Contact Centre Council

Compliance & Regulation Hub Update

December 2018

This month's headlines:

- *Individual company directors, as well as the corporate entities, will now be liable for PECR fines of up to £500,000*
- *The Incredible shrinking TPS: 12% smaller already this year & counting*
- *PCI DSS Guidelines for Phone Payments have been released – and it's bad news for contact centres relying on 'pause & resume' techniques to take themselves 'out of scope'*
- *Only 5 days left to share your views on a new Code of Practice for Direct Marketing with the ICO*
- *The ICO has fined two companies a total of £250,000 for making unsolicited marketing calls to numbers on the TPS – and fined a third firm £200,000 for sending over 14 million texts in breach of the PECR rules*
- *The Fundraising Regulator is to start 'naming and shaming' charities under investigation from 2019*
- *118 providers' prices have been capped by Ofcom*

And hidden away in the Update, a small Christmas Competition!

Directors' Fines

On 17th December the government finally announced that directors would now be liable for fines imposed on their company by the ICO. The DMA's John Mitchison commented ""The DMA warmly welcomes these new changes to PECR. The credibility of responsible telemarketers has forever been tarnished by rogue companies breaking the law and making nuisance calls."

www.dma.org.uk/article/today-telemarketer-director-liability-law-comes-into-force

Image taken from the DMA's news article. It's not clear whether it represents a frustrated consumer or a rogue director who's just heard he's been fined £500,000

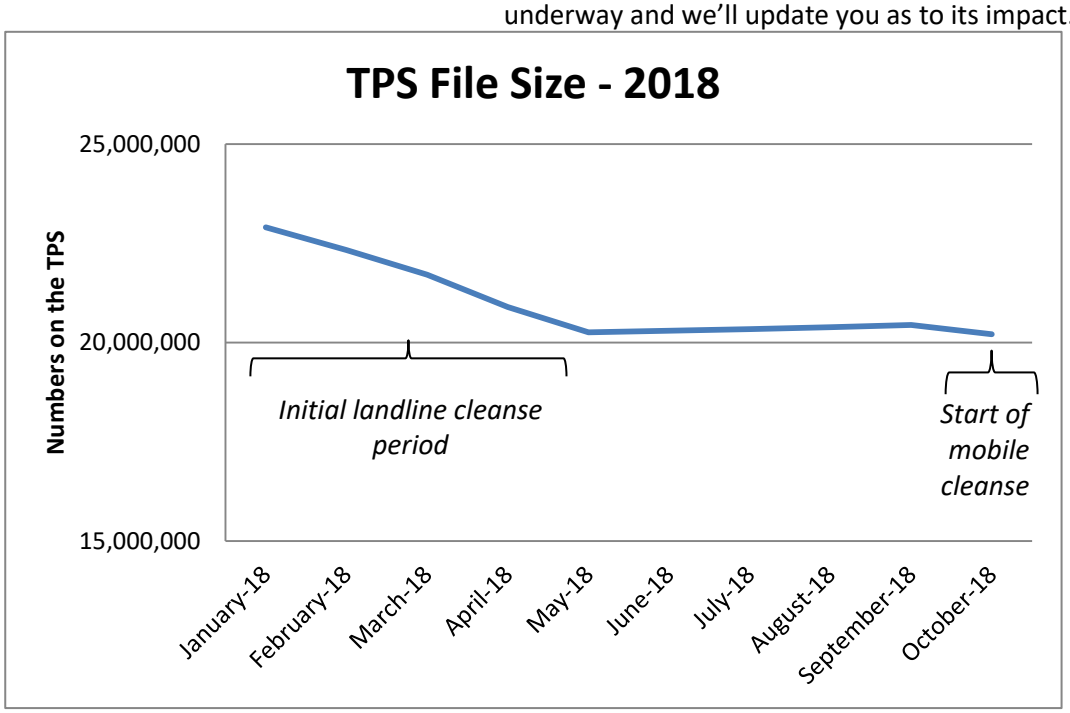
Contact Centre Council

Compliance & Regulation Hub Update

December 2018

Telephone Preference Service (TPS)

John Mitchison briefed the November Contact Centre Council meeting on the progress of the TPS data cleanse (www.dma.org.uk/press-release/dma-and-ico-update-to-tps-system), The file is now 2.7m numbers smaller than at the start of the year after the initial, bulk cleanse of landline numbers. The cleanse of mobile numbers is now underway and we'll update you as to its impact.



