2018 GDPR STUDY

MICKY KHANNA, FOUNDER, GDPRPLAN.COM
Summary of Report

GDPRPLAN.com, are proud to announce the UK's first ever in-depth study to report on the number of cases reported to the UK's Information Commissioner’s Office (ICO) since the EU GDPR came into effect back on May 25th 2018.

The objective of this report is to see whether all of the mass media coverage and publicity (both in leading up to and since enforcement) of the GDPR (as well as Data Protection in general) has had an impact as to whether the public are more aware of what companies are doing with their data, and whether there has been any change in the way the public feel about the way companies are using their data. We saw the first complaint within hours of the regulation coming into force and there hardly seems a week go by without the mention of a personal data breach or compromise from a high street brand or a household name, but what about complaints and cases that the ICO are working on? The aim of this study was to find out the facts.

The methodology used is quite straight forward. GDPRPLAN.com submitted a request to the ICO under the Freedom of Information Act 2000 and the request was to obtain the following information:

- No. of complaints received by the ICO between 25th May 2018 – 31st October 2018, by month, and to obtain the same set of stats across the same period for 2017.

- Proportion of complaints received by the ICO specifically relating to the GDPR/Data Protection between 25th May 2018 – 31st October 2018, by month, and the same set of stats across the same period for 2017.
Once this information had been obtained, we were also able to look at the data and add commentary as to our thoughts on the comparisons and variance and to make assumptions (which are entirely our own opinion and not those of any other party or organisation).

The results – whilst not totally unexpected – are surprising nonetheless.

For example, the headline figure is probably the 24,319 cases that the ICO are working on (based on figures between 25th May 2018-31st October 2018 only). Out of those 24,319 cases, 21,162 cases relate to reported breaches of Data Protection legislation that the ICO are working on. That equates to 87% of total cases that the ICO have received, which relate to Data Protection/GDPR and represents a 133% increase in such cases when compared to the same period in 2017 (where there were 9,099 Data Protection-related cases out of 11,420 cases in total for that timeframe).

Comparing this to the same timeframe across the previous year, the increase in the total number of Data Protection-related cases (the percentage of total cases specifically relating to Data Protection/GDPR was 79.8%) may seem nominal, however, when you convert this into actual numbers, that 8% difference equates to 12,069 increase in cases worked on since the GDPR came into effect between the 25th May and 31st October 2018. To put this into perspective, the total number of cases that fall under either FOIA/Environmental Information Regulations collectively is just 836 more than for the same timeframe for the previous year.

The highest month for “Number of Data Protection-related cases” since the GDPR came into effect was August, where 5,015 cases (out of 5,630 cases – which was also the highest month for total number of cases) were reported to the ICO, and to put that in perspective – that one month in 2018 equates to 55% of the total number of Data Protection-related cases between
25th May-31st October in the previous year. August 2018 alone account for almost **24% of total cases** *(Data Protection and Non-Data Protection related cases)* across the same timeframe in the previous year.

How does the highest month in 2018 compare to last year? Well in 2017 across the same timeframe, the highest month for Data Protection-related cases (again August) was just **1,843** (although the highest total number of cases across the same period was in fact October with **2,274**), so this year’s highest month represents a **172% increase**.

The results in this study should bring home the fact that company owners and CEO’s/MD’s need to know what their obligations are when it comes to Privacy, and how personal data affects each department within the organisation.

“The numbers in this study and percentage difference in complaints is truly astonishing! This proves that the media and the ICO are effectively communicating to the public about their privacy rights, and that they can turn to the ICO to report companies who do not treat personal information with the respect that it is due.”

*Anon*

“The results in this study not only show that the public are well and truly aware of what’s going on with their data, but also the fact that they’re taking action as they’re not happy! Companies should take heed of this information.”

*Anon*
About the Author

This study has been put together by GDPRPLAN.com, who provide training and consultancy solutions to help companies with their compliance obligations and information governance.

