CHANNEL DOCTORS

Compliance Newsletter

January 2020

Compliance News for Customer People

This Month's Headlines

- **Finally, the ICO's released it's draft Direct Marketing Code of Practice for consultation - and it really does need a close read**
- **Keen on using AI, but can't explain how it works? The ICO says you need to be able to!**
- **Data can be breached through cardboard storage boxes and shop tills, not just in the cloud**
- **"Told you so" chorus PCI solution vendors after the ICO quotes its own guidance**
- **How identifying & verifying customers in your contact centre may be about to get even more tricky**
- **The ASA returns to the vexed issue of (banned) gender stereotyping. Do you and your advertising agency understand the confusing rules?**

Start 2020 as you mean to go on... by having a crash course in compliance & regulation news for people in Sales, Marketing & Customer Experience. Read on!

If you can't avoid compliance and regulation, then why not get a better understanding of it? Better informed, you can meet the compliance challenges when acquiring, retaining and servicing customers.

It's been a busy month, so there's lots to cover. Welcome to the eighth issue:

Information Commissioner's Office

Direct Marketing Code

The most important news from the ICO, this month, is that it has produced a Draft Direct Marketing Code of Practice, designed to be aligned with GDPR / the 2018 data Protection Act. This consultation is vitally important for anyone responsible for just about any form of sales and marketing. And even for those in pure customer service roles, as the ICO's definition of 'direct marketing' can be surprisingly broad.

The draft Code is quite substantial (123 pages), but a quick read has already flagged up a number of areas of concern in terms of current marketing techniques that may become forbidden.

The consultation is open until 4th March, so have a read and share your thoughts. You can either do this directly to the ICO (email directmarketingcode@ico.org.uk) or via a trade body like the DMA if you're a member (and the DMA's Privacy Working Group has already started reviewing the draft Code).

AI Transparency - Not Just for Techies

The ICO's consultation on the use of AI and decision making – specifically, how AI-derived decision making is explained to consumers and citizens – is open until 24 January. The consultation is based on the interim Project ExplAIn (geddit?) report which the ICO has co-authored with The Alan Turing Institute . The GDPR doesn't specifically refer to AI, but has plenty to say about 'automated decision making'. The citizen juries' research which informed the report was – understandably – focused on public policy AI decisions in the NHS and criminal justice system. However, the growth of AI techniques in the profiling, targeting and pricing of marketing communications, as well as customer care, all mean that this consultation may well be relevant to us all.

CHANNEL DOCTORS

ePrivacy Regulation

Word on the Brussels street (boulevard?) is that after the failure to get the draft ePrivacy Regulation text agreed before the end of the Finnish EU Presidency at the start of December, then the whole subject is now in the long grass.

ICO Enforcement Actions

Two enforcements in the commercial world, this month. Both are not directly customer-related, but of interest.

Doorstep Dispensaree has been fined £275,000 for breaching the Data Protection Act 2018 and failing to keep special category customer data secure. c.500,000 documents containing names, addresses, dates of birth, NHS numbers, medical information and prescriptions were left unlocked and insecure.

The initial investigation of Doorstep Dispensaree was triggered by a Medicines and Healthcare Products Regulatory Agency (MHRA) email to the ICO in July 2018. The MHRA was investigating the insecure storage of medicines and found 47 crates, 2 bags and a cardboard box containing soggy documents showing personal data left unlocked in a courtyard at the rear of Doorstep Dispensaree's premises.

The ICO rejected Doorstep's defence that their records disposal supplier was responsible for the breach and ruled that as the data controller Doorstep was responsible. If only someone could have warned them of this sort of thing – Oh, we did, in this blog post 2 years ago:

https://channeldoctors.co.uk/2018/01/05/what-s-inside-the-battered-cardboard-box/.

