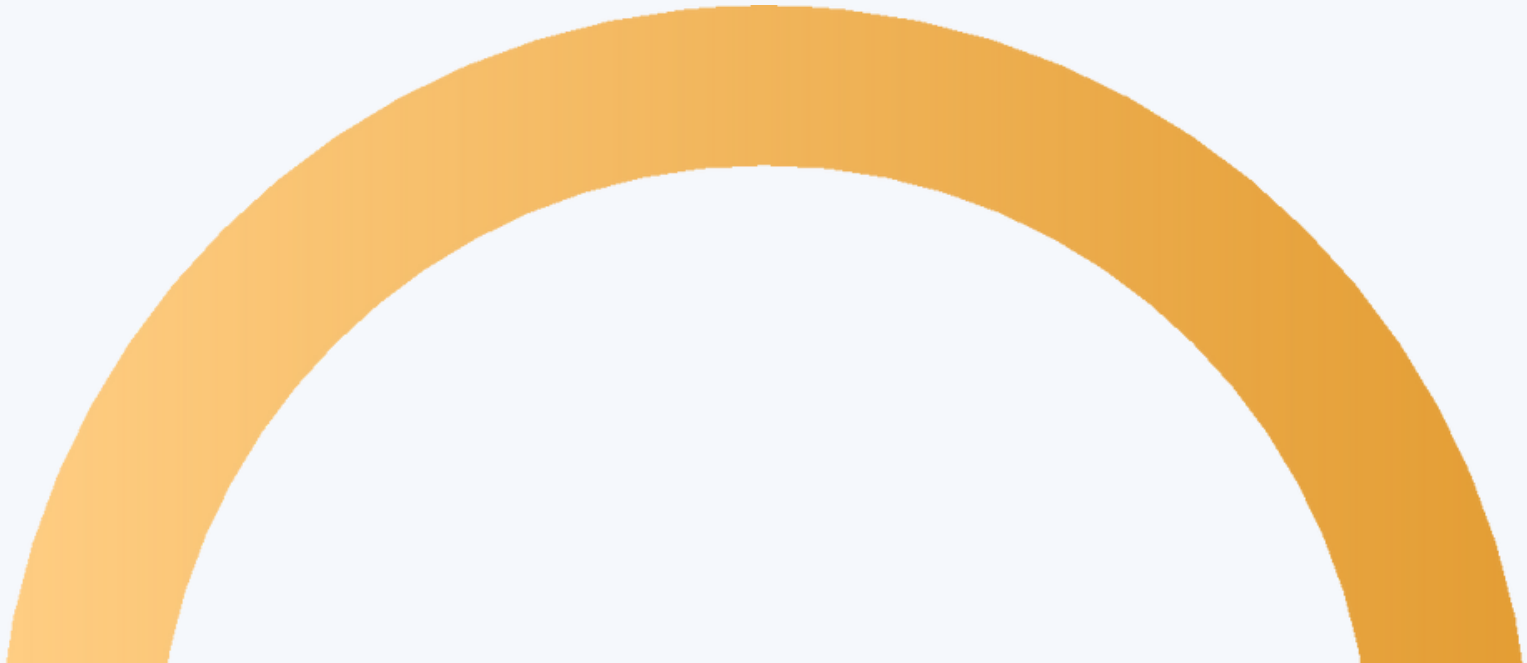
Luke Hull
CTO
Reliance Cyber

Looking Back

The Last 5 Years of The GDPR

Article I:

Looking back at 5 years of GDPR



Looking back at 5 years of GDPR – a comparative analysis of fines and regulators across Europe

The General Data Protection Regulation (GDPR) celebrates the fifth anniversary since it became enforceable on 25 May 2023, and it certainly made a huge impact in that time. The regulation has helped enshrine personal data rights and move them to the forefront of public knowledge, making companies more accountable for observing those rights along the way.

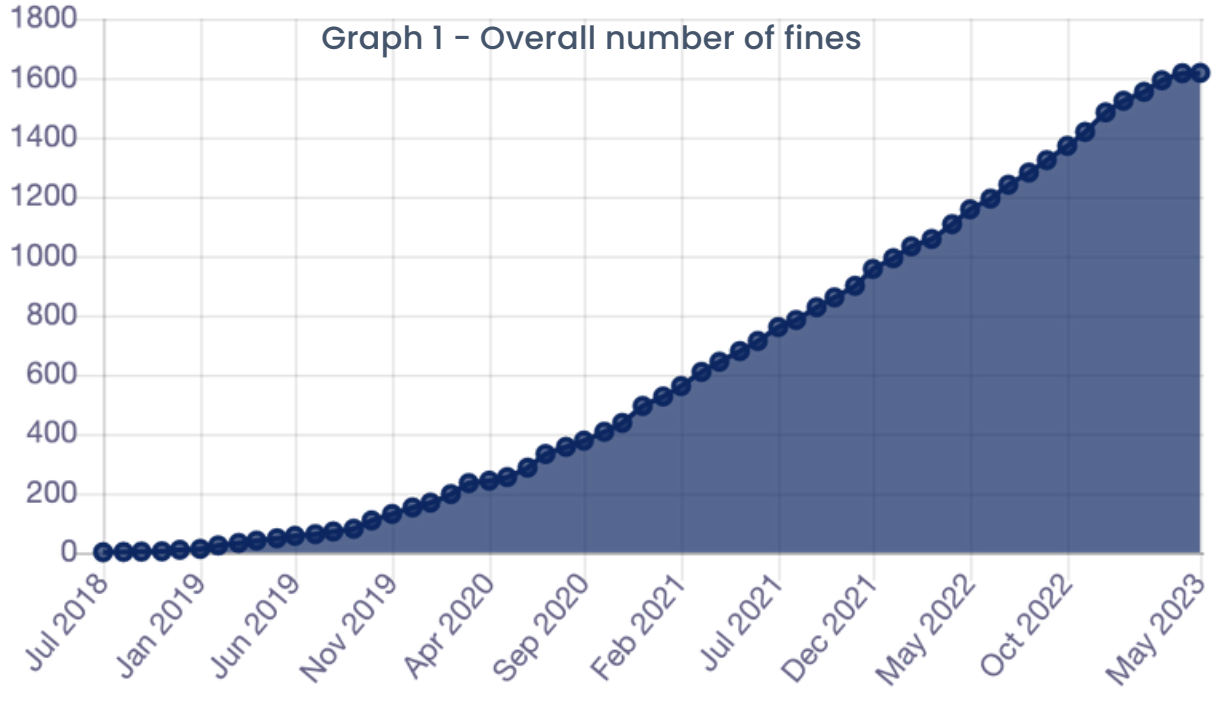
In doing so, Data Protection Authorities (DPAs) have regularly used their powers to sanction organisations who have not fulfilled their obligations in the spirit of the regulation. Though this can take the form of an official reprimand, most prominent examples in the media will take the form of fines issued to various entities who have breached the requirements of the GDPR.

According to data privacy research and advice platform Privacy Affairs, as of 22 May 2023 these fines have totalled in excess of €4 billion spread across 1,702 separate penalties – approximately €2.35 million per fine on average (although this increased from €1.65 million on average overnight after Meta's record fine in May 2023).

However, particularly given the fact that the range of fines goes from €28 at one end of the spectrum to €1.2 billion at the other, there is plenty more to investigate if you delve into the data.

Changes in fines over time

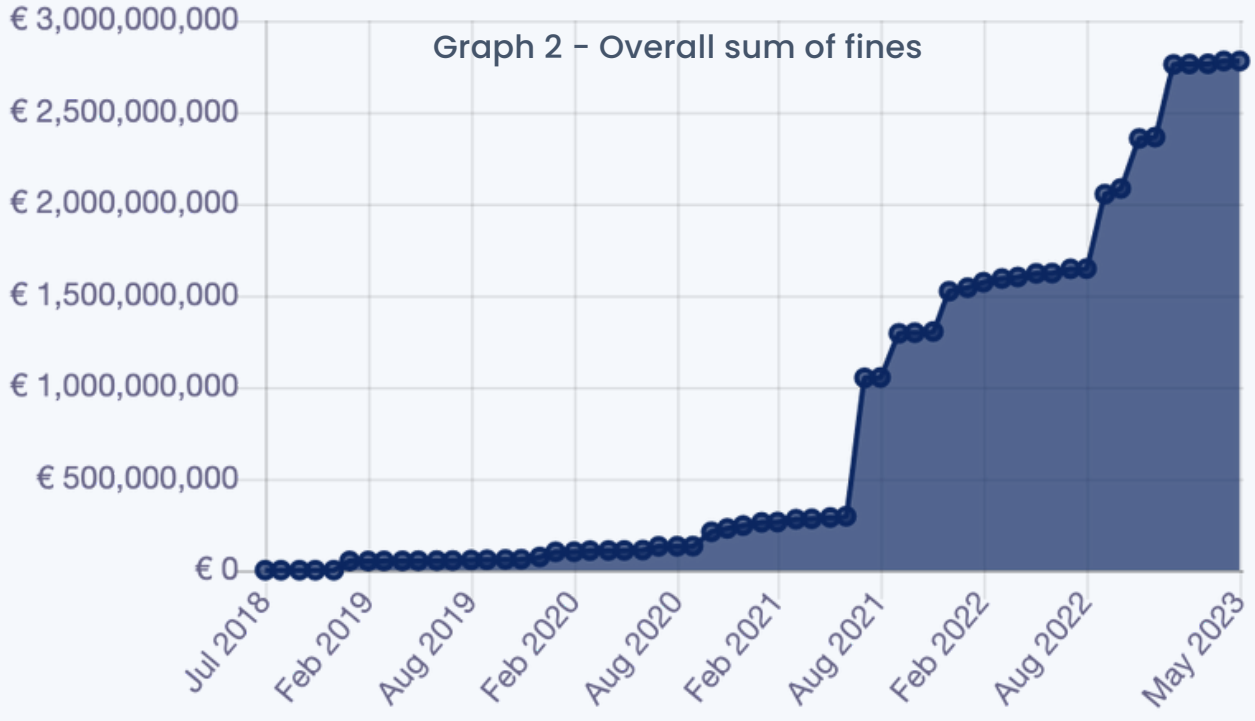
One might assume that, as the GDPR has become more embedded and companies' and regulators' expectations settle, the rate of fines (and likely their value) would increase. However, in the main, this very much does not appear to have been the case.



