



As the UK heads into the 2nd lockdown of 2020 have we become more resilient and will this lockdown be the last? The outlook for the global economy is bleak and our transition period with the EU ends in less than two months. There is a lot to consider for businesses large and small all across the country trying to balance the books and find a way through to survive. There are many ways in which we can support you through these troubling times

In this edition of

News * Events * Offers & Editor Opinion

[Page 2](#)—Spotlight on the recent outcome from the ICO on British Airways & Marriott Hotels' data breaches

[Page 3](#)— DPA (Hamburgs Data Protection Authority) enforcement action against H&M and Experian find themselves in trouble with the ICO.. again..

[Page 4](#)— Updated ICO guidance on the Right of Access & a reminder about Test & Trace data collection arrangements

[Page 5](#)— Partnerships & Free Health Checks

[Page 6](#)—Editor opinion & Meet the Team

Connect with us on Social Media for regular updates



SPECIALISTS IN,
**Data Privacy, Regulatory
Compliance, Culture & Training**

Latest Enforcement Action

October 2020 Roundup

ICO Dishes out record fines

2 global companies have this month been fined by the ICO.



On 30th October 2020 the ICO announced that they had fined Marriott International £18.4 million for failing to keep the personal data of 339 million guests worldwide secure. This is down £80.8 million from the originally proposed fine of £99.2 million issued in July 2019.

The breach relates to a cyber incident which was notified to the ICO by Marriott in November 2018. Starwood hotels group were acquired by Marriott in 2016, however their systems were compromised in 2014. The ICO investigation found that Marriott failed to undertake sufficient due diligence when it bought Starwood and should have done more to secure its systems.

The reduced fine has come after the ICO considered representations from Marriott, the steps they have taken to mitigate the effects of the incident and the economic impact of COVID-19 on their business.



On 16th October 2020 the ICO announced that they had fined British Airways £20 million for failing to protect the personal and financial details of more than 400,000 of its customers. This is down £163.39 million from the originally proposed fine of £183.39 million.

BA were processing a significant amount of personal data without adequate security measures in place. This led to a cyber attack in 2018, which went undetected for more than 2 months. The attacker is believed to have potentially accessed the personal data of approximately 429,612 customers and staff, including the names, addresses, payment card numbers and CVV numbers of 244,000 BA customers.

The ICO has said: "People entrusted their personal details to BA and BA failed to take adequate measures to keep those details secure. Their failure to act was unacceptable and affected hundreds of thousands of people, which may have caused some anxiety and distress as a result. That's why we have issued BA with a £20m fine – our biggest to date".

This fine will have been significantly reduced due to the improvements made by BA since the breach, as well as the ICO considering the economic impact of COVID-19 on their business.

Latest Enforcement Action

October 2020 Roundup

Biggest fine issued by German regulator for breach of GDPR

On 1st October 2020, the Data Protection Authority of Hamburg announced that they have fined H&M with a €35.3 million fine, the highest fine issued to date issued in Germany.



This was due to the wrongful collection of the personal data of some of their employees. The data collected went well above and beyond that which should be reasonably collected by an employer involving those employees private lives.

Included in that data collection some team leaders even collected information on private family issues and religious beliefs in some great detail while having casual conversations with their employees.

The data was accessible by up to 50 managers in H&M and was used to create profiles on employees to make decisions regarding their employment.

H&M apologised to employees and agreed to compensate those affected. They have since put measures in place to address this going forward.

ICO takes enforcement action against Experian

The ICO has ordered the credit reference agency Experian Limited to make fundamental changes to how it handles people's personal data within its direct marketing services.



There has been a 2 year investigation by the ICO into how Experian, Equifax and TransUnion used personal data within their data broking businesses for direct marketing purposes.

The ICO found that significant 'invisible' processing took place, likely affecting millions of adults in the UK. It is 'invisible' because the individual is not aware that the organisation is collecting and using their personal data in that way.

And although Experian made progress in improving compliance, it did not go far enough, did not agree that changes were required as set out by the ICO, and were not prepared to issue privacy information nor cease the use of credit reference data for direct marketing purposes.

Experian have now therefore been served an enforcement notice to ensure they make the changes within 9 months. Failure to do so could result in a fine from the ICO.

ICO Updates

October 2020 Roundup

New guidance from the ICO on Right of Access

On 21st October 2020 the ICO published new guidance on the Right of Access, a key right under the GDPR.

This guidance went out for consultation in December 2019 and 350 responses were received which has helped to shape this published guidance, but there was call for more clarity around 3 areas which the ICO have responded to within the guidance.

This is






1. Stopping the clock for clarification
2. What is a manifestly excessive request
3. What can be included when charging a fee for excessive, unfounded or repeat requests.