ICO monetary penalties may be a civil matter, but calling your company Doorstep Dispensaree should be a criminal offence

Dixons Carphone has been fined £500,000 for its well-publicised 2018 data breach, which exposed the personal data of 14 million customers. A hacker had installed malware on over 5,000 tills in Currys PC World and Dixons Travel stores, giving them access to customers' data for many months. Whether the hacker was successful in exploiting this data in unclear, but what's obvious is that Dixons dodged a big fine bullet by remedying the breach just weeks before GDPR and the 2018 Data Protection Act came in force.

Dixons' case probably wasn't aided by the £400,000 fine for a 2015 data breach levied on Carphone Warehouse in 2018…

By the way, just in case you were getting tired of people (PCI solution vendors, usually) trying to persuade your organisation to change processes and spend money in order to comply with the PCI-DSS rules, it just gets worse: The ICO's notice says "Although compliance with the PCI-DSS is not necessarily equivalent to compliance with the GDPR's security principle, if you process card data and suffer a personal data breach, the ICO will consider the extent to which you have put in place measures that PCI-DSS requires particularly if the breach related to a lack of particular control or process mandated by the standard." We've been warned.

"Although compliance with the PCI-DSS is not necessarily equivalent to compliance with the GDPR's security principle, if you process card data and suffer a personal data breach, the ICO will consider the extent to which you have put in place measures that PCI-DSS requires particularly if the breach related to a lack of particular control or process mandated by the standard."

Meanwhile, about that £282m...

This article by Jon Baines explains that the massive, GDPR-era fines the ICO announced last summer that it was minded to impose on BA and Marriott for their respective data breaches have still not been confirmed. A 3 month extension of the process has been agreed, but why and whether negotiations to reduce the fines are underway is unclear.

Global Data Review has reported that the ICO will no longer offer its traditional 20% discount on monetary penalties to companies that pay up within 28 days and don't appeal the fines. The ICO hasn't explained why.
The number of fines are only likely to increase in the future, a 20% reduction would come in handy if you had the funds to pay (a £36m saving for BA if the ICO's proposed £183m fine stands) and - as we explained last month - a failed appeal can sometimes result in an even bigger fine. So, the end of the early payment reduction scheme seems a little odd.

Although different EU regulators' interpretations of the GDPR rules vary, here's a cautionary tale from Germany.
The German equivalent of the ICO has fined internet services provider 1&1 £8m for what it considered the inadequacy of its identification and verification of customers through contact centres. 1&1 used name and date of birth which the regulator considered to be far too widely accessible to be secure. 1&1 is appealing the fine and has since introduced a customer Personal Identification Number, for customers.


Technology

Internet provider faces big GDPR fine for lax call centre checks

By Leo Kelion
Technology desk editor

11 December 2019

Share

GETTY IMAGES

The fine will serve as a warning to other call centre operators, say experts

If your internet services provider allocated you a PIN code that had to be used every time you needed to contact them - say, when your website was down - do you think that would help your customer experience? I doubt it!
How to allow customers to securely identify themselves without making the whole process arduous for customers is a perennial one. And if the German experience is anything to go by it will only become more challenging.

Accreditation
Although there are lots of training courses and awards in data protection law available, none are yet certified by the ICO for GDPR and the 2018 Data Protection Act. The ICO is required to set up an accreditation scheme and before Christmas it announced that it would be working with the UK Accreditation Service to do so - which seems to make sense.

The Insolvency Service
The directors of firms which have failed to pay ICO fines (and, typically, failed to pay HMRC and carious other creditors too) are increasingly being pursued by the Insolvency Service and handed out bans on their acting as company directors in future.

Charlotte McKeever has been banned as a company director for 7 years. McKeever was the MD of Advanced VOIP Solutions. This case dates back over 3 years to when the ICO fined Advanced £180,000 for its central role in a network of Manchester and Cheshire-based operations making automated claims management marketing calls about personal protection insurance, packaged bank accounts and flight delays which generated over 6,000 complaints to the ICO. The fine was never paid and the company folded, which prompted the Insolvency Service's involvement.

One aspect of the PECR infringements which didn't seem to be publicised at the time of the fine is that Advanced also offered to block future calls to consumers – if they paid a fee! Thrillingly, there's even a brief video from the ICO of their raids (featuring FBI-style blouson jackets, of course).