As Graph 1 shows, there has actually been a relatively consistent number of fines given out month-on-month basis. After a slow start (2018 saw only 9 fines at € 436,388 in value) the growth has been steady with around 30-60 new fines a month. However, what is perhaps more interesting is the value of the fines over the course of this five-year period.

Changes in fines over time

Here we see a large change and fines have increased significantly over this time – the cost of GDPR fines went from €158.5 million in 2020 to €1.087 billion in 2021 and then €2.92 billion levied in 2022. These are huge increases, numbers which suggest that the regulation has acquired real teeth and that regulators are not scared to go after offenders. Nothing underlines this more than the unprecedented €1.2 billion fine given to Meta in May 2023 for infractions regarding EU-US data transfers – a figure only barely smaller than all combined fines from 2020 and 2021 combined.



Interestingly though, the data does appear to be severely impacted by a few notable leaps where large fines have been issued. The trend has otherwise been relatively steady with month-to-month increases of around €10 million, suggesting that certain prominent cases are generally responsible for the increases we see, rather than fines across the board necessarily all becoming larger.

The 'mega fines'

If we examine Graph 2, we see a few distinct jumps – these can all be explained by milestone fines that occurred at very particular points and somewhat skew the averages. The first month to note would be January 2019. This is when Google were fined €50 million for failing to have a legal basis on how users' data was processed. This was the largest fine to come of GDPR at the time, accounting for over 99% of the entire value of fines at this time.

2021 is the next key turning point, a sizable year for fines. In July of this year Luxembourg's DPA issued the largest fine to date targeting e-commerce giant Amazon who received a staggering €746-million penalty for the non-compliance with the general data processing principles.

For comparison, the month prior issued out only €6,551,600 worth of fines – hence a massive leap in the data.

In September 2021, another milestone WhatsApp were fined €225 million for infringements around the transparency of processing. That wasn't the end for 2021 though, with Google receiving two fines of €90 million and €60 million in France over infractions concerning consent and the ease with which users could refuse cookies – and Facebook also receiving a €60 million fine for the same reason.

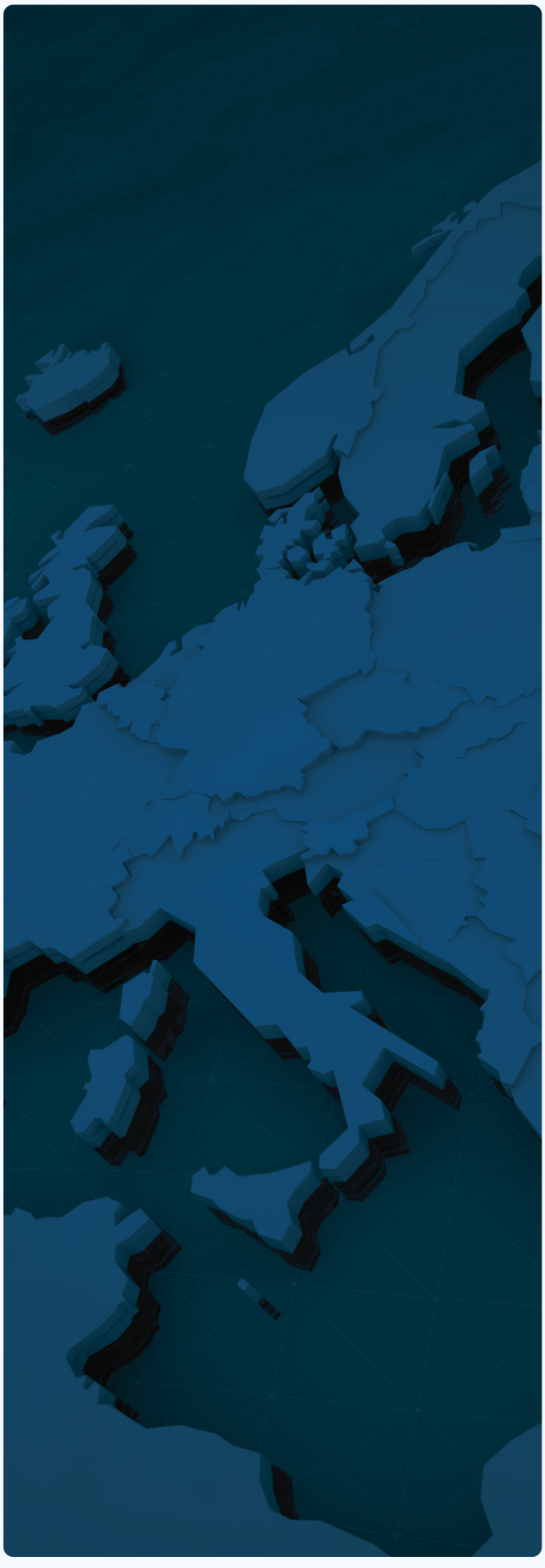
The 'mega fines'

Meta over the last two 9 months has incurred a further four giant fines. The aforementioned €1.2 billion fine announced by the Irish DPA, the Data Protection Commission, on 22 May 2023; two for non-compliance with general data processing principles equating to €795 million (€405 million in September 2022 and €390 million in January 2023); and finally fine given was for the insufficient technical and organisational measures to ensure information security hitting €265 million in December last year. This overall makes Meta comfortably the 'most-fined' company under the GDPR, with penalties totalling around €2.545 billion when including WhatsApp and Facebook.

How enforcement and fine issuance differ across Europe

The GDPR has always had some room for interpretation. Each member state interprets the GDPR in accordance with its own national approaches and idiosyncrasies. This means that, though it is one law, the application based on jurisdiction is subject to particular nuances and changes in perspective.

How does this bear out in the data if we compare different countries and their enforcement of the regulation? In the first case, as Chart 1 below, some DPAs are apparently much more likely to an issue a fine than others, with Spain comfortably the most prolific. However, what does this mean for organisations and how does it play out in practice?



How enforcement and fine issuance differ across Europe

Country	Number of Fines
SPAIN	**640** (with total € 59,349,670)
ITALY	**260** (with total € 123,321,596)
GERMANY	**148** (with total € 54,810,633)
ROMANIA	**138** (with total € 749,250)
HUNGARY	**58** (with total € 2,048,961)
GREECE	**57** (with total € 30,601,000)
NORWAY	**50** (with total € 10,417,950)
POLAND	**49** (with total € 3,433,469)
BELGIUM	**39** (with total € 1,822,000)
CYPRUS	**34** (with total € 1,344,250)

