ICO penalties in UK

Pridatect
POWERING PRIVACY COMPLIANCE

CONTENT

1. Introduction 3

2. Regulatory framework 4

2.1. Article 55 of Data Protection Act 5

2.2. Principles of Data Protection Act 6

2.3. Privacy and Electronic Communications Regulations 7

3. Charts 8

4. Differences between DPA 1998 and DPA 2018 11

5. Cases 12

6. Conclusion 15

1. INTRODUCTION

In this ebook we analyze the 61 resolutions that the Information Commissioner's Office (ICO) made in the last two years which the requested party has been sentenced to pay pecuniary sanctions.

From the cases studied we can highlight that most entities have been sanctioned for carrying out marketing actions without the consent of the user.

The ICO has used, fundamentally, these English legal provisions: the Data Protection Act and the Privacy and Electronic Communications Regulations.

2. REGULATORY FRAMEWORK

The Data Protection Act 1998 (DPA) regulated the use and protection of personal data, delineating the responsibility of companies in the handling of these data and replacing the old Data Protection Act 1984. The DPA transposed Directive 95/46/EC and although both are now repealed, the events concerned in the 61 cases studied took place while they were still in force.

Its successor was the Data Protection Act 2018, which entered into force on 25 May 2018, making it the third generation of data protection legislation in the United Kingdom's regulatory framework. The new DPA aims to modernise the provisions in this area, ensuring their effectiveness for the coming years, and accompanies the already known General Data Protection Regulation (GDPR).

Fundamentally, the resolutions that have ended with pecuniary sanctions have been based on the principles of Schedule 1 and section 55 of the DPA 1998 and the Privacy and Electronic Communications Regulations 2003 (PECR). On the basis of this regulation, only those serious infringements will be fined and the amounts to be paid will depend very much on the circumstances of each case: the sector of the company, its size, the economic resources it has...

The Commissioner will take an objective approach in considering whether there has been a serious breach of the Act and, while a single breach may be sufficient to reach this threshold, it is more likely to occur where there are multiple breaches to seriously contravene the Act.

The application of pecuniary sanctions has an extensive addressee type. They include large and small companies, individual traders, charities and data controllers in both the public and private sectors, among others.

According to the Data Protection Regulations 2010 the maximum fine must not exceed £500,000. In addition, it should be noted that in the event that the Commissioner receives full payment of the fine within 28 days of notification, the amount will be reduced by 20%.

2.1 Article 55A DPA

Article 55A DPA gives the Commissioner the power to impose pecuniary sanctions. It provides that:

"1) The Commissioner may serve a data controller with a monetary penalty notice if the Commissioner is satisfied that:
(a) there has been a serious contravention of section 4(4) by the data controller,
(b) the contravention was of a kind likely to cause substantial damage or substantial distress, and
(c) subsection (2) or (3) applies.
(2) This subsection applies if the contravention was deliberate.
(3) This subsection applies if the data controller:
(a) knew or ought to have known
i) that there was a risk that the contravention would occur, and
(ii) that such a contravention would be of a kind likely to cause substantial damage or substantial distress, but
(b) failed to take reasonable steps to prevent the contravention".

2.2 Principles

Schedule 1 DPA 1998[1] contains the eight principles of data protection. The principles of the old DPA are very similar to the GDPR, therefore the fines imposed in the cases we will analyse below would also be an infringement applying the GDPR.

1 "Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
at least one of the conditions in Schedule 2 is met, and
in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data".

2.3. Privacy and Electronic Communications Regulations

In more than 50% of the cases studied, articles 21 and 22 of the PECR have been contravened, an implementation of Directive 2002/58/EC in the United Kingdom.

This regulation was created with the aim of protecting the fundamental right of individuals to privacy in the electronic communications sector.

Article 21 PECR refers to unsolicited telephone calls for direct marketing purposes. It states that:

"A person shall neither use, nor instigate the use of, a public electronic communications service for the purposes of making unsolicited calls for direct marketing purposes where:
the called line is that of a subscriber who has previously notified the caller that such calls should not for the time being be made on that line; or
(b) the number allocated to a subscriber in respect of the called line is one listed in the register kept under regulation 26".