Micky Khanna, Founder of GDPRPLAN:

Micky began his digital marketing career in 2001 and has been part of many organisations operating within the AdTech/Martech services including Search Engine Optimisation and Pay Per Click, through to Affiliate, Email, Mobile, and Social Media Marketing, at both Network and Media Owner-side at companies such as Daily Mail General Trust, where he was part of the launch team for londonjobs.co.uk, before joining the UK’s first Pay-Per-Click network e-spotting media (later rebranded to MIVA). In 2007 he joined buy.at, a leading affiliate network which was acquired by AOL in 2008. In his last role (2010-2017), Micky steered the growth of performance marketing agency Optimus Performance Marketing, where, as Commercial Director he introduced over 120 brands and retailers across 14 international markets to the agency. It’s fair to say that there has been a lot of personal data that flows through each of the disciplines and organisations Micky had worked within. Combining his digital marketing experience with qualifications gained within Information Security & Data Protection, this led to the conception of GDPRPLAN.COM, to help businesses identify and assess the personal data they store, process or transfer in order to then plan and implement the right systems and measures in order to demonstrate the appropriate steps towards compliance.

We hope you enjoy the report, and feel free to provide feedback or contact us with any questions that you may have with regards to the report or indeed with your Data Protection & Privacy requirements at info@gdprplan.com.
Contents

Introduction ............................................................................................................................ 7
Methodology .......................................................................................................................... 12
Findings ................................................................................................................................. 13

Study 1: Yr on Yr Comparison of the Total Number of Cases (25/5-31/10) .................. 14
Study 2: Yr on Yr Comparison of Data Protection Related Cases with the ICO (2017-18) . 16
Study 3: Yr on Yr Comparison of Non-Data Protection (or “Other”) Related Cases/Complaints .................................................................................................................. 18
Study 4: Proportion of Total Complaints Relating to GDPR/Data Protection & “Other” to the ICO (Total & by Month, 2017/18) .................................................................................. 19

Study 4.1 Comparison of the Data (as a no.): 2017/18 .................................................. 20
Study 4.2 Comparison of the Data (as a percentage): 2017/18 .................................. 20

Conclusion .......................................................................................................................... 22

Appendix 1: Data Protection News Stories 25/5/18–30/11/18 ............................................ 25
Appendix 2: Data and Stats ............................................................................................... 26
Introduction

GDPRPLAN.com are proud to announce the UK’s first ever in-depth study to report on the number of complaints to the Information Commissioner’s Office since the EU GDPR came into effect back in May 25th 2018. We decided to put this report together as – quite frankly – nobody else had, although the International Association of Privacy Professionals did release a news article on the 25th June to show, by EU country, the number of complaints submitted to each Supervisory Authority, where they stated that the UK ICO had received 1,124 complaints (see https://iapp.org/news/a/cataloguing-gdpr-complaints-since-may-25/).

Given that GDPRPLAN.com provides consultancy and training for companies to help them understand their obligations and duties under GDPR, we wanted to see whether the general public are indeed as concerned as we’re led to believe. Are there really thousands of complaints being submitted to the ICO – or is it just a red herring and nobody really cares?

We wanted to find out if there was an increase of interest in the way the public feel that their personal data is handled, and whether the volume of complaints in comparison to the previous year suggest that companies are taking their Data Protection obligations seriously and demonstrating transparency, lawfulness, and fairness in the way they collect and process data. If they are, then we wouldn’t expect to see a significant increase in complaints/cases to the ICO as the public would be presented with a choice from those companies and have the option to opt-out before going to escalating the complaint to the supervisory authority.

We thought that by compiling this study it would give us (and readers) the facts.
Before we look at the stats, tables and charts, we wanted to reflect on some of the news stories that have captured the attention of the mainstream media since 25th May 2018 (we have included a list of events that have occurred since 25th May 2018-30th November 2018 in Appendix 1). Firstly, within a few hours of the GDPR coming into force, we saw the first complaint to Supervisory Authorities in France, Germany, and Austria relating to tech companies headquartered in Ireland and in the USA. There has hardly been a week pass by where there hasn’t been an announcement by a household brand name of a data compromise which has resulted in unauthorised access (potentially leading to a) loss of control of personal information relating to its customers. Whether you’re a large high street retailer, a multinational business, even an exam board, or a political party, the GDPR has had an effect and is now the number one subject matter on the agenda in the boardroom. It doesn’t even have to be the actions of a company directly that can lead to being found guilty either.