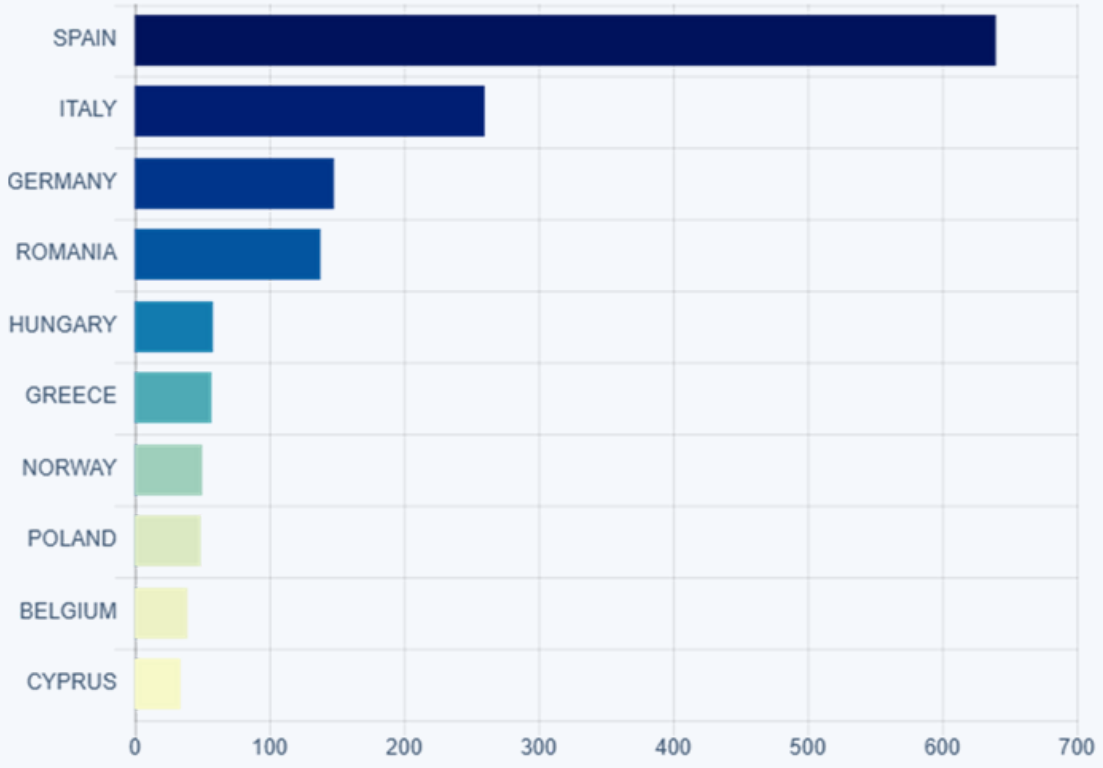


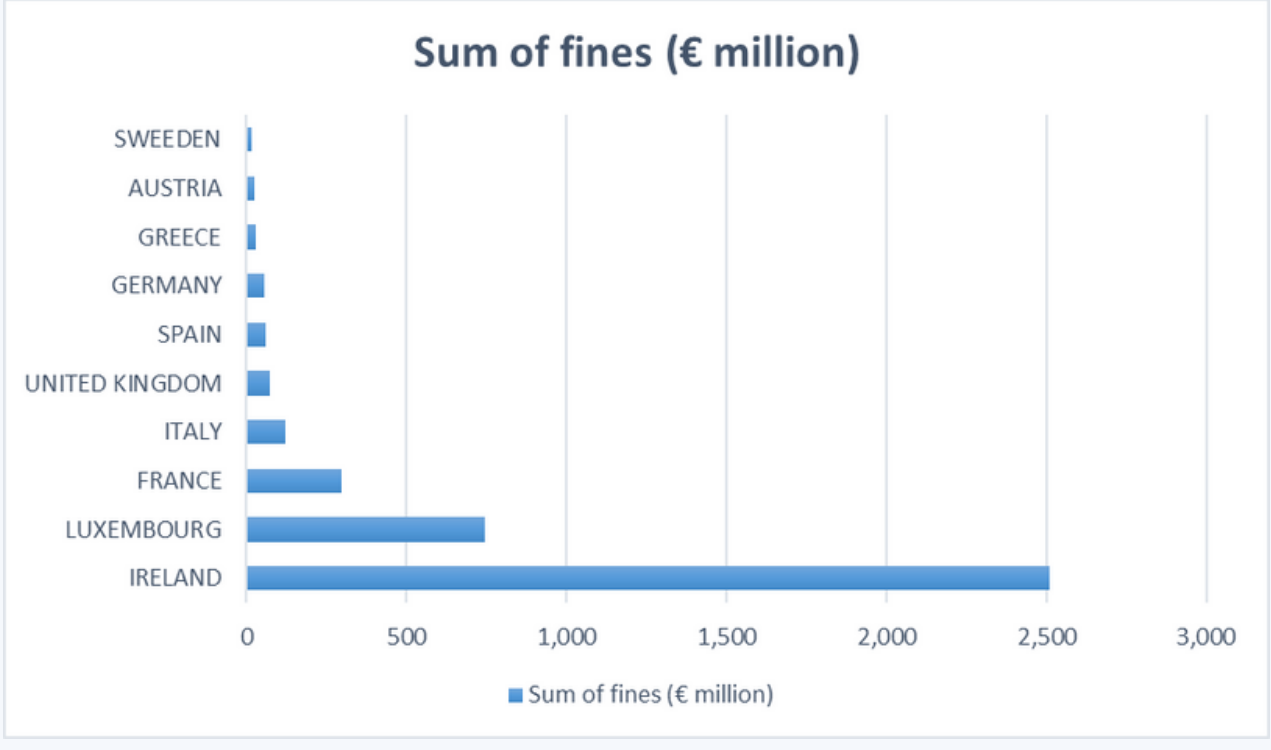
Chart 1 - Overall Number of Fines per Country (Credit: GDPR Enforcement Tracker)

The case of Spain

Spain's DPA instantly stands out due to the 640 fines it has given out, the most of any DPA and around 2.4x more than Italy in second place. Spain's 640 fines are equivalent to €59,349,670 which is on average €92,733 per fine.

This is, as many observers might note, a low average and, tellingly, the value of fines issued by the Spanish DPA is only the sixth largest (see Chart 2). Spain has had some significant fines hitting Google for €10 million, Vodafone for €8.15 million and €3.94 million, Caixbank for €6 million, Banco Bilbao Vizcaya Argentaria for €5 million and another six for over €1 million. However, most of its fines are small amounts, with 331 of its fines (over half) sitting between €1000-€10,000.

Chart 2 – Fine Values per Country



How does this compare with other jurisdictions?

The UK

The UK has issued €75,132,800 from 13 fines in the past five years including against some recognisable companies such as British airways (€22 million), Marriott International (€20.45 million), TikTok (€14.5 million), Clearview AI (€9 million) and Interserve (€5.033 million) to list the largest five. On average the UK's Information Commissioner's Office (ICO) issues €5,779,446 per fine.

At this point, we should stress that this is specifically for GDPR fines.

In 2022, the ICO actually issued 34 monetary penalties, only five of which related to GDPR breaches with the rest constituting infractions of Electronic Marketing Rules.

The proportion has slightly shifted towards GDPR fines (from 8.33% in 2021 to 15% in 2022). This suggests that the UK are selective with their fines, given there are only 13 on record, and lean towards more serious infractions with larger penalties.

France

The Commission Nationale Informatique & Libertés (CNIL), France's DPA, has issued a similar number of fines as Luxembourg, hitting 34 over the course of the 5 years. The total of all of their fines adds up to €293,544,300 with the average fine arriving at €8,633,655 which is higher than the UK with many more fines. The two significant fines are against Google (€50 million) and Clearview AI (€20 million).

majority of the CNIL's fines (18 to be exact), however, reside within the hundreds of thousands, typically between €125,000 and €800,000.

Ireland and Luxembourg

Ireland and Luxembourg are significant anomalies in this analysis. These two DPAs have issued the largest overall fines (to Amazon, Google, and Meta) with Ireland's overall value fines totalling in excess of €2.5 billion. However, these numbers are almost solely due to the fact tech firms have chosen to base themselves in those jurisdictions, and these are where the vast majority of fines for the Irish and Luxembourgish DPAs derive.

. If you remove fines from Amazon, Google and Meta, the average value of fines is generally quite low. For Ireland this tends to be below €750,000 and for Luxembourg below €20,000. To give you a clear understanding, without Amazon's fine Luxembourg sits at €311,500 for their total fine amount, and Ireland at €2,840,900 without the fines issued to Meta.

What drives the differences between DPAs and enforcement?

We have established at this stage that there are considerable differences to how DPAs enforce the GDPR. However, it does prompt the question as to why this should be the case. In the first instance, it does appear that different DPAs have different focuses entirely.

For instance, Spain with its 'high volume, low value' fine philosophy seems to focus on enforcement considering more 'administrative' aspects of GDPR breaches.

304 fines issued by the Spanish DPA relate to Article 5 (Principles relating to processing of personal data), 227 relate to Article 6 (Lawfulness of processing), and 154 relate to Article 13 (Information to be provided where personal data are collected from the data subject).

And when focus on the most common range of fine values (€1000-€10,000) 91 of them focus on Article 13. It does appear that the Spain DPAs approach brings it to focus on lower-value fines and infractions.

What drives the differences between DPAs and enforcement?

We have established at this stage that there are considerable differences to how DPAs enforce the GDPR. However, it does prompt the question as to why this should be the case. In the first instance, it does appear that different DPAs have different focuses entirely.

For instance, Spain with its 'high volume, low value' fine philosophy seems to focus on enforcement considering more 'administrative' aspects of GDPR breaches. 304 fines issued by the Spanish DPA relate to Article 5 (Principles relating to processing of personal data), 227 relate to Article 6 (Lawfulness of processing), and 154 relate to Article 13 (Information to be provided where personal data are collected from the data subject). And when focus on the most common range of fine values (€1000-€10,000) 91 of them focus on Article 13. It does appear that the Spain DPAs approach brings it to focus on lower-value fines and infractions.

This particularly appears to be the case when we look at the UK where many of the fines relate to Article 32 – which concerns the security of processing – with France's CNIL also often citing Article 32 (14 in total). Determining a breach around security and determining its seriousness generally involves a thorough investigation into an organisation's controls and environment, culminating in the types of detailed reports we see in the ICO's Monetary Penalty Notices, where infractions and punishments are outlined in with a granular level of specificity. This requires a good amount of time, personnel, and expertise.

Certainly, in comparison, administrative breaches are more black and white – though often seen as less 'serious' and thus only qualifying for lower fines. So, why the difference between Spain's DPA and its colleagues in France and the UK? Is it the case, therefore, that Spain's DPA lacks some of the resources to go after more complex investigations that bring bigger fines? Their budget suggests that this may well be the case.

What drives the differences between DPAs and enforcement?

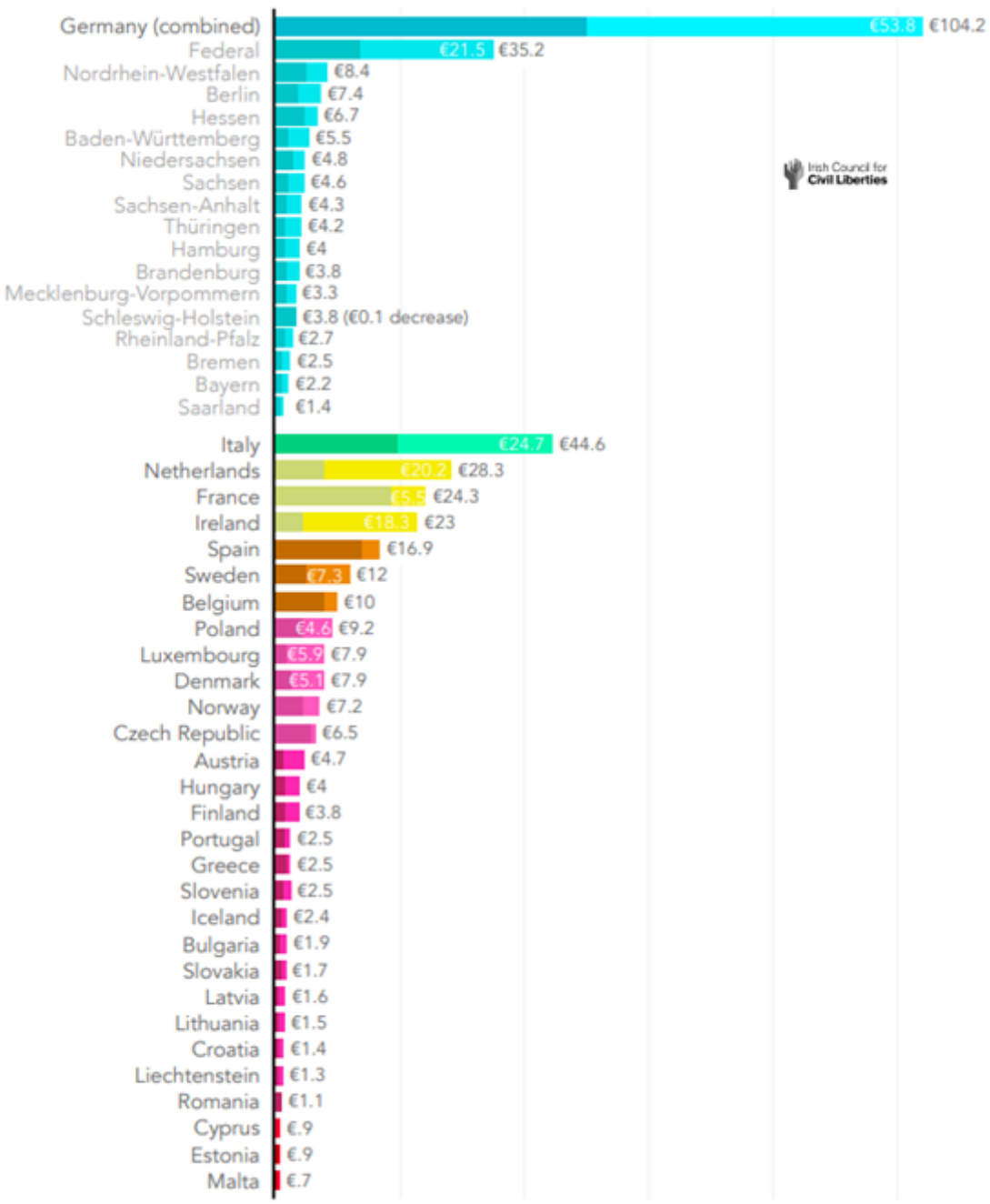


Chart 3 - DPA Budgets in Millions from 2016 (darker) to 2022 (lighter) – EU countries only (Source: Irish Council for Civil Liberties 2023 report on EEA data protection authorities)

What drives the differences between DPAs and enforcement?