ICO Consultation on a Code of Practice for Direct Marketing

The ICO's consultation on a Code of Practice for Direct Marketing, which the Data Protection Act 2018 obliges it to produce is open until 24 December

www.ico.org.uk/media/about-the-ico/consultations/2260292/direct-marketing-code-of-practice-call-for-views.pdf

The DMA is understandably keen to be involved in the consultation and has asked members to contribute and specifically to address some questions which we've listed in an Appendix at the end of this Update.

Contact Centre Council

Compliance & Regulation Hub Update

December 2018

An Ofcom representative joining the Contact Centre Council's November meeting and gave a useful overview of Ofcom's research and priorities – including Persistent Misuse, which embraces silent and abandoned calls. The Council also discussed with Ofcom how robust statistics could help the Council to work with the industry to improve the consumer experience, while championing appropriate and value-generating outbound contact.

Ofcom has stepped in to cap the prices charged by 118 (Directory Enquiries) service providers to a maximum £3.65 maximum per 90 seconds. 118 118 has been charging an astonishing £11.23 for 90 second call and other providers up to £20!

www.ofcom.org.uk/about-ofcom/latest/features-and-news/new-price-cap-on-118-numbers

Also, in November Ofcom fined EE £6.3m and Virgin Media £7m (plus and additional £25,000 for not providing Ofcom with information when it was originally asked for) for over-charging millions of contract customers Early Exit fees. As part of the mitigation measures agreed, both organisations have changed their fees, processes and contact centre agent training and briefing.

www.ofcom.org.uk/about-ofcom/latest/features-and-news/ee-and-virgin-media-fined-for-overcharging-customers

Pensions Cold Calling Ban

Although in the summer the government confirmed its intention to get parliamentary approval to amend the PECR legislation to specifically ban pensions cold calling - with the ICO responsible for enforcement and the ability to fine companies up to £500,000 – there's still no sign of it happening.

Clearly there must be some more pressing business in Parliament, just now…

At last! PCI issues Guidance for Phone-Based Card Payments

A couple of years late, in November the Payment Cards Industry Security Standards Council issued v3.0 of its Guidance from the Protecting Telephone-Based Payments Special Interest Group. This Guidance specifically addresses contact centres and new phone and digital based 'scope reduction' technologies.

No doubt we will revisit the implications of the Guidance over future months, but we have had some clear interpretation from the Contact Centre Council's own Tom Davies (www.ultracomms.com):

Securing Telephone-Based Payments

The PCI SSC have now released guidance on protecting telephone-based payment card data to clarify how accepting spoken account data over the telephone puts personnel, the technology used, and the infrastructure to which that technology is connected into scope of PCI DSS.

The document provides supplemental guidance, which does not add, extend, replace, or supersede PCI

DSS requirements. Merchants and third-party service providers should work with their acquirers and/or payment card brands to understand their compliance validation and reporting responsibilities.
Three key areas are covered by the guidance; Call Recording, Call Routing/Processing and Third-Party Service Providers:

Call Recording
The challenge many call centres face is that local laws or regulation may require call recordings to be retained for a number of years. Organizations should consider the use of technologies which prevent card holder data (CHD) entering the call recording, while allowing the full call to be recorded.
Pause-and-resume technologies may be manual or automated, and whilst a properly implemented pause-and-resume solution could reduce applicability of PCI DSS by taking the call-recording and storage systems out of scope, the technology does not reduce PCI DSS applicability to the agent, the agent desktop environment, or any other systems in the telephone environment
Where pause-and-resume is used for call recordings, especially where initiated by the agent, it is recommended to verify that the call recordings do not contain CHD or sensitive authentication data (SAD) be undertaken on a regular basis preferably weekly.
Manual pause-and-resume implementations require constant monitoring and verification. The merchant will need to regularly confirm that the call recorder and call storage do not contain any CHD or SAD. This can be achieved by supervisors regularly listening to recorded conversations.
The degree of oversight and supervision required for manual solutions is much greater than for automated solutions.
The effectiveness of an automated solution relies largely on its integration with the agent's workflow process and the agent performing the correct steps at the correct time. If any ability exists for the agent to bypass the integrated process, the pause-and-resume technology could be circumvented and rendered ineffective.
In order to meet PCI DSS, controls should be in place to ensure that SAD is either not recorded or, if it is recorded, that it is securely deleted immediately upon authorization of the transaction. Where a merchant has failed to prevent the storage of SAD after authorization, the business MUST take all possible steps to immediately delete SAD. Additionally, analysis of the failure should be performed, and corrective measures identified and implemented to prevent the failure reoccurring.

Call Routing
Securing the voice transmission outside of the merchant's infrastructure is not considered within the merchant's scope, as the merchant cannot control the methods used by the cardholder to make and receive phone calls.
When an internal call transfer to a third-party payment processor is employed, the switching method within the merchant's environment remains in scope of PCI DSS.
If a service provider supplies a device onsite, upstream of an SBC or other telephony infrastructure, to redirect or re-invite the call away to carrier network service, this device is in scope for PCI DSS requirements
Where the service provider is situated close to the carrier network and the account data will be "intercepted" before it reaches the merchant's infrastructure rather than being redirected from it. This redirection should not have any impact on the merchant's infrastructure scope for PCI DSS.

Third Party Service Providers
The use of a third-party service provider does not relieve the merchant of ultimate responsibility for its own PCI DSS compliance, nor does it exempt the merchant from accountability and obligation for ensuring that its payment card data and card data environment (CDE) are secure.

The merchant must manage the relationship with the service provider as per PCI DSS Requirement 12.8, including listing of service providers, maintaining agreements and acknowledgement of responsibilities, carrying out due diligence prior to engagement, and monitoring the service provider's PCI DSS compliance status.

Summary
The PCI SSC have now made it clear - to fully de-scope the call centre environment from PCI DSS requirements; the voice transmission should be secured from outside of the merchant's infrastructure, with no on-premise equipment, and where the merchant cannot control call redirection to the payment solution. A fully network-delivered, "No-CDE" solution for telephone payments is the most effective way to secure personnel, the technology used, and the infrastructure to which that technology is connected.

The information Supplement can be found here: https://www.pcisecuritystandards.org/documents/Protecting_Telephone_Based_Payment_Card_Data_v3-0_nov_2018.pdf

More about Ultracomms here: https://ultracomms.com/news/ultracomms-warns-businesses-to-review-processes-as-telephone-payment-security-watchdog-issues-strict-new-guidelines/

Thanks Tom!

The Fundraising Regulator (FR)

The FR has announced that in 2019 it will have a new Chair – Lord Harris of Haringey – in succession to Lord Grade www.fundraisingregulator.org.uk/more-from-us/news/new-chair-fundraising-regulator

Controversially, from 1st March 2019 charities which are investigated by the FR will be named (not necessarily shamed?) *irrespective of the investigations' eventual findings*, in place of their current anonymous treatment.
www.fundraisingregulator.org.uk/more-from-us/news/fundraising-regulator-start-naming-organisations-it-investigates

DMA Privacy Taskforce

The Privacy Taskforce continues to focus on two main areas:

- Collaboration between DMA, its brand members and ISBA (www.isba.org.uk) to get some common ground on the implications of GDPR on advertising and big data
- Creating practical guidance around the requirements of implementing Privacy by Design

Contact Centre Council

Compliance & Regulation Hub Update

December 2018

Brexit News

Last week, the ICO issued data protection guidance to companies in the event of a 'no deal' Brexit.
This included 6 key steps that should be followed by way of preparation:
www.ico.org.uk/media/for-organisations/documents/2553958/leaving-the-eu-six-steps-to-take.pdf

DMA Awards

The winners of the DMA Awards special GDPR Communication category were The Guardian, Unicef & Suzuki.