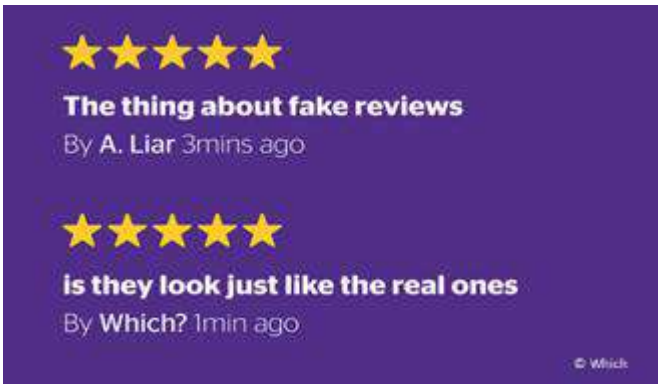
Jason Gambling of Basingstoke has also been banned from acting as a company director for 7 years. Gambling was the sole director of telemarketing lead generation firm The Legend Alliance.
The ICO started to investigate The Legend Alliance in January 2017 after consumer complaints about unsolicited calls. The ICO established that over 21 million unsolicited calls were made between February and May 2016, in breach of the PECR regulations.

Gregory Rudd was the sole director of Keurboom which was fined £4000,000 under PECR in 2017 for being responsible for making 99.5million automated marketing calls to consumers without their consent. After winding up the firm without paying the fine, Mr Rudd has been barred from acting as a company director for 6 years.

The CMA released its initial findings from a major investigation into the UK digital market before Christmas. Unsurprisingly, it identified that Facebook and Google are in very dominant market positions*. The CMA's investigations will continue to consider whether Facebook and Google are exploiting their market dominance and what regulatory actions may need to be taken if they are.

** This sounds like 'what bears do in woods' or 'the Pope's current religion' stuff, but it's a start*

Separately, Facebook and eBay have pledged to combat fake reviews after a CMA investigation. The CMA's press release emphasised that it wasn't alleging that Facebook or eBay were intentionally allowing fake reviews to appear, but it would be optimistic to think that fakery can be addressed quite so easily; the CMA may well be returning to this topic.



There was no mention of Amazon or Goggle in this, so presumably their reviews are all genuine?

Ofcom's announced the withdrawal of service of 0500 numbers. As none have been newly issued in 20 years and there has been a 3 year process of either closing or migrating remaining 0500 numbers, this *shouldn't* have an impact on anybody.

But if yours is a large, established organisation, it may be worth a quick check that legacy references to old 0500 numbers aren't still hidden about your website or other collateral

The **ASA (Advertising Standards Authority)**'s recent rulings allow us to ponder the advertising of alcohol the fraught role of social media influencers, and gender stereotyping...

BrewDog is regularly on the ASA's naughty step and is again after its 'Sober as a Motherf____' billboard was banned from being re-used. For fairly obvious reasons.

CHANNEL DOCTORS

It's almost as if BrewDog and their agency* wanted *the ASA to ban its ads and create lots of free additional publicity….

Two Southern Comfort social ads – Instagram posts – have been banned because they were promoted by social media influencers (Francesca Perks & Jack Remmington – *no, me neither*) who both either were or appeared to be under 25 years old, which is against the rules.

Two ads have been banned for breaking the ASA's new(ish) rules on gender stereotyping:

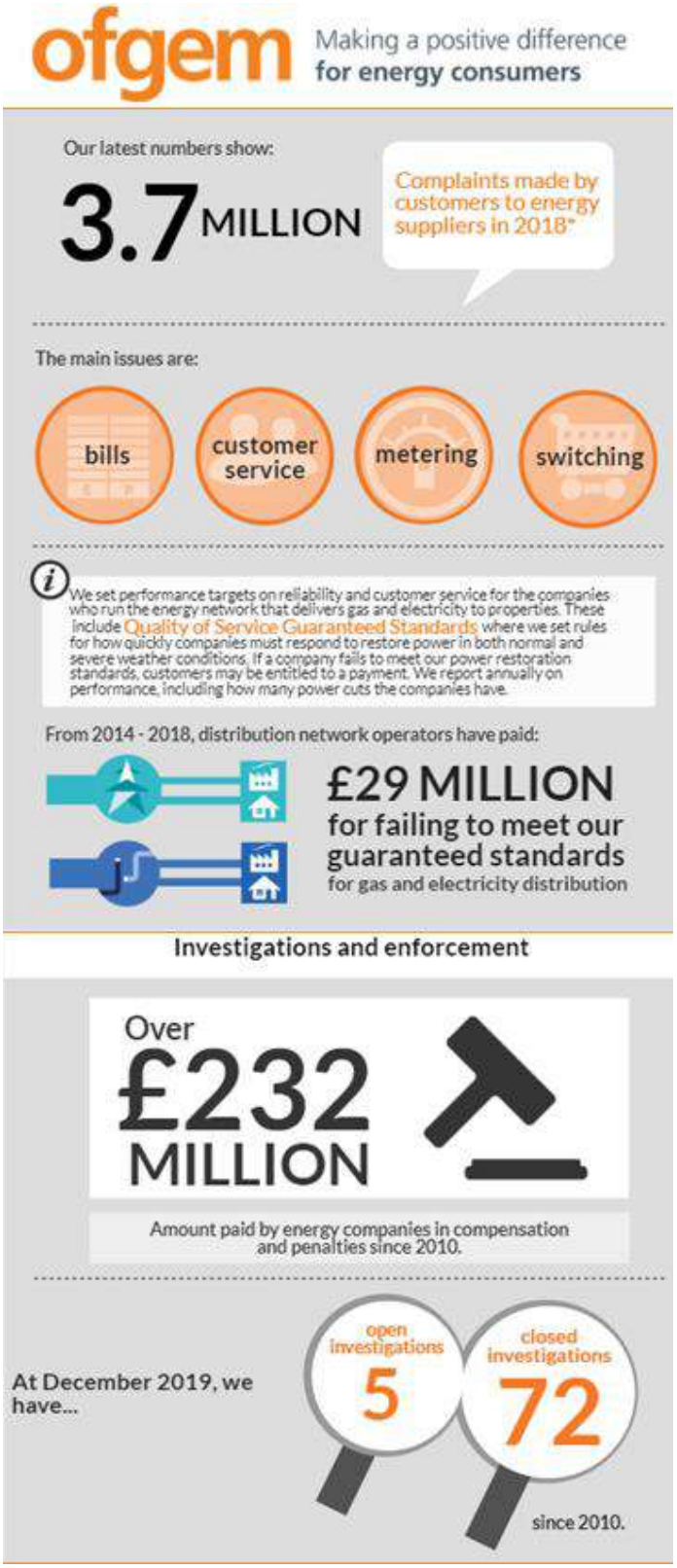
1.PC Specialist's TV ad featuring male PC users doing high-end gaming, coding, illustrating and music production has been banned after complaints that it perpetuated gender stereotypes.

2. Freelance worker website People Per Hour has had a tube advert featuring a female business owner labelled a 'girl boss' has also fallen foul of the ASA's gender rules.

The ASA has reiterated that its rules don't mean advertisers can't have adverts just featuring one gender, but that to do so while implying only one gender had the expertise for a certain activity – e.g. gaming or music creation, in the case of PC Specialist - isn't acceptable (even if 87% of PC Specialist's customers are male). People By the Hour's 'Girl Boss' ad was just considered patronising.