Chart 3 shows the budgets of European DPA's between 2016 and 2022. An immediate takeaway here is that France's CNIL has a significantly higher budget in 2022 (€24.3 million) than Spain (€16.9 million). The CNIL has also enjoyed a larger increase over the period (€5.5 million) since 2016. It is perhaps no surprise, then, that the CNIL has more in its arsenal to go after complex cases targeting the likes of Google and Facebook.

This is perhaps strengthened by looking at the UK, not presented in Chart 3 by dint of having left the EU, with the ICO's budget coming to €61 million, also allowing the body to work on more in-depth investigations.

This picture appears reinforced when you take the example of Germany, where the federal and regional combined budget was €104.2 million in 2022. Germany does not make its figures available for all fines, but it is worth noting that it has given out the largest non-tech fine to retailer H&M (€35 million in 2020).

The same trend can be seen with second-placed Italy (€44.6 million budget in 2022). Italy has given out both a lot of fines under the GDPR (260) and to a relatively large value (over €123 million) – see Chart 2.

What drives the differences between DPAs and enforcement?

With Italy's DPA, the average fine value is fairly low (216 of the 260 fines all being €20,000 or under) but the authority has managed to conclude a number of high-profile and complex investigations: e.g., fines for Telecom Italia (€27.8 million in 2020), Enel Energia (€26.5 million in 2022) and Wind (€17 million in 2022) being three of the largest in the GDPR history.

It is telling also that Ireland, ahead of its record fine against Meta in May 2023, has seen its DPA's budget climb rapidly since the GDPR become enforceable, becoming the fifth highest in Europe in 2022 at (€23 million).

Quite clearly, the more money a DPA has in its budget, the more chance it has of executing intricate investigations, which also tend towards larger fines – though potentially fewer of them. This may seem something of an obvious, even facile, explanation, but the data shows this unambiguously.

The future of DPAs and GDPR enforcement

If we can take anything from the gargantuan €1.2 billion fine issued to Meta in May 2023, it's that DPAs are not afraid to go after large organisations. No one is untouchable and complex, years-long probes are no longer off the table.

There is a school of thought that going after multinationals with expensive and aggressive legal teams was something of a folly for a public regulatory body and that the fine is always likely to be reduced if the matter goes to court. That fear no longer seems to persist.

The combined budget of EEA DPAs (UK excluded) has doubled since 2016, from €167.1 million to €337.6 million in 2022. These authorities are, generally speaking, well-funded, increasingly well-resourced, and capable of taking on giant firms and cases.

DPAs also understand that they need to evolve to meet growing trends and developments, with many setting up specialist AI divisions – the Dutch data protection body, for example, has already opened a new algorithm oversight division, with a budget of €1 million in 2023 that will increase to €3.6 million by 2026.

The trend for tighter enforcement and bigger fines is only growing. The European data protection regime is not perfect (10 national DPAs still have budgets under €2 million and cross-border EU complaints often fall flat due to a lack of coordination) but the momentum, as the data shows, is unmistakable.

Article II:

ICO vs the Tech Giants: Data and the Rights of Individuals

ICO vs the Tech Giants: Data and the Rights of Individuals

Much like its EU equivalents, the Information Commissioner's Office (ICO), the UK's independent regulator for data protection and privacy, has high expectations when it comes to organisations taking individual responsibility for maintaining standards of privacy and data protection.

Critically, the ICO expects firms to be extremely proactive and vigilant around risks in this regard. Working to ensure that there is adequate security around data, that a lawful basis for processing exists, and that data subjects are treated fairly and their rights observed, are requirements that the ICO and other Data Protection Authorities (DPAs) are always looking for from organisations.

DPAs, notably the ICO, have indicated that they want to see the right behaviours and attitudes from organisations regarding data protection.

The ICO has repeatedly warned that the biggest cyber risk to an organisation is not a 'hacker,' but in fact complacency; companies leaving themselves open to cyber-attacks through lack of due diligence are warned to expect fines by the ICO.

Of course, many organisations fail in demonstrating the adequate level of complacency-avoidance the ICO and others demand – and are sanctioned accordingly. No sector, however, appears to receive quite the attention the tech industry does in this regard – and recent record fines, the most recent being a staggering €1.2 billion issued to Meta in May 2023, show no sign of this trend abating.

Singled out by DPAs?

It takes little more than a casual understanding of data protection and privacy developments to know that tech giants are very regularly in the firing line. Nine of the ten largest GDPR fines (as of 22 May 2023) have been issued to firms in this sector – notably Amazon, Google and Meta.

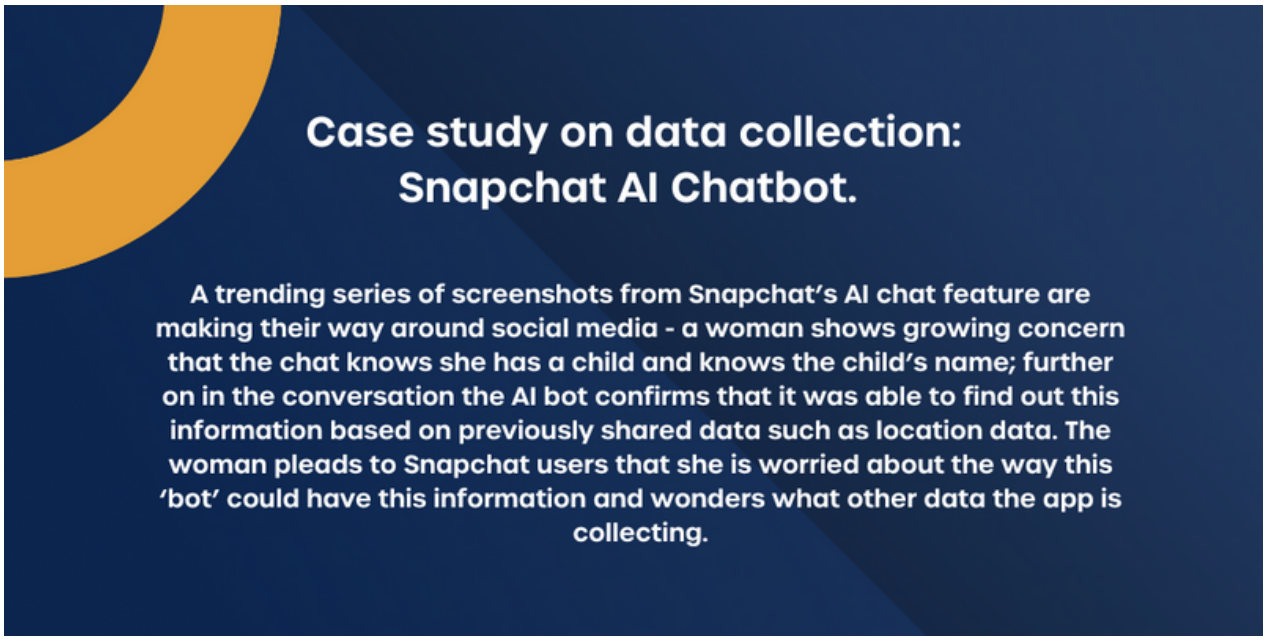
These fines, headed by a record €1.2 billion penalty given to Meta in May 2023 (beating the former record of €746 million issued to Amazon in 2021), have been levied against tech firms with an increasingly regular basis – and with values that dwarf those given to other companies.

To illustrate this point, the largest fine given to a non-tech firm was €35.3 million, received by retailer H&M in 2020 by the Data Protection Authority in Hamburg, Germany, for illegal surveillance of its employees. This, while undoubtedly serious, would not even make it into the top 10 of GDPR's largest fines.

The question, then, is why do tech firms tend to butt up against DPAs so much? One could look at the millions of euros in fines and conclude that tech giants might be valuable cash cows for regulators, there is an underlying perception in the public sphere that their attitude towards data handling is lax and their respect for data rights severely lacking.

Too much data, not enough rigour?

Tech firms process huge volumes of personal data, particularly given that many rely so heavily on using that data for revenue-generating purposes – generally targeted and non-targeted advertising. The sheer amount of data collected – including everything from location information to browsing history and biometric data – presents a large risk to data subjects, especially given it is often collected without the individuals' realisation or understanding.



Too much data, not enough rigour?

With this high-volume processing comes a large amount of responsibility, in terms of keeping that data secure, respecting the rights of individuals and ensuring that individuals are informed about how their data is being used. Whilst data can be used for a variety of purposes, under the UK/EU GDPR it should be collected for an explicit legitimate purpose and not processed beyond that – and individuals should understand that purpose and the implications of the processing on them.

Tech giants have regularly been criticised for a lack of transparency around data collection and use. Many tech companies have murky policies when it comes to data privacy, and it can be difficult for individuals to understand exactly what information is being collected and how it is being used.

This is, admittedly, not always easy to do correctly (be it through appropriate privacy notices or other means), but it is a vital obligation under data protection regulations – and ultimately is underlined by the desire of an organisation to act transparently and in good faith towards their users and customers.

Too much data, not enough rigour?