You can access the guidance by clicking [here](#)

Contact Tracing — Five Steps for Businesses

Track & Trace, also known as Test & Trace is the new norm when visiting pubs, restaurants and cafes, however some businesses are unaware of the laws that protect the obtaining of personal data, and many businesses are getting it wrong. Follow the 5 steps issued by the ICO so you don't become a feature of our enforcement news in the coming months!

	Ask for only what's needed — You should only ask people for specific information that has been set out in government guidance, such as name, contact details & time of arrival. You should not ask for identify verification unless it's standard business practice - e.g., ID checks in pubs
	Be transparent with customers — You should be clear, open & honest with people about what you are doing with their personal information. Tell them why you need it and what you will do with it. You could do this by displaying a privacy notice.
	Carefully store the data — You must look after the personal data you collect. That means keeping it secure on a device if you're collecting data digitally, or for paper records, keeping information locked away and out of public sight. Click here for more guidance on simple security measures you can take.
	Don't use it for any other purpose — You cannot, and must not use the personal information you collect for contact tracing for other purposes, such as marketing, profiling or data analytics. It's your responsibility to ensure your employees don't use contact tracing data for their own use.
	Erase it in line with Government guidance — You should not retain the data for longer than the government guidance specifies. It's important to securely dispose the data to reduce the risk of someone else accessing it. Shred paper documents and permanently delete digital data, including backup cloud storage.

Beacon Updates

October 2020 Roundup

Beacon Partners

We recognise the importance of collaborating in order to help our business to succeed. We don't aim to be experts all in all fields, but recognise that there are important aspects surrounding data where others have relevant expertise that can assist.

We have therefore partnered with the following carefully selected partners (please click an image to visit their website).



HARNESS



Our latest webinar can be viewed [here](#) which looks at staying data safe in the new world of business as a result of the pandemic. Our affiliate partners, Accelerate Technologies joined us to bring the technical aspect of how businesses of all shapes and sizes can ensure they have the right technical controls and systems in place to prevent data loss and cyber attacks.

More information on our partnerships in general, can be found [here](#)

Free health checks—a great way to check compliance

We want to support businesses big and small in understanding what their position is when it comes to compliance with DP law and also adherence to the ISO27001 standard for information security.

We do this free of charge and even provide you with a report, providing recommendations and RAG statuses to help you understand your level of risk.

There is no obligation to take the relationship any further, but if you would like Beacon to help you to implement some of the recommendations, then we are here to help.

We've pulled together a couple of handy blogs to help you understand more about what the health checks involve.

Please [click here](#) to find the blogs.

Editor Writes..

October has been a busy month in terms of fines and regulatory activity. There is more that we could talk about in this newsletter, such as the ICO assessing companies contact-tracing services to pubs and restaurants for how they are approaching their data protection responsibilities. The Information Commissioners Officer confirmed it has written to 15 companies to assess their data protection practices including direct marketing.

The fines to the Marriott and British Airways are the first substantial fines issued by the ICO in the new world of GDPR, but they are a lot less than the originally proposed figures. This is understandable based on the climate that those companies find themselves in during the pandemic, but some will question whether the ICO is really showing their teeth and making other companies take note, that they are a regulator that should be taken seriously or face the consequences.

With less than 2 months to go before the end of the UK's transition period ends it's highly likely that we will exit without an EU trade deal. With us all being consumed over the past 9 months with the pandemic, the survival of our businesses and protecting ourselves and loved ones has been our main focus. We still don't know what the 1st January will bring and how businesses will be impacted but that shouldn't allow complacency. For data protection, third party contracts should be reviewed and you should identify your data flows to understand whether they cross borders will put you in good stead. To support you, we will be launching a GDPR & Info Sec Health Check in November to highlight any areas that need action taken to avoid your business being impacted by the UK's exit at the end of this year.

If you would like to keep up to date with these moving developments visit our [news page](#) or follow us on [Linkedin](#) or [Twitter](#)

Meet the Team

[JAMIE SWAN PC.DP](#)



Specialising in Data Privacy law, Jamie has worked with blue chip organisations, serving millions of customers to implement their GDPR programme. Jamie has also supported organisations to understand the implications of Brexit on data protection, ensuring appropriate mechanisms are in place to maintain compliance, as well as helping companies to change cultures and bring their Data Protection compliance up to standard.

[PETER BERRY PC.DP](#)



Peter's main area of expertise is regulatory compliance, working with some of the largest energy suppliers and generators in the UK. He is a member of a number of industry working groups and committees, advising on regulation, including data privacy.

He is a qualified business coach, and this helps to embed a culture of compliance rather than black and white rules enforced on people and organisations.