CHANNEL DOCTORS

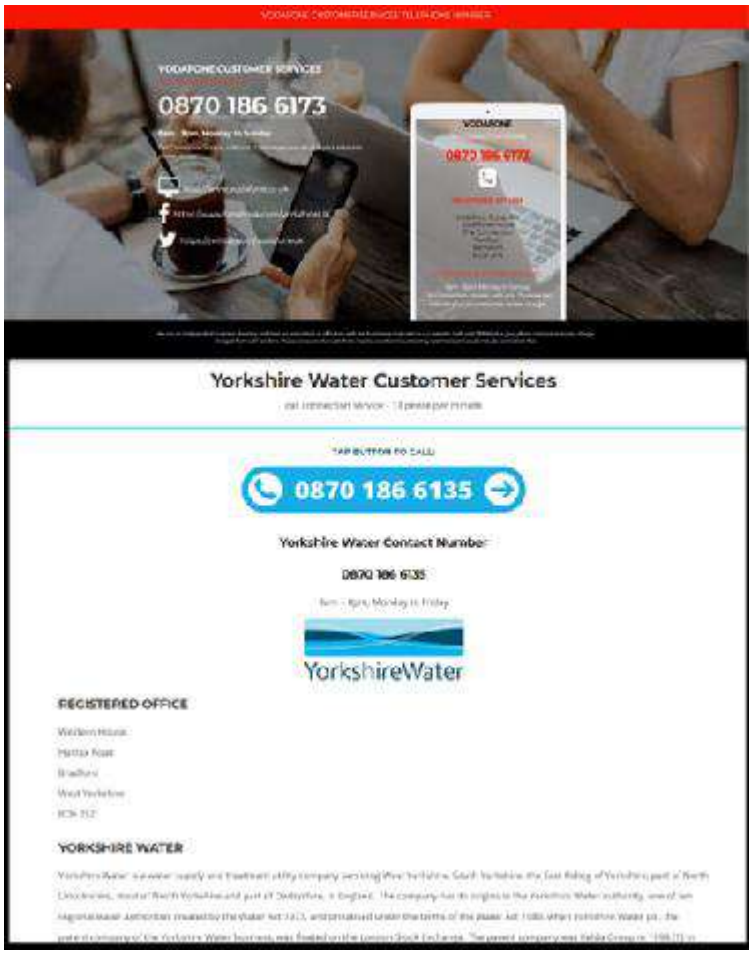
If all these bans, fines and restrictions are getting you down, this infographic from Ofgem shows how much harder life could be if you worked in the energy sector:



PSA

Phone-paid Services Authority

Tobaji – a company which has failed to pay a PSA fine levied in late 2018 – has been barred from operating in the premium rate world for another 5 years.



The PSA has fined ECN Digital £250,000 for operating a fraudulent - or at least deceptive - 'call connection' service (is there any other kind?).

Their online service provided big brands' customer service and contact numbers to consumers via paid Google searches. However, ECN was unclear that the webpages provided were theirs, not the brands' own content; didn't clearly explain that they were running a charged service; and were insufficiently clear that they charged a connection fee of "13PPM" which was confusing in itself.

CHANNEL DOCTORS

Some interesting research findings were issued by the Fundraising Regulator, this month. The FR sampled some charities' annual reports and found that 60% failed to give sufficient information about their fundraising practises to meet the requirements of the 2016 Charities (Protection and Social Investment) Act. Themes identified included:

- limited detail about how fundraising campaigns are run and managed, including who carries out the work;
- failure to demonstrate how the Code of Fundraising Practice is used to guide their work;
- a lack of thorough description about fundraising carried out on behalf of the organisation;
- frequent omission of the number of complaints received; and
- limited explanation of how vulnerable people are protected in the organisations' fundraising work.

Although this is obviously only a concern for people working in fundraising (and, crucially, charity trustees who will be held responsible for the accuracy and quality of the information held in annual reports), there are some issues identified with wider currency for all marketers:

- The treatment of people with vulnerabilities
- Being able to detail how (marketing) campaigns are run and managed – including 3rd parties and service providers' roles
- The tracking of complaints

Before you go

Are we covering the regulatory bodies and areas that keep you awake at night? Who and what else would you like to see covered in 2020's monthly newsletters about the world of regulation and compliance as it affects customer engagement? Let us know at hello@channeldoctors.co.uk

Subscribe here http://eepurl.com/gqxzw5 and you will receive next month's edition direct to your in-box in February