This study isn’t necessarily aimed at marketers – but Marketing are one of the highest risks where an organisation’s marketing strategy comprises digital marketing & direct response activity as they will need to demonstrate proof of consent or another form of legal basis (and the general consensus is that current consent frameworks do not comply with the regulation, and it’s difficult to claim “legitimate interest” when the interest weighs more in favour of the ad agency/trading desk/merchant than the user). We only have to take a look at the online behavioural advertising industry where – even as this report is being created – display advertising is traded on the profile of users’ and their browsing behaviour on a merchant’s website, with that data being traded via ad agencies and trading desks through numerous platforms (and then repackaged to multiple buyers) without even the knowledge (let alone consent) of the user – even though the GDPR came into effect over 6 months ago. Consent frameworks created by tech giants and organisations who are trying to keep the digital marketing industry self-regulated have proven to be ineffective, despite numerous warnings (including one from an industry expert, whose detailed explanation as to why these frameworks are ineffective was confirmed when the French supervisory authority “La Commission nationale de l’informatique et des libertés” (CNIL) also stated that the current
adopted consent framework is not adequate, within their response to a complaint about a Demand Side Platform (DSP) company, noting that the company was unable to demonstrate that the data collected through real time bid (RTB) requests are subject to informed, free, specific and unambiguous consent – read the full article here: https://brave.com/cnil-consent-rtb/).

We created a video to show how personal data flows around the digital ecosystem and highlights the challenges that face the intermediaries that sit between the brand/advertiser, and the publisher, which you can watch here: https://youtu.be/T56SP11X7po.

The way that the Human Resources department (who probably have access to the most detailed level of personal information out of all departments) operate to perform their function and their processes could also be a significant risk to an organisation. They don’t just hold information on current employees, but it is likely that they also hold personal information about prospective employees (CV’s in response to a job ad) as well as personal (and possibly sensitive) information about past employees too. CV’s for prospective employees are likely to be shared with the relevant departments across the organisation and transmission is usually via email or sent (wirelessly) to a Multi-Function Device for printing (and that MFD can probably store records of printing jobs) and sometimes even shared with individuals further up the ladder. What happens to that CV after the recruitment process has passed? Is it stored on file for future potential openings? If so then how does that affect the integrity of the data say – 6 months down the line and that candidate’s work history and experience has changed?

There’s also Customer Services, who are responsible for protecting client data and (particularly within B2B), there may also be a responsibility to handle transactional data
relating to their clients’ customers too. What happens to the data when the client parts company with the organisation?

Of course, if the company is collecting personal information from 3rd parties (recruitment agencies for example) or sending personal information to 3rd parties (recruiter-to-recruiter services for example) for other jobs, then it is vital to update contracts with vendors and suppliers to ensure that checks and balances are in place to protect the controller if the processor suffers a breach (and vice versa). It is also vital that users are informed of how their data is being used, and that there is a legal basis for carrying out the process.

The results in this study should bring home the fact that company owners and CEO’s/MD’s need to know what their obligations are when it comes to Data Protection & Privacy, and how personal data affects each department within the organisation - whether that’s HR, Sales, Customer Services, Legal, I.T, and (although mentioned last it is definitely not the least in terms of hierarchy) facilities management. Think about the data you collect, why you collect it, and whether you’re collecting more data than you actually need to perform the business function. Think about the way that data is stored within your organisation, and how you transmit information and data between departments – internally and externally to clients and business partners.

Where you utilise the services of an agency or outsource any business function, what controls are in place to protect data that you have given responsibility to your outsourced partner to manage? How secure is that information from bad actors who could (potentially) bring down the company and indeed the company CEO’s reputation.
Whilst a lot of speculation and fearmongering seems to have centred around the level of fines that the supervisory authorities have the power to impose, it should be noted that if a company is told to stop processing until it has resolved the problems (which led to the enforcement), that could have much more of an impact than a fine.