Tech firms have habitually fallen foul of this requirement. There have already been numerous instances of tech companies being accused of using their data and algorithms to manipulate users - from the Cambridge Analytica scandal to accusations of bias in search results and social media algorithms – and, bearing this in mind, it is little wonder that they have attracted so much scrutiny from regulators and distrust from the public at large.

A welfare issue – processing children's data

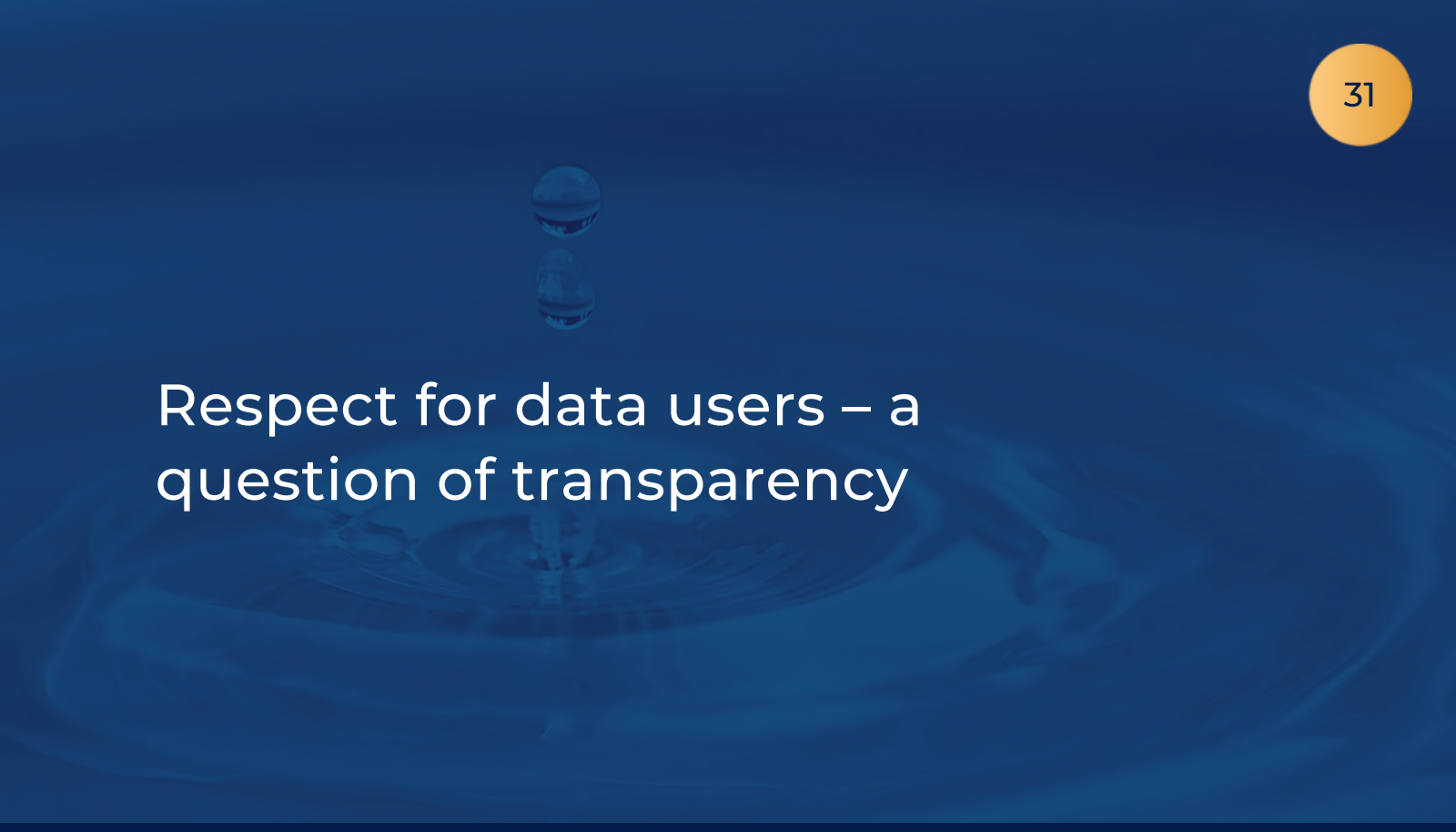
One of the largest, and most contentious, pitfalls that customer-facing firms have is processing children's data. This is particularly important for social media providers where there is a high likelihood of children wanting to use their services and therefore having their data processed.

The UK/EU GDPR make special provisions for protecting children's data intended to enhance the protection of children's personal data and to ensure that children are addressed in plain, clear language that they can understand – especially where parental consent is not required or received.

Regulators take a dim view of firms not adequately protecting children's data rights – and tech firms have been found wanting in this regard on several occasions.

In the UK, we have recently seen tech giant TikTok receive a £12.7 million fine for several data protection breaches including failure to use children's personal data lawfully and failure to implement policies it laid out in order to protect children.

As with most aspects of data protection compliance, there are no easy solutions to the problems firms face here, but appropriate rigour (risk assessments, child-friendly design, transparency, limiting features on children's profiles (e.g., geolocation being turned off) and preventing children's data being shared) will get you a long way. This rigour, however, is all too often absent.



Respect for data users – a question of transparency

The modern world is complicated with regards to data. With increasing numbers of users of online platforms, apps, browsers etc. we cannot expect every person to fully understand their rights as an individual. There are a plethora of examples concerning tech companies that illustrate this, where firms are using data in a manner that their customers might not expect or understand.

Take behavioural advertising, sending ads targeted using user-profile information, for example.

Meta was fined €390 million in January 2023 by the Irish Data Protection Commission (DPC) for relying on contract terms as a lawful basis for personalised advertising on Instagram and Facebook.

The DPC ruled that using terms when people sign up for Meta's platforms as a basis for behavioural advertising was invalid. This seems like a reasonable conclusion – how can users be sure what their data is being used for if they don't provide informed and explicit opt-in consent?

Respect for data users – a question of transparency

Another potential issue is international data transfers. Transfers of personal data between the EU and US (where the Metas, Googles, Amazons and Apples of this world are typically based) are viewed sceptically by Europeans, particularly given the possibility of the US government using this data for surveillance. This creates a danger for the rights of UK and EU nationals to be undermined – particularly if their data is sent to the US without their knowledge and without appropriate additional safeguards being implemented. This is exactly what prompted the DPC to fine Meta a colossal €1.2 billion in May 2023 after a decade-long complaint.

Tech firms need to be responsible partners in protecting individuals' data. Ensuring that there is data privacy by design – where rights and freedoms of users are considered at the set-up phase of a project – is vitally important. Equally so is ensuring that users have a clear choice and meaningful control over their data usage while organisations show that there is genuine transparency and accountability on their side.

A long road ahead

With the vast amounts of personal information that tech companies collect and store, many data savvy individuals are worried about how this information is being used and who has access to it, there is also concern about the potential for abuse; with so much personal information at their disposal, these companies have the power to shape public opinion and even influence political outcomes.

Data privacy and data protection is complex and multifaceted; it will require a concerted effort from individuals, governments, and the tech industry itself to find solutions that balance the benefits of technological innovation with the need to protect privacy and individual rights. This is all the more important with the rise in prevalence of sophisticated AI solutions and new technologies that could benefit companies at the expense of the rights of individuals.

GDPR is certainly beginning to show it has teeth – though many of the rulings made against tech giants (notably Meta's €1.2-billion Amazon's €746 million fines) are being fiercely fought in the courts and it remains unclear what changes these penalties will drive to the benefit of data subjects at large.

For now, individuals need to remain vigilant when disseminating their data. Of course, tech giants bring lots of real-life benefits, making the world more connected and many services more innovative and easier than access to ever. However, understanding how that data is being used is often hard to disentangle and the tech giants have shown that they have a way to go to demonstrate the accountability and good practice DPAs demand.

Looking Forward

The Future of The GDPR

Article III:

The great data protection gamble – could the UK's post-Brexit stance mean the end of EU data adequacy?

The great data protection gamble – could the UK's post-Brexit stance mean the end of EU data adequacy?

The UK's departure from the EU has not been a smooth journey. However, away from the protracted saga that was the conclusion of the EU-UK Trade Cooperation Agreement, there has been a singular apparent oasis of calm – data protection regulation. To date, UK and European businesses have been spared any disruption concerning the transfer of personal data. The UK government has retained the EU's General Data Protection Regulation (GDPR) in law meaning that such transfers can occur freely – at least for now.

The retention of this status quo regarding personal data transfers is rooted in the European Commission's adequacy decision in July 2021, where it established that the UK's regulatory framework was sufficient to guarantee privacy safeguards comparable to EU standards.

This was hardly surprising given that the UK had only just left the EU, but it is worth noting that this decision is far from permanent and sits on very shaky foundations.

The current adequacy decision is expected to last until June 2025 after which it would need to be extended by the European Commission. However, this extension is no certainty and, particularly with the UK government signaling intent to relax its regulatory framework, it may only be a matter of time before EU-UK personal data transfers become significantly more difficult.

How the EU establishes adequacy

Before looking at why the UK's adequacy is in jeopardy, it is worth establishing how the EU makes such decisions. The adoption of any adequacy decision involves a series of steps, including 1) a proposal from the European Commission; 2) an opinion from the European Data Protection board; 3) an approval from EU members' representatives; and finally, 4) the adoption of the decision by the European Commission.

Two observations immediately spring from this. Firstly, this is a very involved process with input needed from three distinct institutions. The result is that there is no guarantee that gaining adequacy is a swift process. In fact, the shortest timeframe for an adequacy decision to be made thus far is 18 months (in the case of Argentina) – meaning that if the UK was ever cast adrift, regaining adequacy would be far from immediate.

How the EU establishes adequacy

The second point to note is that the European Commission plays a pivotal role in this process. Article 45 of the GDPR outlines the elements that the Commission must take into account concerning awarding adequacy to a non-EU country, namely:

1. the rule of law, respect for human rights and fundamental freedoms, relevant legislation implemented by the country in question – including, data protection rules, professional rules, and security measures, including rules for the onward transfer of personal data to another third country or international organisation;
2. the existence and effective functioning of one or more independent supervisory authorities; and,
3. any international commitments or legally binding conventions the third party being assessed for adequacy has entered into.