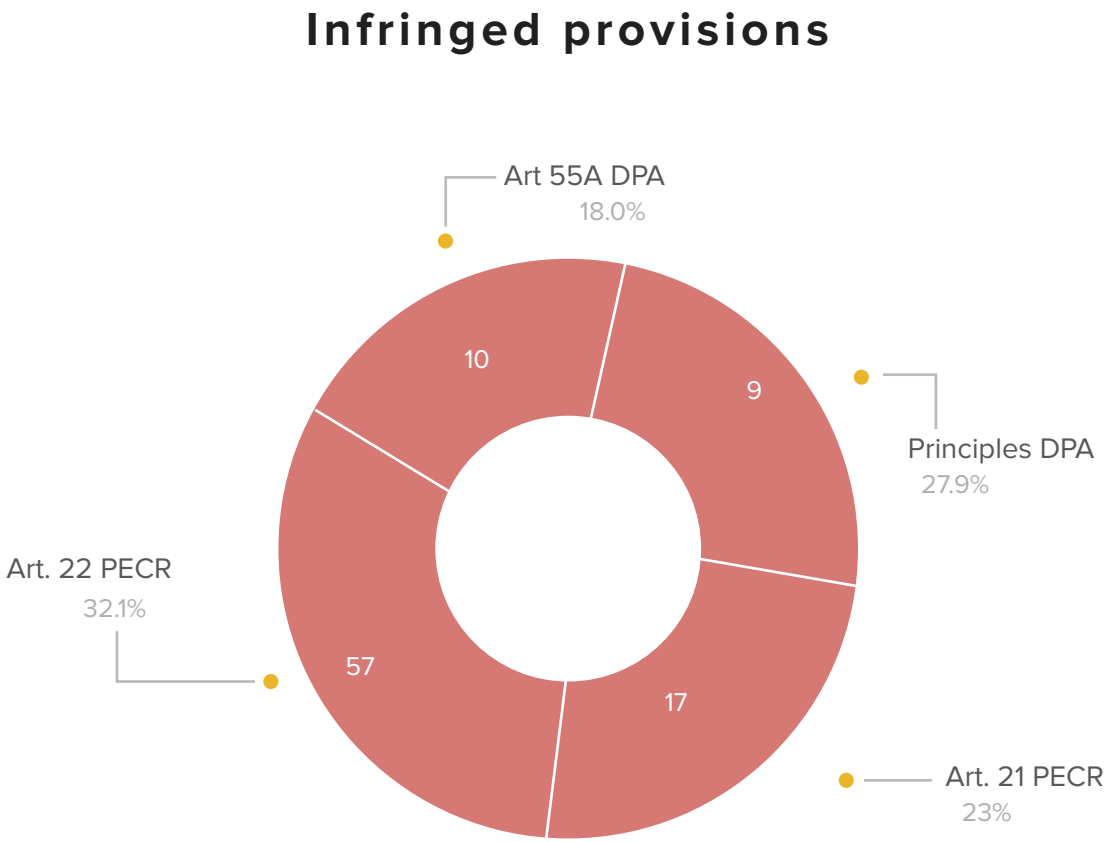
On the other hand, article 22 PECR refers to the use of electronic mail for marketing purposes. We read,

"Except in the circumstances referred to in paragraph (3), a person shall neither transmit, nor instigate the transmission of, unsolicited communications for the purposes of direct marketing by means of electronic mail unless the recipient of the electronic mail has previously notified the sender that he consents for the time being to such communications being sent by, or at the instigation of, the sender".