*For example, if you’re a social media network and have been instructed to stop processing (until you can demonstrate compliance), if it takes 6 months to fix the issues, that could have far more of an impact to your business than a €20m fine or 4% of your global annual turnover.*
Methodology

To obtain the stats required for this report, a request was made to the Information Commissioner’s Office, to obtain the number of cases/complaints that they have received since 25th May 2018, by month and to also obtain the same data across the same period in 2017.

The data was received but included cases in relation to other (Non-Data Protection) issues, such as the Freedom of Information Act 2000 and the Environmental Information Regulation 2004. So we went back and asked if the data could be categorised as follows:

- Data Protection related cases from 25th May 2018 to-date, by month
- Non-Data Protection related cases from 25th May 2018 to-date, by month
- Data Protection related cases across the same timeframe for 2017
- Non-Data Protection related cases across the same timeframe for 2017

The ICO kindly provided the stats, and they also informed us that “many of these complaints and breach reports will relate to potential breaches of Data Protection Act 1998 (DPA 1998) rather than the General Data Protection Regulation/Data Protection Act 2018.”

We have included the transcript in Appendix 2. Over the following pages you will see that we have taken the data and have separated them out into the following sets of data:
Study 1: Year on Year comparison of the total number of Cases: 25th May-31st Oct

Study 2: Year on Year Comparison of the Data Protection Related Cases

Study 3: Year on Year Comparison of Non-Data Protection Related Cases to the ICO

Study 4: Proportion of total cases relating to GDPR/Data Protection & “Other”

   Study 4.1: Comparison of the data (as a no.) 2017-2018

   Study 4.2: Comparison of the data (as a percentage) 2017-2018

Whilst the stats provided in this report are based on what we have received from the ICO, the commentary and interpretation of the data as well as the compiling of this report are purely the views and opinions of GDPRPLAN.com and not those of any supervisory authority or government organisation. We sent draft versions of the report to various industry experts and some have provided commentary which we have included in this study. They have chosen to remain anonymous and we thank them for their feedback.
Findings

Study 1: Year on Year Comparison of the Total Number of Cases (25/5-31/10)

This chart shows the total number of new cases (Data Protection related and Non-Data Protection related), by month, between the 25th May and 31st October 2018 and we have compared the numbers with across the same period in 2017. What stands out is the number of cases/complaints that the ICO have received in 2018, which at 24,319 is 12,899 more than for the same period in 2017 where there were 11,420 cases in total. This represents a 113% increase Y/Y for this timeframe:

As the stats for May only cover a 7-day period (25th-31st) if we just focus on the full months (June-October), that means that as an average there were 2,200 cases per month in 2017 which has now increased to 4,720 cases per month for the same timeframe in 2018 and that pushes the percentage a little higher to a 114% increase. In terms of percentages, the average monthly growth in new cases for 2017 was just 2%, and in 2018 this has increased significantly to 10% - an increase of 2,521 new cases per month compared to 2017 which was just 2%.
It is probably not too much of a surprise that there has been a considerable increase in the number of total cases, but remember – these figures show the collective number (so they also include cases relating to Freedom of Information Act 2000 and Environmental Information Regulations 2014, as well as Data Protection related cases).

So, in order to ascertain whether the increase in numbers are to be attributed to the GDPR, we need to categorise the numbers into those which are related to Data Protection, and those which are not, which leads us to the next study: “Year on Year Comparison of Data Protection-Related Complaints to the ICO (2017-2018)”.
Study 2: Year on Year Comparison of Data Protection Related Cases with the ICO (2017-2018)

This chart shows the total number of Data Protection related cases by month, between the 25th May and 31st October 2018 and we have compared the numbers with across the same period in 2017. What stands out is the significant increase in Data Protection related cases/complaints which has increased by 12,063 cases to 21,162 cases, compared to 9,099 cases across the same period in 2017, which represents a 126% increase – outgrowing the collective (all cases) figure by 13% Y/Y:

<table>
<thead>
<tr>
<th>Month</th>
<th>2017</th>
<th>Diff M/M</th>
<th>2018</th>
<th>Diff M/M</th>
<th>Diff Y/Y (No.)</th>
<th>Diff Y/Y (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>May</td>
<td>321</td>
<td></td>
<td>620</td>
<td></td>
<td>299</td>
<td>93%</td>
</tr>
<tr>
<td>June</td>
<td>1629</td>
<td>3%</td>
<td>3091</td>
<td>36%</td>
<td>1462</td>
<td>90%</td>
</tr>
<tr>
<td>July</td>
<td>1742</td>
<td>6%</td>
<td>4218</td>
<td>36%</td>
<td>2466</td>
<td>142%</td>
</tr>
<tr>
<td>Aug</td>
<td>1843</td>
<td>6%</td>
<td>4015</td>
<td>19%</td>
<td>3172</td>
<td>172%</td>
</tr>
<tr>
<td>Sept</td>
<td>1740</td>
<td>6%</td>
<td>3960</td>
<td>21%</td>
<td>2220</td>
<td>128%</td>
</tr>
<tr>
<td>Oct</td>
<td>1824</td>
<td>5%</td>
<td>4268</td>
<td>8%</td>
<td>2444</td>
<td>134%</td>
</tr>
<tr>
<td>Total</td>
<td>5099</td>
<td>3%</td>
<td>21162</td>
<td>11%</td>
<td>12063</td>
<td>286%</td>
</tr>
<tr>
<td>Average per mth (exc May)</td>
<td>1756</td>
<td>3%</td>
<td>4108</td>
<td>11%</td>
<td>2353</td>
<td>233%</td>
</tr>
</tbody>
</table>

However, as the stats for May only cover a 7-day period (25th-31st) if we just focus on the full months (June-October), that means that (as an average) out of the 2,200 collective cases per month, 1,756 cases per month in 2017 specifically relate to Data Protection. In 2018, the number of Data Protection related cases increased by (on average) 2,353 new cases per month than in 2017 since the GDPR came into effect, or 133% increase (which is higher than the figure if we include the 7-days data from May).
The month which saw the most Data Protection-related cases again was August for both 2017 and 2018, with 1,843 and 5,063 cases respectively. Whereas the percentage difference between the highest month of collective cases in 2017 (October: 2,274) and 2018 (August: 5,630) was a 148% increase (as shown in the graph in Study 1), the difference between those specifically relating to Data Protection cases was even an even greater increase at 172% increase.

The average growth in new cases by month is 11% for 2018, compared to just 3% for the same period in 2017 (so outperforming the collective number of cases shown in the previous chart).

“These are truly astonishing figures and shows quite clearly that the public are concerned about the way that their personal information is handled”.

Anon

“Whilst the figures show the obvious increase in complaints to the ICO, they also suggest that the ICO are effectively communicating to the public about their right to be informed as to what companies are doing with their data.”

Anon
Study 3: Year on Year Comparison of Non-Data Protection (or “Other”) Related Cases/Complaints

This chart shows the total number of Non-Data Protection related cases by month, between the 25th May and 31st October 2018 and we have compared the numbers across the same period in 2017. Whilst we saw a significant increase in Data-Protection related cases in the previous chart, we also see quite an increase in those other cases too, which we will cover in the next chart.

Taking the full months (June-October) into account only, the average volume of Non-Data Protection-related cases that the ICO are working on in 2018 is 612 per month, up from 444 per month in 2017.

“This increase can probably be attributed to the fact that the ICO have effectively communicated their authority as an organisation and also as a body who the public can turn to for more than just Data Protection related issues”

Anon
Study 4: Proportion of Total Complaints Relating to GDPR/Data Protection & “Other” to the ICO (Total & By Month, 2017/2018)

In the previous charts (Studies 1-3) we broke down the number of Cases/Complaints submitted to the ICO by Data Protection-related, and those categorised under “Other” (which we understand to be either related to Freedom Of Information Act 2000 or Environmental Information Regulation 2004). This study looks at the proportion of Cases/Complaints over 2017 & 2018 across the date ranges of 25th May-31st October, and if we start with the headline numbers that reflect the percentage increase in Data Protection-related cases that the ICO are working on:

The headline figure we can take from the above is the growth from 79% of total cases Data Protection-related cases in 2017 to 87% in 2018. Even though the percentage of Non-Data Protection related cases as a proportion of total cases has decreased from 21% in 2017 to
13% in 2018, the volumes have increased significantly from 2,321 (2017) to 3,157 (2018), which equates to a 36% increase.