Clearly, this is a wide remit for considerations and goes significantly beyond a country seeking adequacy having a strong data protection regime – which goes a long way to explaining why the UK's status is so under threat.

The potential consequences of the UK's bullish data protection strategy

In March 2023, Michelle Donelan, the Secretary of State for Science, Innovation and Technology, re-introduced the Data Protection and Digital Information Bill in UK parliament. This bill is the centerpiece of the UK government's new data protection strategy, which seeks to keep many of the fundamental aspects of the GDPR whilst being a "business-friendly" framework.

Key points introduced by the bill include:

- Changes to consent requirements to facilitate scientific research;
- Simplifying 'legitimate interest' as a basis for processing by introducing a list of "recognised legitimate interests";
- Increased fines for improper direct marketing;
- Replacing the Data Protection Officer (DPO) with a Senior Responsible Individual ("SRI");
- Continuity regarding international transfers;
- Relaxing rules on cookies to 'cut red tape'; and,
- Abolishing the Information Commissioner's Office (ICO), the UK regulator, to be replaced by an Information Commission.

The potential consequences of the UK's bullish data protection strategy

The end goal, ultimately, is to make life simpler and cheaper for businesses (the UK government predicts that these changes, by lessening the administrative burden, will save businesses £4.7 billion) while preserving data subjects' rights. This sounds perfect in theory – but big questions remain over whether this idyllic vision will be realised quite so effectively in practice.

The EU expressed concern about the UK's data protection regime before the Data Protection and Digital Information Bill was even a notion. In 2016, for instance, the European Court of Justice ruled that the UK's Data Retention and Investigatory Powers Act actually breached EU law by allowing "general and indiscriminate" retention of individuals' data by law enforcement agencies. A similar ruling in 2017 also critcised the UK government's approach to gathering large volumes of data in investigations, recommending that the UK be "more careful" and justify its requirements for doing so.

Bearing in mind this concern over government surveillance, combined with fears about what the proposed divergence in law outlined above might lead to with regards to data subject rights, it is no surprise that the UK's adequacy decision might not find too many proponents in European circles.

This is without even considering the UK's legislative strategy in other areas – such as threats to withdraw from the European Convention on Human Rights to facilitate the deportation of asylum seekers to Rwanda or the introduction of the potentially invasive Online Safety Bill – introduce more divergence in the areas of human rights, a factor which is considered when assessing adequacy by the EU.

Scenarios for the UK losing adequacy

Considering all of this, it is worth examining the scenarios that could lead to adequacy being removed. The following represent the most likely avenues of this occurring:

1. **Legal challenges by privacy activists**. There is certainly precedent for the EU to make a ruling on adequacy only for individuals to challenge this in the courts and have it overturned. As things stand, the status quo serves the EU well, given there is an economic benefit to making data flows between the EU and UK restriction-free. However, this economic rationale would go out of the window if someone like Max Schrems, the Austrian privacy campaigner who has twice successfully challenged the legitimacy of EU-US transfer mechanisms, was to make a formal case to the European Court of Justice (ECJ).

   It is worth remembering that US adequacy was annulled due to concerns that private citizens' data could end up in the hands of US security services. Considering UK national security laws have had similar concerns raised about them (see above), it is not hard to imagine that a complaint could be made against the UK in the not-too-distant future.

Scenarios for the UK losing adequacy

2. **The UK diverges too far**. The EU may have a certain tolerance for the UK's data protection – particularly while there is an economic and political benefit to keeping relations strong and data flows simple – but there is a point at which the UK could go too far. If the EU deems that UK legislation is too far from the standard required, adequacy could be removed very quickly.

   Both the European Parliament and the Council of Ministers can ask the European Commission to amend, or withdraw, an adequacy decision at any time if they feel the UK has lowered its privacy standards and put EU data subjects' rights at risk.

3. **The UK tries to circumvent EU rules**. The UK may simply push things too far by trying to placate its global partners by allowing free cross-border transfers with the likes of Australia and the US – countries the EU does not consider adequate. The EU is likely to take a dim view if EU citizens' data ends up being transferred to a 'non-safe' third party country just because the UK wants to realise its global ambitions.

The other point to make here is that data privacy could be used simply as political leverage. It does not take much of a leap of imagination to conjure an instance where the EU might want to exert some pressure on the UK, for instance with regards to Northern Ireland, and may choose adequacy as a tool to achieve this. The UK has robust privacy laws (much more so than currently 'adequate' New Zealand, for example) but that may not be enough for the EU to consider the UK government a 'reliable partner' in the sphere of data protection.

Consequences for UK-European business

The final and most pertinent question around adequacy remains however – why should anyone care? Sure, the UK might not be able to send data back and forth between the EU quite so easily, but is this really such a problem?

It is possible that, for a business that has no dealings with EU clients, this will have relatively little direct impact. However, for the many organisations who do interact with EU nationals and entities, the effects will be profound. Losing adequacy will likely mean a) an increased cost of doing business, involving more compliance and contractual measures over data transfers; b) a reduction in trade; c) reduced investment; d) relocation of businesses out of the UK; and e) a risk of increased GDPR finds by EU regulators.

It is hard to quantify what this disruption would mean for businesses. The UCL European Institute published a report in November 2020 where it estimated that compliance costs alone could be as much as £3,000 for a micro-business, £10,000 for a small business, £19,555 for a medium business and £162,790 for a large business – costing an aggregate of around £1-1.6 billion. This, however, is without considering the wider economic impact on the UK.

Losing adequacy is both highly possible and highly damaging for the UK. Businesses should brace for negative impacts and costs if this happens and start contingency planning now.

Ensuring that you have the requisite data privacy and protection program in place – with suitable Data Privacy Impact Assessments, Transfer Impact Assessments, and facility to include contractual safeguards (such as Standard Contractual Clauses) in any agreements concerning the transfer of EU data – and the right personnel and processes to manage it, will go a long way to preparing for the worst.

Single organisations cannot do much about the EU's adequacy decision – and even the UK government maintaining a world-class data protection schema and retaining alignment with the EU GDPR might not be enough. However, preparation can at least soften the blow.

Article IV:

Shifting sands and personal liability – is the Data Protection Officer role only becoming more challenging?

Shifting sands and personal liability – is the Data Protection Officer role only becoming more challenging?

The role of the Data Protection Officer (DPO) has never been a straightforward one. Article 39 of the EU/UK General Data Protection Regulation (GDPR) sets out what the DPO's key responsibilities are – advising on data protection obligations; monitoring and promoting compliance with data protection in an organisation; overseeing Data Protection Impact Assessments; cooperating with supervisory authorities; and acting as a point of contact for any data protection-related matters.

Fulfilling these tasks is no trivial matter and requires an individual with a relatively broad skillset. In effect, it demands someone who understands the requirements of the GDPR (and potentially other data protection regulations) deeply, who has a knowledge of technology and security controls, who knows how to manage change and develop policies and procedures, and someone who can convince others and achieve buy-in for their initiatives.

The interesting thing about the DPO role is that it initially started as essentially just interpreting the GDPR and translating it for others in a business, but it has now become much more profound. DPOs today are expected to take a proactive role in guiding organisations towards more responsible and ethical data use and are increasingly strategically focused (particularly with personal data implications having to be considered in many cases where new systems and processes are implemented).

There is no shortage of challenges in this regard - technologies are becoming more complex (with DPOs having to consider the development of AI tools, AdTech, MedTech, the Internet of Things and their consequence among others) and the global regulatory landscape constantly shifting, as evidenced by the UK's proposed changes in the Data Protection and Digital Information Bill (more on that later). It might make you wonder – who would be a DPO?

A cornerstone of a company's accountability requirements

Accountability is one of the key data protection principles under the GDPR, requiring companies to be able to actively demonstrate their compliance with the regulation. There are a number of ways this can be achieved – such as introducing data protection policies and procedures, implementing data privacy by design and default and having suitable technical controls in place – but one which many organisations will opt for is to appoint a DPO.

Not everyone has to appoint a DPO of course – the compulsory requirement is reserved for public bodies, organisations whose core activities consist of regular and systematic monitoring, or whose core activities consist of processing special category or criminal data on a large scale – but many organisations choose to do so. And that approach makes a lot of sense – having a single person devoted to data protection is a good way to make sure that bases are adequately covered.

A cornerstone of a company's accountability requirements

However, it is not always practical for an organisation to have a full-time DPO, particularly if it is a small entity with a tight budget. In these circumstances, firms may choose to contract out the position of DPO to a third-party (a 'virtual-DPO' service) or indeed ask a member of staff to 'double-hat' and act as a DPO alongside their 'day job'. The GDPR allows for both options, but with a caveat. If we examine Article 38 (6) of the GDPR, we see the following:

> *"The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests."*

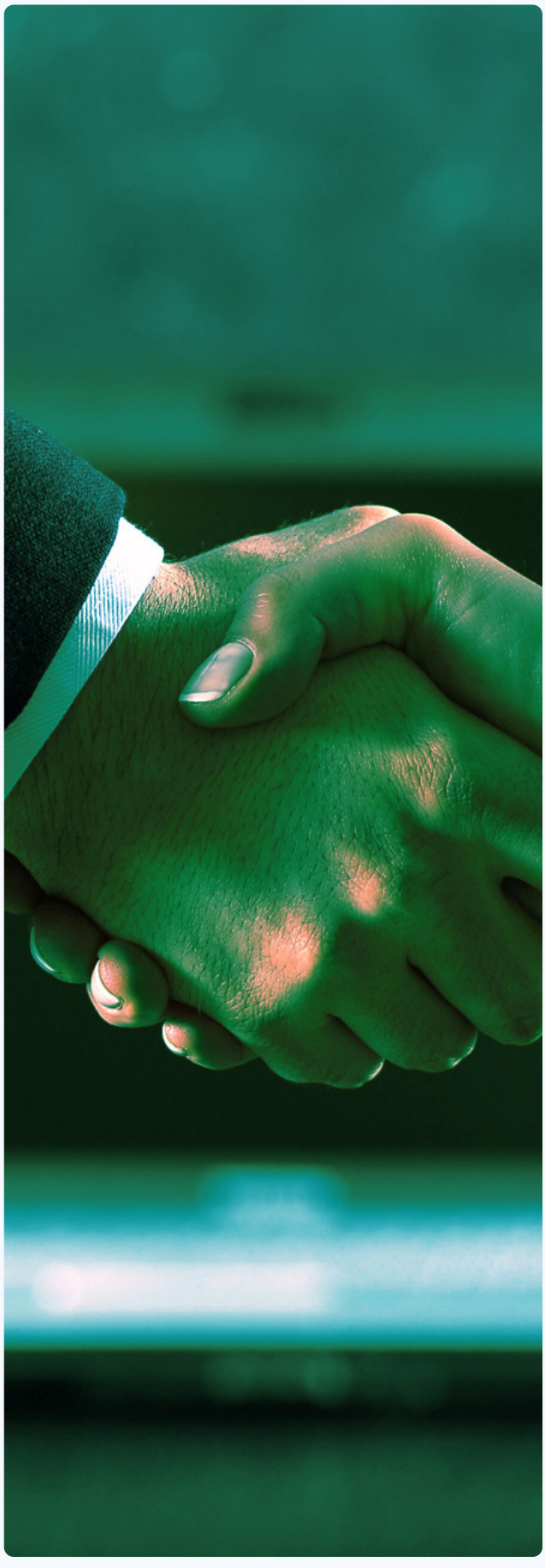
The key thing to note here is 'conflict of interests'. The DPO, whether internal or external, must be able to act independently. This means there must be a job description (or a formal contract), resources to help the DPO fulfil their responsibilities (such as budget and mandate to employ external legal counsel), and they must be given license to carry out their duties without interference.