3. CHARTS

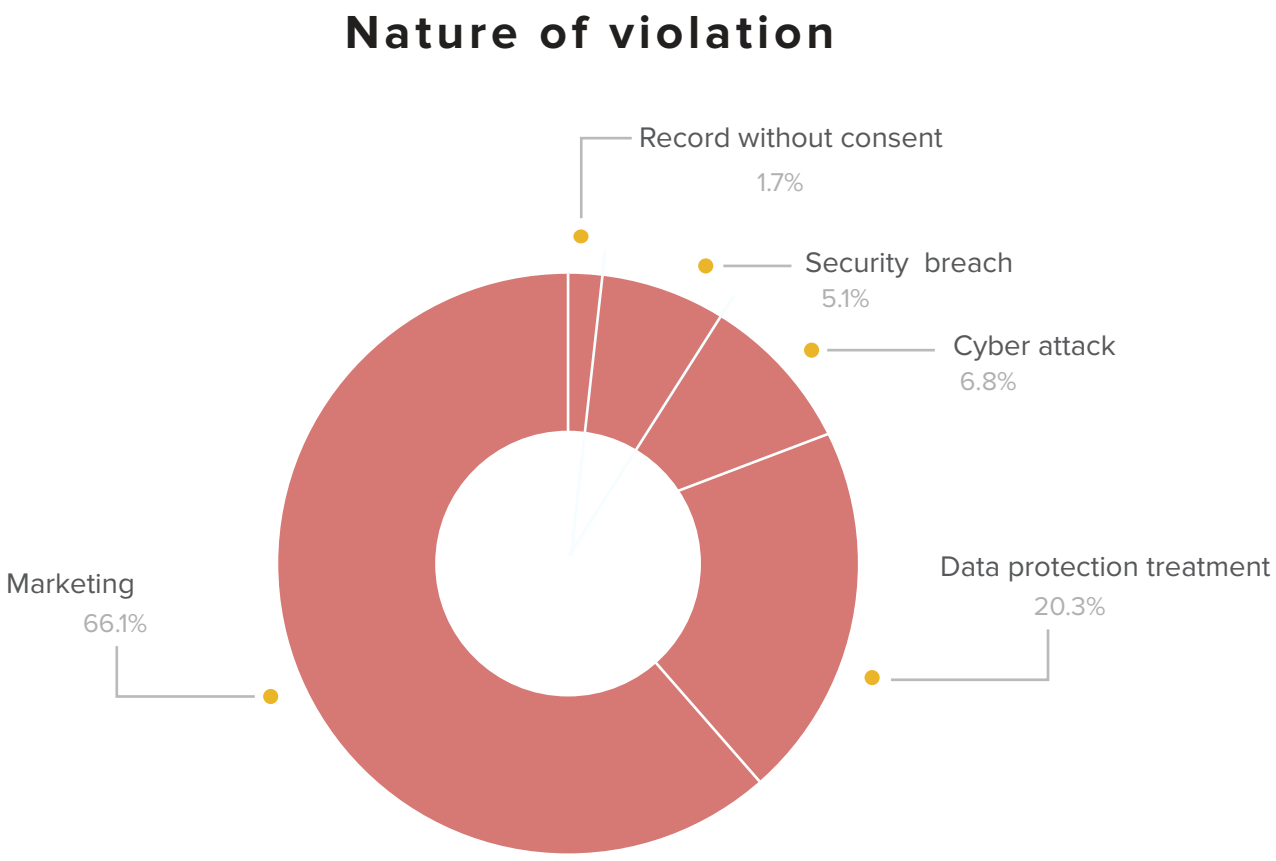
Until today, the ICO has published 61 resolutions urging the requested party to pay a fine. Seventeen of the cases have been for contravening the principles of the DPA, 14 cases for contravening the article 21 PECR and 19 for contravening Article 22 PECR. In the remaining 11, the ICO relied solely and fundamentally on Article 55A of the DPA, which is common to all of them.

Graphic 1. Infringed provisions



More than half of the infringements were carried out by performed marketing actions without the user's consent, either by email or telephone calls. The other half is concentrated primarily in cases where adequate technical and organizational measures were not taken against unauthorized or unlawful processing of personal data, cyber attacks and security breaches.