With regards to those actual Data Protection-related cases, in 2017 there were 9,099 cases reported to the ICO, whereas across the same timeframe in 2018 this figure increased to 21,162 cases, which (as reported in Study 2) equates to a 133% increase. If we overlap the two sets of data to illustrate the differences better (2018 columns are faded):

Study 4.1 Comparison of the Data (as a no.): 2017/2018

![Comparison of the Data (as a no.): 2017/2018](chart1.png)

Study 4.2 Comparison of the Data (as a percentage): 2017/2018

![Comparison of the Data (as a percentage): 2017/2018](chart2.png)
On a side note the highest month (for this timeframe) for total cases in 2017 is October with 2,271 cases, and for 2018 the highest month was August with 5,630, but the increase is significant, as August 2018 saw 3,359 more cases than October 2017, an increase of 148%.

If we exclude May (as that data range is only between 25th-31st) and focus on the full monthly averages, that’s 4,108 cases per month in 2018 with the ICO (compared to 1,756 in 2017), which represents a 134% average monthly increase. Non-specific cases works out per full month, an average of 612 cases in 2018 (compared to 444 cases per month in 2017) which works out at 38% increase per full month. That’s an 89%:11% (9/10) cases that relate to Data Protection.

“Working on an average of 4,100 Data Protection/GDPR cases per month shows quite clearly that the public have become increasingly aware of their rights when it comes to their data, and are genuinely concerned as to what companies are doing with their data.”

Anon

“It looks like the ICO have not only effectively communicated awareness of Data Protection rights, but it seems that the public are also more aware of the ICO as an organisation”

Anon
Conclusion

So what can we take away from the findings and the stats? We believe that our questions were answered quite clearly, in that the “hype” and mass media awareness created by the arrival of the biggest change to Data Protection in 20 years has led to the public being far more informed of the way in which their personal information is being used, and the stats also suggest that they are not happy with the way in which companies use their information.

The fact that has been a **133%** increase in cases reported to the ICO that relate to Data Protection, and that **9 out of 10** cases reported to the ICO relate to Data Protection shows quite clearly that the public are more aware of their rights when it comes to how their personal information is used, and that they are now far more likely to take action and report companies if they’re not happy with the way that companies are using their information.

One may also draw from this research that – now that we’re over 6 months in – companies still have a lot of work to do in terms of implementing appropriate measures so as to demonstrate compliance with the new regulations.

If you’re the CEO or owner of a company that processes personal information then it is vital that you start taking your obligations seriously and rather than assume that it won’t affect you. Start the process by carrying out an audit of the personal information that you collect and process so that you can take the necessary steps to protect that information and be confident that you have a solid legal basis for doing so.

Of course, no plan is 100% fool-proof and as the biggest threat to any organisation is usually from within (as we’ve also seen in the news with the report about the ICO flexing its
supervisory powers to impose the first custodial sentence under the Computer Misuse Act 1990\textsuperscript{13}), so it is vital that training and awareness is carried out so as to demonstrate that organisational and technical measures are being taken to work towards compliance. Those who do not have Privacy or Data Protection at the top of their list probably do not collect or process personal information, but if they do, (collect or process personal data), then it is highly that those companies will be at risk of receiving enforcements or sanctions by a supervisory authority as a result of suffering from a breach due to negligence or poor Data Protection policies.

As there is an increase in “other” related cases that the ICO are working on, this suggests that the ICO have indeed increased awareness of their organisation, and (probably) increased awareness to the public of their investigatory powers.

**The future?**

For the next report one might add further analysis (perhaps over a 12-month period from May 25\textsuperscript{th} 2018) and link data breach/hack-related news stories to the data to see if there’s any correlation. One might also look to seek out whether the cases are regarding public or private sector organisations, or by Industry Sector (Retail, Finance, Travel etc). Another useful metric might be to look at the number of cases that relate to companies headquartered in a specific country. If we are able to categorise cases/complaints into those with under/over 250 employees this might give useful insight as to the complaints and cases by size of company. Looking at the reason for the complaint could be another useful metric to see what category the most common cases fall into.
It would probably give even greater insight if the cases could be categorised into those which are being investigated under DPA ’98, GDPR/DPA 2018 and PECR, but we also have to understand the limitations of what data can be obtained under the FOIA.