Ideally, this should mean that, within an organisation's governance structure, they sit somewhat to the side and report directly to the most senior management. Most importantly though, given the responsibility that a DPO has – conducting audits, leading post-breach investigations, providing advice – they absolutely must be able to work without being pressured into a particular direction. After all, could a DPO be called 'independent' if they report to a manager who makes it clear that they must work towards a defined outcome?

A cornerstone of a company's accountability requirements

The other point to reiterate is that the DPO position is a skilled role. Ongoing training and professional development are paramount to ensure that a DPO is equipped with the necessary knowledge and skills to effectively carry out their duties – and organisations should make sure they can provide this. Without adequate training, it is hard to imagine that any individual can competently navigate the ever-evolving landscape of data protection laws, best practices, and technological advancements.

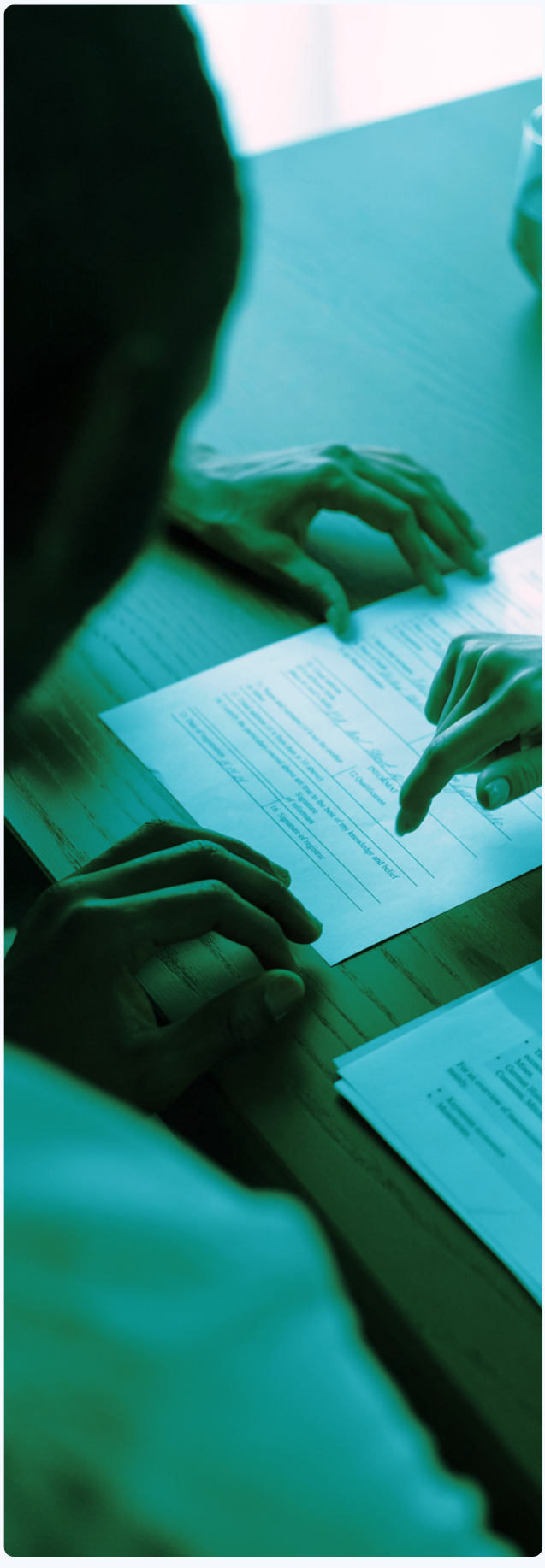
Organisations have an obligation under the GDPR to support their DPO, ensuring that they are involved in data protection matters in good time, operate independently, and have the right resources, access, and support to conduct their duties. The DPO isn't in themselves responsible for compliance – the organisation that employs them is – but they are integral to showing that a business is meeting its responsibilities. However, there are signs that a DPO may not always be shielded from personal blowback where there is a breach in GDPR compliance.



A cornerstone of a company's accountability requirements

Accountability is one of the key data protection principles under the GDPR, requiring companies to be able to actively demonstrate their compliance with the regulation. There are a number of ways this can be achieved – such as introducing data protection policies and procedures, implementing data privacy by design and default and having suitable technical controls in place – but one which many organisations will opt for is to appoint a DPO.

Not everyone has to appoint a DPO of course – the compulsory requirement is reserved for public bodies, organisations whose core activities consist of regular and systematic monitoring, or whose core activities consist of processing special category or criminal data on a large scale – but many organisations choose to do so. And that approach makes a lot of sense – having a single person devoted to data protection is a good way to make sure that bases are adequately covered.



The probability of liability?

There is a lot that can go wrong with regards to personal data. A company has an obligation to make sure that breaches that impact data subjects adversely are reported and otherwise ensure that data is processed securely, lawfully, and transparently.

Generally, the guidance provided by data protection experts is that a DPO is not personally liable for compliance with the GDPR and the organisation employing them is ultimately culpable if anything goes wrong. The question, however, is whether this will be the case in every instance.

While the GDPR does offer protections for DPOs, it does not completely protect them from all liability. Article 38 of the GDPR stresses that DPOs cannot be "dismissed or penalised" for doing their jobs; however, it does not discuss what might happen if a DPO fails to do their job and commits an error that results in serious regulatory enforcement action, particularly they are deemed to have acted negligently.

The concept of individual negligence resulting in legal ramifications for an individual (particularly when a company suffers damage due to that negligence) is far from unheard of. Even if a company chooses not to punish or dismiss an employee in those circumstances, customers or shareholders may also look to file damages if a DPO is directly responsible for a breach that adversely impacts them or indeed a company's share price.

The probability of liability?

One real-world, if not directly related, example that highlights the possibility of personal liability in such a case concerns Joe Sullivan, the former Chief Security Officer (CSO) of Uber. In 2022, Sullivan was found guilty by a court in San Francisco of criminal obstruction for failing to report a 2016 cybersecurity incident to authorities and was sentenced to three years' probation.

This is a case that should be viewed with interest by DPOs. Here we have a person in a position of responsibility who was found to have been negligent for not reporting a breach and was subsequently convicted of a felony. Granted, this was in an entirely different jurisdiction to where the EU/UK GDPR operates but it raises an interesting question - could this situation play out if a DPO was similarly found guilty of malicious (or incompetent) non-reporting of a breach? There is no real precedent for this happening to a DPO but, equally, it cannot categorically be ruled out

DPOs can certainly protect themselves to some degree from this. Directors and Officers (D&O) insurance, which provides coverage for directors and officers in case of civil or criminal actions, is a sensible avenue to consider– and given its ubiquity for senior management, should certainly be appropriate for DPOs.

Aside from this, the DPO must ensure that they are vigilant, both to what is happening in an organisation that they represent, and to what their obligations and entitlements are. A DPO should push for their employer to act within their responsibilities (providing independence, resources and freedom for the DPO to act) and ensure, critically, that they document their activities and requests.

For example, if a DPO was to give crucial advice concerning data protection that was subsequently ignored by senior management, it would be highly advisable to make note of this, ideally in meeting minutes. Certainly, if the threat of liability could dangle over your head, it would make sense to protect yourself as much as possible.

DPOs in a post-Brexit world

As discussed throughout this article, the DPO role is complex and has evolved considerably throughout its short history. Those changes seem to be continuing in the UK where the UK's Data Protection and Digital Information Bill is seeking to remove the position entirely, replacing it with a requirement for a Senior Responsible Individual (SRI).

Much like a DPO, only certain companies will need to appoint an SRI – public bodies and those whose processing activities are considered high risk. The key point here is that, while the duties of an SRI and a DPO are broadly analogous, the former must be occupied by a senior management figure (and not outsourced), assigned to be carried out alongside someone's normal role, and with the opportunity to share duties amongst two or more people.

If we assume for now that the bill will be passed (the second iteration was introduced in March 2023), it raises two immediate questions – 1) does this eliminate the DPO role in the UK; and 2) is this a positive development? In short, particularly at this early stage, potentially 'yes' and 'no'.

DPOs in a post-Brexit world

In reality, many of the obligations required of a DPO apply to SRIs (monitoring compliance, running awareness campaigns etc.), but the proposed legislation is also meant to reduce some of the bureaucracy and admin that accompanies the GDPR. However, while it may cut some red tape, the bill potentially neglects to ensure that much more fundamental aspects of data protection are observed, at least with the SRI role – expertise, rigour and freedom from conflict of interest. And those omissions run the risk of undermining the entire data protection regime.

A look to the future

The danger with lowering the standards – which is what the UK reforms may do – is that it results in a data protection regime that is no longer robust enough to protect individuals' rights. One concern in this respect is whether the 'senior management' appointees would be skilled, experienced or time-rich enough to do justice to the position, even if it is split between parties, and what the ramifications might subsequently be for companies managing personal data and the data subjects themselves.