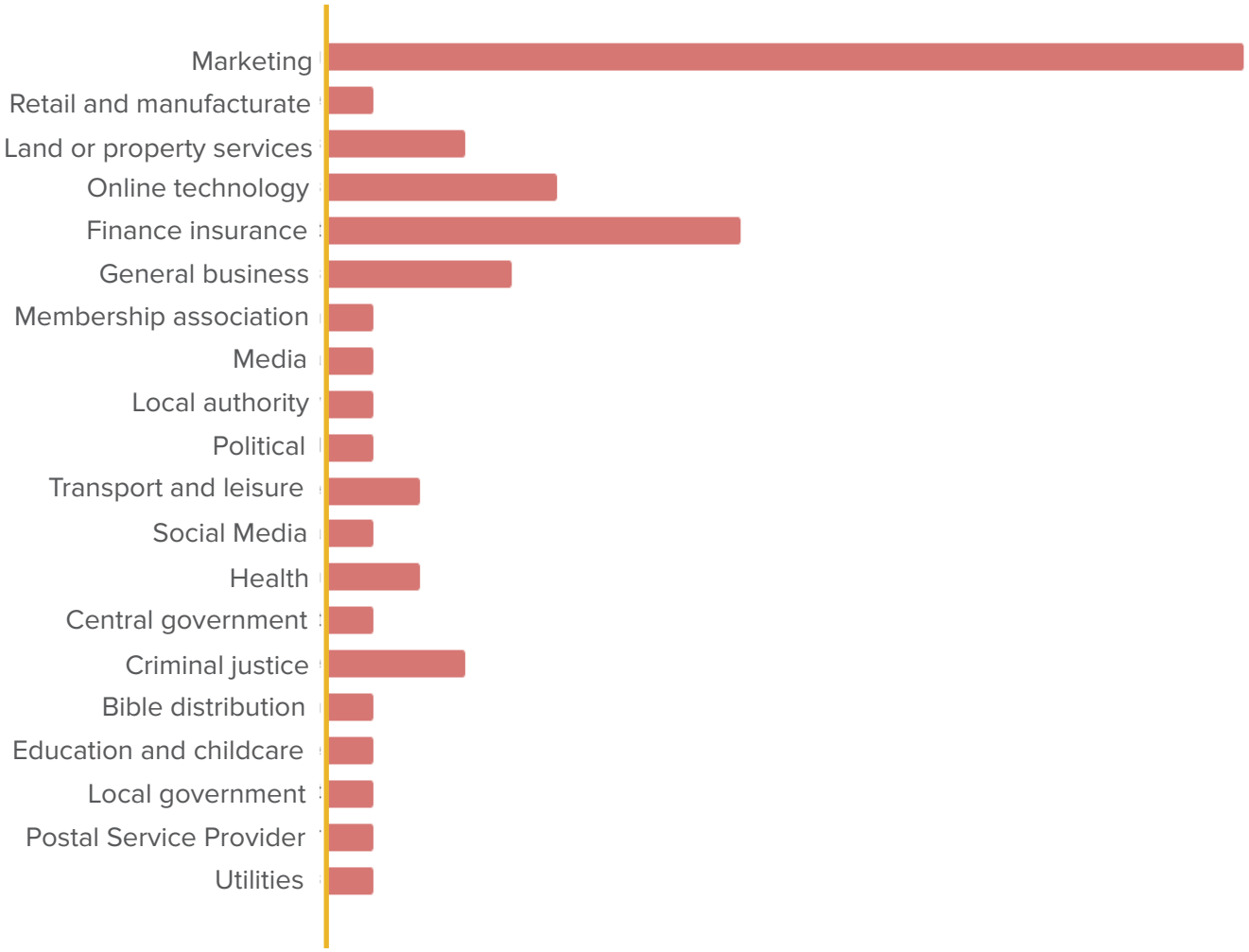
Graphic 2 . Nature of violation



Although the sectors of activity of the fined entities are most varied, the predominant one is the marketing sector.

This is followed by entities specialised in insurance and credit, followed by public entities.

Graphic 3. Sector



4. DIFFERENCES BETWEEN DPA 1998 AND 2018

Since 25th May 2018 the data protection framework in the United Kingdom is made up of the Data Protection Act 2018 and the General Data Protection Regulations of the European Union (GDPR). The Data Protection Act 2018 is an Act of the UK Parliament updating the old Data Protection Act 1998.

The DPA 2018 adapts how the GDPR is applied in the UK, for example by granting exemptions. It also regulates data protection rules for law enforcement authorities, extends data protection to other areas, such as national security and defence, and sets out the functions and powers of the ICO.

One of the most substantial changes between the two laws is that while under the 1998 DPA the maximum fine was £500,000, the update states that it will have a maximum of £17 million or up to 4% of the entity's total turnover.

According to expert Steve Sands this change is good because it means that data protection will be elevated to the list of companies' priorities.

With the new law, there is a change from eight to six principles and these focus on any data being used in a legal, fair and transparent manner, and being for specific, explicit and legitimate purposes. In addition, it also focuses on data being adequate, relevant and limited to what is necessary in relation to the purpose of access to the data. Another important issue is the length of data retention, which does not have to be longer than necessary.

Finally, another important novelty is that a data protection officer is required in those larger companies (those with more than 250 employees or processing data from more than 5,000 people).

5. CASES

5.1 Facekook Ireland Limited[1]

For now, the company that has paid the largest amount together with Equifax Limited has been Facebook Ireland, which was fined on 24th October 2018 for paying a total of £500,000. The imposition of this fine arises from a very serious breach of data protection of users of the platform that took place before 25 May 2018, so the DPA 1998 applies. In this case, principles 1 and 7 of Schedule 1 were considered to have been breached.

The ICO investigation revealed that between 2007 and 2014 Facebook unfairly processed personal information of its users. It failed to perform adequate checks, thus allowing an App called This is your real life, created by Aleksandr Kogan of Global Science Research Limited (SCL), to collect Facebook data from millions of users worldwide without their knowledge, as it was used in conjunction with the platform.
Even users who had not downloaded the application but were “friends” of people who had downloaded it were allowed access. Subsequently, a subset of this data was shared with other organizations, including SCL Group, the parent company of Cambridge Analytica that participated in political campaigns in the United States.