When we received the data from the ICO, they also informed us that they are “unable to determine which specific legislation each case relates to because the case management system was not built with changes of legislation in mind, and the only way to achieve certainty regarding the number of Data Protection cases which are being investigated under DPA 1998 or the current framework would be to conduct a manual trawl through each of the 21,162 case files, which would likely be in breach of FOIA section 12.”

Of course by the time we get to an annual review post GDPR enforcement date, the UK may well have crashed out of the European Union (and without a deal). The implications of Brexit are still unknown with regards to Data Protection and what arrangement will be in place.

We hope that you found this report to be useful and if you have any questions, feedback or would like to discuss collaboration opportunities for future reports, please email info@gdprplan.com.
Appendix 1: Data Protection News Stories 25/5/18–30/11/18


4. 29th August 2018: “Exam result details now obtainable for free under GDPR” https://www.bbc.co.uk/news/technology-45343286


8. 10th August 2018: “Butlin’s says guest records may have been hacked” https://www.bbc.co.uk/news/technology-45141880


11. 29th September 2018: “Facebook security breach: Up to 50m accounts attacked” https://www.bbc.co.uk/news/technology-45686890


15. 16th November 2018: “Microsoft menaced with GDPR mega-fines in Europe for ‘large scale and covert’ gathering of people’s info via Office” https://www.theregister.co.uk/2018/11/16/microsoft_gdpr/


Appendix 2: Data and Stats

Email From the ICO:

“The numbers provided relate to the number of complaints received under the Freedom of Information Act 2000, the Environmental Information Regulations 2004 and requests for assessment under the Data Protection Act 2018.

<table>
<thead>
<tr>
<th></th>
<th>May</th>
<th>June</th>
<th>July</th>
<th>August</th>
<th>September</th>
<th>October</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017</td>
<td>421</td>
<td>2085</td>
<td>2215</td>
<td>2248</td>
<td>2177</td>
<td>2274</td>
</tr>
<tr>
<td>2018</td>
<td>717</td>
<td>3670</td>
<td>4821</td>
<td>5630</td>
<td>4458</td>
<td>5023</td>
</tr>
</tbody>
</table>

You have asked:

“...how many of those complaints were specifically related to the data protection act/GDPR? Would you be able to provide this for me in the same format as you’ve provided the data in the last email (by month and previous year - same period) please?”

Below I have provided a table of the total number of Data Protection complaints received by the ICO from 25 May 2017 to 1 November 2017 by month, compared with the total number of complaints brought to the ICO by individuals.

<table>
<thead>
<tr>
<th></th>
<th>May</th>
<th>June</th>
<th>July</th>
<th>August</th>
<th>September</th>
<th>October</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017</td>
<td>321</td>
<td>1629</td>
<td>1742</td>
<td>1843</td>
<td>1740</td>
<td>1824</td>
</tr>
<tr>
<td>2018</td>
<td>620</td>
<td>3091</td>
<td>4208</td>
<td>5015</td>
<td>3960</td>
<td>4268</td>
</tr>
</tbody>
</table>

As the table above indicates, between 25 May 2018 and 1 November 2018, the Information Commissioner’s Office has set up 21,162 pieces of casework relating to reported breaches of data protection legislation.

It should be noted that many of these complaints and breach reports will relate to potential breaches of Data Protection Act 1998 (DPA 1998) rather than General Data Protection Regulation/Data Protection Act 2018. However, we are unable to determine which specific legislation each case relates to. This is because our case-management system was not built with changes of legislation in mind.

The only way to achieve certainty regarding the number of data protection cases which were being investigated under DPA 1998 or the current framework would be to conduct a manual trawl through each of the 21,162 case files. This would likely be in breach of FOIA section 12, so I have interpreted your request for the number of data protection cases rather than for a split between the number we are investigating under GDPR and the number under DPA 98.”