www.dma.org.uk/article/dma-awards-winners-2018-1

ePrivacy Regulation

No real ePrivacy news or updates, this month.
As this recent DMA article explains, the EU Council of Ministers has committed to try and agree the rules around direct marketing – but it still seems likely that whatever's agreed won't get through the Parliament before elections in May 2019
www.dma.org.uk/article/eu-council-vows-to-continue-eprivacy-discussions

Contact Centre Council

Compliance & Regulation Hub Update

December 2018

GDPR, the new Data Protection Act and ICO

ICO Advisory Visits

The ICO has been publicising its free-of-charge advisory visits to assess and guide organisations. https://ico.org.uk/for-organisations/resources-and-support/advisory-visits/. The visits are theoretically open to all small & medium organisations, including companies, but resources are limited and nearly all of those to date have been in the third sector.

ICO Regulatory Sandbox

The ICO is busy developing a Regulatory Sandbox www.ico.org.uk/about-the-ico/news-and-events/blog-ico-regulatory-sandbox/. Data Privacy provocateur Tim Turner thinks it's an expensive "gimmick", but then he understands what a Regulatory Sandbox is. I don't.
By way of a Christmas Competition there'll be a small prize for the first person to send a plausible explanation to ccc@dma.org.uk

ICO in the Media

The ICO has been on the TV more often than Jacob Rees-Mogg, recently. Here's our friend Andy Curry on Watchdog the other night: www.bbc.co.uk/iplayer/episode/b0bv24fs/watchdog-series-40-episode-6

ICO Enforcement – Direct Marketing

There have been three marketing / contact centre-related enforcement cases from the ICO, this month. Covering a range of businesses – home improvements and tax rebates – all three highlight familiar ICO Enforcement themes.

DM Design of Cumbernauld has been fined £160,000 after making over 1.6m unsolicited calls to TPS subscribers between April and November 2017.
DM Design did have a TPS license to screen numbers, but investigations in 2018 showed that it hadn't been used for 18 months…
Two interesting aspects to this case:
1. In 2013 the ICO fined DM Design £90,000 for similar transgressions. As we've noted before (and the following cases illustrates), it's best not to have 'form' with the ICO.
2. DM Design's is another enforcement case that has been helped by the ICO lodging a Third Party Information Notice with 8x8 (www.8x8.com) - the parent company of DM Design's dialler technology provider, DXI. The fourth case to date, I think.
www.ico.org.uk/media/action-weve-taken/mpns/2553857/d-m-design-bedrooms-limited-mpn-23-november-2018.pdf

Contact Centre Council

Compliance & Regulation Hub Update

December 2018

Solartech North East, a solar energy installation firm based in Middlebrough, has been fined £90,000 for making over 74,000 unsolicited marketing calls to numbers registered on the TPS between May & June 2017.

As we have seen in other enforcement cases, recently, Solatrech show a pattern of non-compliance. They first came to the ICO's attention in 2014 with a high number of TPS complaints. At the time Solartech told the ICO that they had assumed that they third party data they had purchased for telemarketing had already been TPS screened, but purchased a TPS license so they could carry out TPS screening themselves. Again in 2016 Solartech came to the ICO's attention due to complaint volumes and received guidance and advice. The final investigation concluded that Solartech wasn't TPS screeing numbers nor carying out due diligence of its third party suppliers – despite their repeated assurances and guidance from the ICO.

Tax Returned Limited of London – a tax rebate claims company – has been fined £200,000 for sending over 14.8m unsolicited text messages in breach of PECR rules in 2016-17. Although a third party sent the emails, the ICO confirmed that Tax Returned was the instigator and therefore responsible for compliance. www.ico.org.uk/media/action-weve-taken/enforcement-notices/2553956/tax-returned-limited-en-20181210.pdf

Data Breaches

> "This was not only a serious failure of data security on Uber's part, but a complete disregard for the customers and drivers whose personal information was stolen. At the time, no steps were taken to inform anyone affected by the breach, or to offer help and support. That left them vulnerable."

Uber has been fined £385,000 by the ICO for a 2016 data breach – due to "avoidable data security flaws" - which led to the release of the personal details of 82,000 UK drivers. Uber waited a year to reveal the breach and paid the hackers $100,000 to destroy the driver data they'd captured.