While the application was downloaded 270,000 times, it is understood that data of at least 87 million was obtained because This is your real life was able to take advantage of Facebook’s privacy weaknesses.

1 https://pdf.browsealoud.com/PDFViewer/_Desktop/viewer.aspx?file=https://pdf.browsealoud.com/StreamingProxy.ashx?url=https://ico.org.uk/media/action-weve-taken/mpns/2260051/r-facebook-mpn-20181024.pdf&opts=ico.org.uk#langidsrc=0&locale=en

5.2 Equifax Limited[1]

On 19th October 2018 the ICO set the maximum penalty of £500,000 to Equifax Limited in the insurance and financial credit sector for failing to protect the personal data of up to 15 million British citizens during a cyber attack in 2017.

Of the 8 principles set out in the DPA, the ICO considered Equifax to have breached the 1st, 2nd, 5th, 7th and 8th principles. In reaching this conclusion, it considered the purpose for which the personal data was processed and the transfer of data from the United Kingdom to the United States.

Between 13th May and 30th July 2017, data held by Equifax's parent company in the United States, Equifax Inc, was subject to cyberattack. The compromised data included personal data contained in up to 15 million unique UK personal records. While the cyber attack was perpetrated in the US systems, the ICO ruled that, with regard to UK data, Equifax Limited "had not taken adequate technical and organisational measures against unauthorised and unlawful processing" (Principles 5 and 7).

There was also a breach of Principle 1 with regard to the way in which the data were processed, of Principle 2 with regard to the purpose of the processing and of Principle 8 with regard to transfers of data from the United Kingdom to the United States.

1 https://pdf.browsealoud.com/PDFViewer/_Desktop/viewer.aspx?file=https://pdf.browsealoud.com/StreamingProxy.ashx?url=https://ico.org.uk/media/action-weve-taken/mpns/2259808/equifax-ltd-mpn-20180919.pdf&opts=ico.org.uk#langidsrc=0&locale=en

5.3 The Energy Saving Centre[1] Limited

ICO fined on 16th April 2018 £250,000 to Energy Saving Centre Limited (ESC) for contravention of section 21 of the Privacy and Electronic Communications Regulations 2003 (PECR).

ESC received this sanction as it was deemed to have made previously unsolicited calls for the purpose of marketing to subscribers who had registered with the Telephone Preference Service.

Article 21 provides that if a company wishes to promote its products or services by calling the telephone number of the Telephone Preference Service, the individual in question must have given his or her consent for that purpose.

In this case, ESC, a company offering home improvement services, made a total of 7,191,958 calls for commercial purposes in 7 months, leaving 1,138 complaints from users.

In addition, the ICO has taken into account the following aggravating factors:

- Lack of participation in the investigation.
- ESC had no consideration for the provisions of the PECR.
- ESC has continued to carry out commercial calls having been alerted by the ICO.

The ICO, in its resolution, ends by pointing out that the fact of imposing the pecuniary sanction aims to promote compliance with the PECR as this type of behaviour is “a matter of great public interest”.

1 https://pdf.browsealoud.com/PDFViewer/_Desktop/viewer.aspx?file=https://pdf.browsealoud.com/StreamingProxy.ashx?url=https://ico.org.uk/media/action-weve-taken/mpns/2258727/energy-saving-centre-ltd-mpn-20180416.pdf&opts=ico.org.uk#langidsrc=0&locale=en

6. CONCLUSION

With this work we have been able to verify that not only the big companies are fined in terms of data protection, but also SMEs have been fined, which leaves no doubt that the application of the GDPR, together with the DPA 2018, is a reality from which companies, whatever their size or sector, cannot and should not escape.

Although the resolutions analysed are of the utmost topicality, these infringements had still been committed under the repealed law. Without prejudice to this, the sanctions studied would also have resulted in infringements with the GDPR, since the general principles of data protection are practically identical.

In spite of this, everything seems to indicate that this precedent of the ICO is much more benevolent than the one to come, since the innovations introduced by the GDPR are more demanding and harsh than the previous one.

Changes in laws in recent years have increased the burden on data controllers and data processors. Experts wonder how prepared and able most companies are to cope with all these changes, so we encourage all companies to consider how all these changes affect them and plan accordingly.

“la aplicación del Reglamento General de Protección de Datos es una realidad a la que las empresas ya no pueden dar la espalda”

SIMPLIFYING DATA PROTECTION FOR PROFESSIONALS

More information at
pridatect.com

Contact
info@pridatect.com