This is without considering whether being compliant with the UK regulation will be sufficient to satisfy the requirements of the EU GDPR, potentially meaning that some organisations in the UK will have the challenge of observing (at least) two distinct sets of regulations. Surely, that is exactly the sort of challenge that would be befitting of a dedicated, trained resource who is an expert in data protection?

While we might see changes in the DPO role, it will not simply disappear. The position has evolved to the point where it has a wide remit and one which can help shape a company's compliance, risk management and strategy towards implementing technology and processes.

The skillset of a top-class DPO has elements belonging simultaneously to a lawyer, a head of IT, a cybersecurity professional, a head of operations and an adept communicator. This isn't a job just anyone can do, especially without the right support and environment to thrive. And that brings us back to an earlier question – who would be a DPO? As the role continues to grow in complexity and stakes continue to rise, we may find that it becomes only more difficult to answer.

Meet the Team

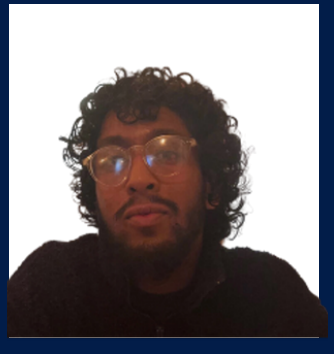
Introduction and foreword:
Luke Hull, Cyber Security Manager, Reliance Cyber

Luke is a seasoned Information Security professional with over 22 years of experience in managed and consultancy services. He has a strong background in threat intelligence and has played a pivotal role in transforming detection and response capabilities for major organisations in EMEA. Luke's expertise extends to integrating AI capabilities with incident response and MDR services. With a focus on intelligence-led approaches and automation, Luke brings high-value capabilities to clients at Reliance Cyber

Author:
Andrew Wychrij, Cyber Security Manager, Reliance Cyber

Andrew Wychrij is a highly dedicated security professional specialising in information security and data privacy. With a profound understanding of regulatory and business challenges, Andrew excels in assisting clients in comprehending and mitigating risks to their businesses. With a pragmatic approach, Andrew constructs comprehensive cyber security programs that precisely align with clients' specific requirements, ensuring robust protection against the evolving regulatory environment.

Contributor:
Imnul Ali, Cyber Security Consultant, Reliance Cyber



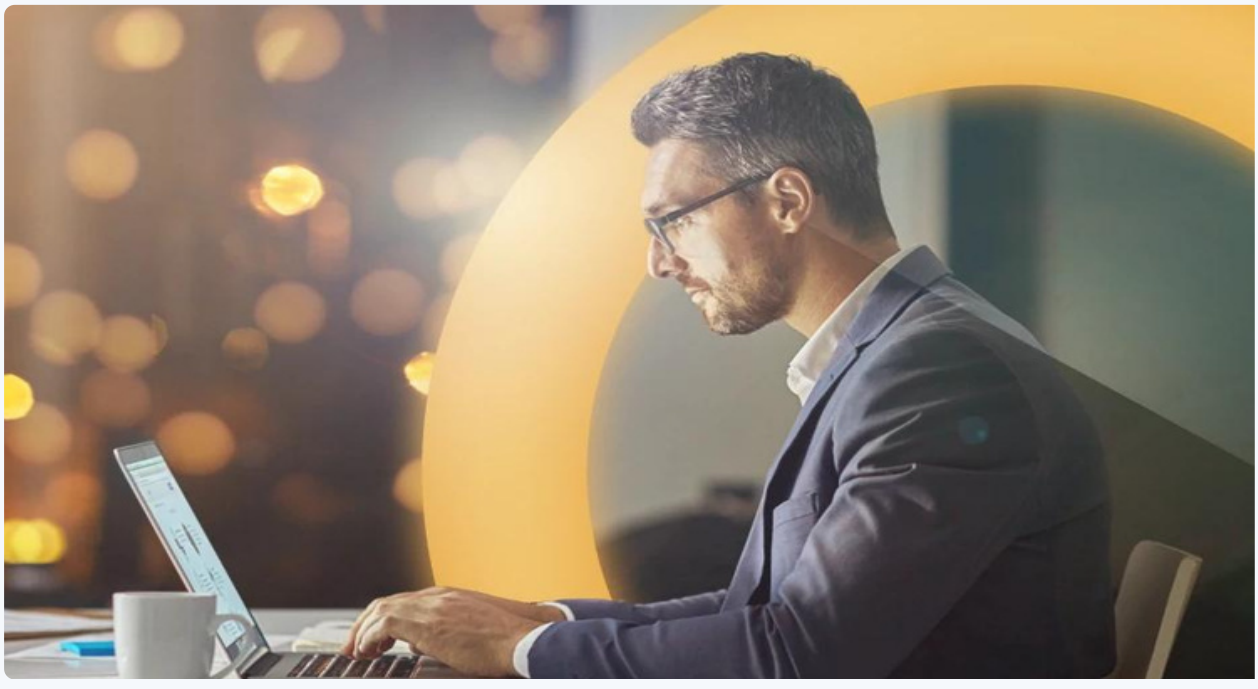
Imnul Ali is a skilled Software Engineer with a focus on governance, risk, and controls. His attention to detail and commitment to maintaining compliance makes him a valuable asset in addressing governance and risk challenges.

Contributor:
Katherine Arthur, Cyber Security Consultant, Reliance Cyber

Katherine Arthur is a highly skilled Data Scientist, ISO/IEC 27001 Provisional Implementer, PCI Professional (PCIP), and Cyber Security Consultant. Katherine's expertise in ISO/IEC 27001 and PCI compliance enable her to effectively address complex security challenges and safeguard critical assets for organisations.

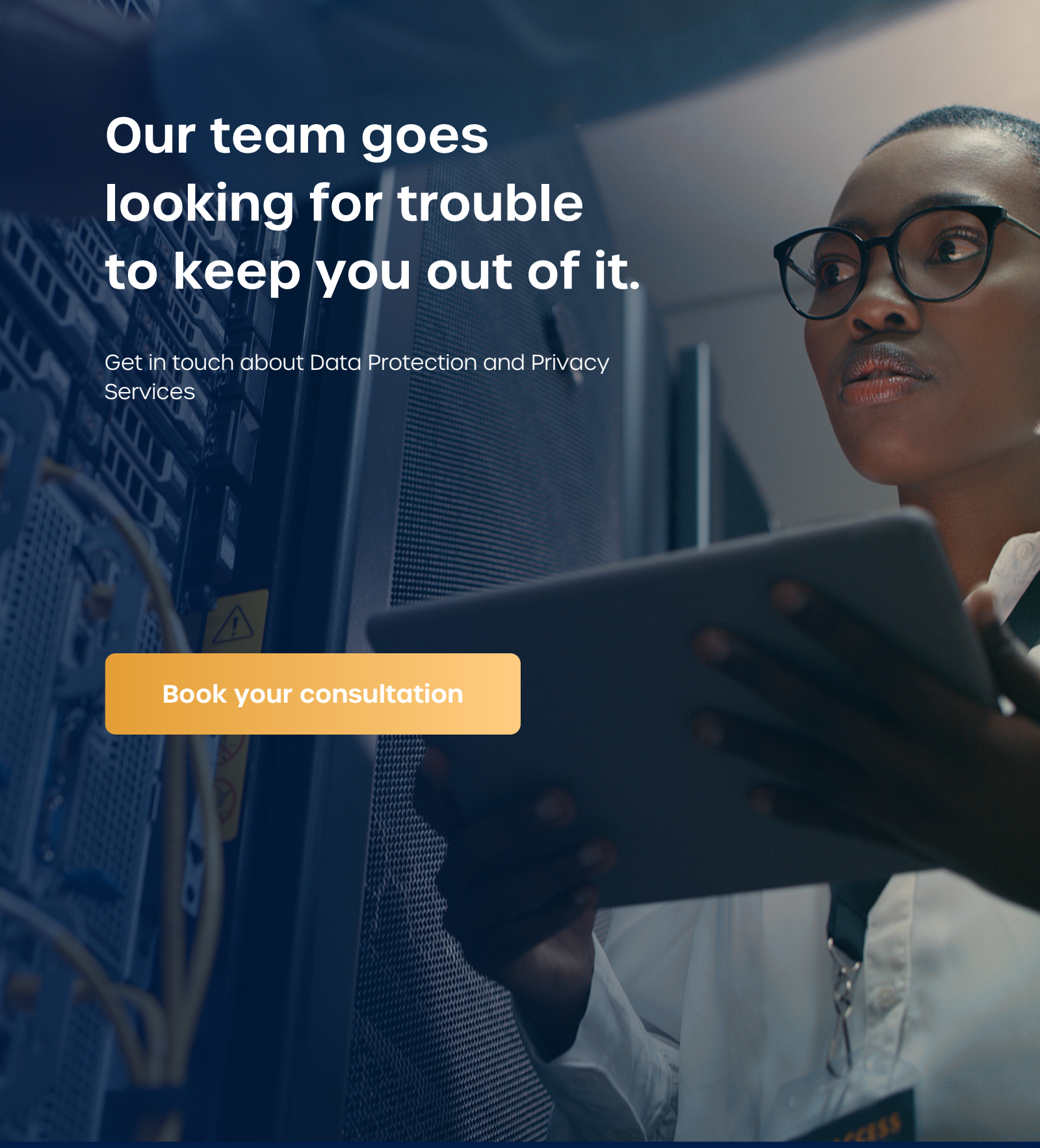
About Reliance Cyber

At Reliance Cyber, we believe in truly partnering with our customers. We work with organisations in many different sectors, to defend them against advanced cyber threats including up to nation-state-level. We develop a real, in-depth understanding of the risks an organisation faces and develop bespoke solutions. Our industry-leading cyber security expertise and experience enable organisations to focus on the things that they do best.



Get a free Data Privacy & Protection Consultation with one of our cyber consultancy team today

Book Your Free Consultation



Our team goes looking for trouble to keep you out of it.

Get in touch about Data Protection and Privacy Services

Book your consultation

RelianceCyber

www.reliancecyber.com

contact@reliancecyber.com

+44 (0) 20 3872 9000

1 Valentine Place |
London SE1 8QH | United Kingdom