Meanwhile the ICO has issued 100 fines to organisations – across a range of sectors including business services, construction, finance, health and childcare - which have failed to pay their annual Data Protection Fee.

Research from law firm RPC, shows a 165% increase in whistle-blowers' data breach reports to the ICO since GDPR came into force last May - 82 reports from June-August vs 31 February-March, pre-GDPR. www.rpc.co.uk/press-and-media/gdpr-introduction-sees-whistle-blower-reports-on-data-breaches-rise-165-percent/

Contact Centre Council

Compliance & Regulation Hub Update

December 2018

Just before 'Black Friday' Amazon admitted to a data security flaw which made customer data vulnerable to external access, but refused to say how many customers' data was exposed.

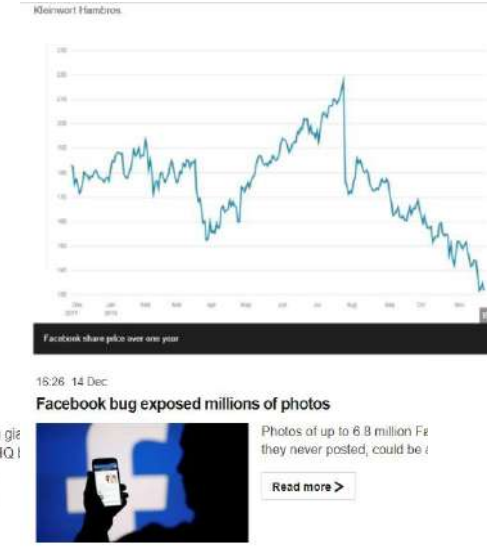
Marriott Hotels Group has revealed a data breach impacting 500m guests, which included information such as passport numbers, emails, date of birth, gender and mailing addresses – and possibly payment card data, too. The data had been exposed for up to 4 years. The ICO and the New York Attorney General are investigating…

Politics Corner

Facebook has appealed the ICO's £500,000 fine for its inappropriate use and sharing of users' data for UK political campaigning.

www.ico.org.uk/media/action-weve-taken/mpns/2260051/r-facebook-mpn-20181024.pdf

And elsewhere Facebook's barely been out of the news over the past month…



Contact Centre Council

Compliance & Regulation Hub Update

December 2018

Direct Marketing Commission

No news from the DM Commission this month – and probably won't be until next year's annual report for 2018.
www.dmcommission.com/?attachment_id=3507

And Finally

A really fascinating article in the New York Times, last week, which revealed the hundreds of apps which are tracking consumers' movements – apparently without any of the transparency that the GDPR requires (at least in theory) in the UK and Europe
www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html

Appendix

The DMA has gathered member's thoughts for the ICO's consultation on a new direct marketing Code of Practice

www.dma.org.uk/article/what-do-marketers-need-from-the-icos-new-direct-marketing-guidance

but you still have until 24th December to respond directly to the ICO. Some question the DMA posed to its members which may help frame your thoughts are:

Q1 The code will address the changes in data protection legislation and the implications for direct marketing. What changes to the data protection legislation do you think we should focus on in the direct marketing code?

Q2 Apart from the recent changes to data protection legislation are there other developments that are having an impact on your organisation's direct marketing practices that you think we should address in the code?

Yes/No

Q3 If yes please specify

Q4 We are planning to produce the code before the draft ePrivacy Regulation (ePR) is agreed. We will then produce a revised code once the ePR becomes law. Do you agree with this approach?

Yes/No

Q5 If no please explain why you disagree

Q6 Is the content of the ICO's existing direct marketing guidance relevant to the marketing that your organisation is involved in?

Yes/No

Q7 If no what additional areas would you like to see covered?

Q8 Is it easy to find information in our existing direct marketing guidance?

Yes/No

Q9 If no, do you have any suggestions on how we should structure the direct marketing code?

Q10 Please provide details of any case studies or marketing scenarios that you would like to see included in the direct marketing code.

Q11 Do you have any other suggestions for the direct marketing code?