

A BIBA BROKERS' GUIDE TO

DIGITAL TECHNOLOGY

2020 – Issue 2



BIBA

In association with



DAC BEACHCROFT



WELCOME

CONTENTS

- 3** Balancing innovation and regulation in the insurance industry
- 4** Big Data: The only way is ethics
- 6** Big Data challenges
- 7** Preparing for a driverless future?
- 9** Cyber and the legal landscape
- 10** 5G and connected cars



BIBA's supplements are brought to you through a partnership of BIBA, Allianz and DAC Beachcroft.

We hope that you find DAC Beachcroft's legal expertise, Allianz's industry knowledge and BIBA's desire to share these with you helpful.

We welcome ideas for future subjects.

BIBA cannot guarantee, and does not accept any responsibility or liability for the accuracy or completeness of the content by other authors.



As we publish this Brokers' Guide to Technology in June 2020 many of us are working at home and relying greatly on technology to carry out our usual daily tasks. It is opportune then to provide guidance on this topic.

Innovation and technology have certainly helped us get through lockdown but the application of both is much wider.

This guide considers the ethical, legal and regulatory aspects of using data, and the added complication of 'Big Data'.

We also look to the future – E-mobility, connected cars and driverless vehicles as well as artificial intelligence. And no guide to technology would be complete without a look at cyber-crime (and its increase during the Covid-19 crisis), data security and the coming use of 5G.

All of these have implications for insurance and I think you'll find this a compelling read.

Mike Hallam, ACII, Chartered Insurance Practitioner, Head of Technical Services, BIBA

BALANCING INNOVATION AND REGULATION IN THE INSURANCE INDUSTRY

Increasingly, customers expect digital interactions when making purchases from companies and insurance customers are no exception. From arranging and purchasing insurance at the touch of a button, to notifying claims through apps, customers and brokers not only want convenience but also a more tailored service.



AUTHOR:
ADAM RATES, HEAD OF IT STRATEGY &
ARCHITECTURE, ALLIANZ



This could be achieved through flexible 'on-demand' insurance (e.g. cover required for only a short period of use) or through methods such as telematics for individual and motor fleet insurance. The insurance industry is recognising that embracing innovation and exploiting new and emerging technologies can go a long way to achieving true customer-centricity.

A REGULATED INDUSTRY

However, the digitalisation of insurers is not without its challenges and risks. True customer personalisation requires data – and lots of it. As a heavily regulated industry, insurers are (quite rightly) subject to a wide breadth of legislation and regulation. Arguably the most prominent of recent times is the General Data Protection Regulation (2018 GDPR) and as insurers collect more granular data on customers, the more they will fall under the scrutiny of the Information Commissioner's Office (ICO).

Data also attracts the attention of cyber criminals and cybersecurity has been named as the top emerging technology which insurers are investing in globally¹. Cyber presents a very real threat to companies and places new burdens on directors and data protection officers, as discussed in-depth on page 9.

ARTIFICIAL INTELLIGENCE

Artificial Intelligence (AI) is already being used to the industry's advantage, such as the application

of chatbots for answering customer queries or selling policies, or for image recognition in claims assessment. However, some experts are calling for greater regulation around the use of AI². In December 2019, the ICO, together with The Alan Turing Institute, published detailed guidance entitled, "[Explaining decisions made with AI](#)"; this referenced GDPR, the Data Protection Act 2018 and the Equality Act 2010 as being relevant wherever AI uses personal data. However, there's an argument that working in such a highly regulated market can be an advantage rather than a blocker when it comes to implementing AI. Insurers have always been required to explain their decision-making processes and AI enables this to be more transparent and auditable, since the outcome can be traced back to certain inputs and algorithms.

SUMMARY

Historically, innovation and regulation have seemed to be at opposite ends of a spectrum with the former associated with experimentation and risk-taking and the latter with control. However, there's growing evidence that adopting new technologies can help insurers automate and de-risk processes, making it easier to comply with regulation whilst offering more superior products and levels of service to customers.

¹ Global Emerging Technology Trends Survey 2019. GlobalData. 2019

² Why Google thinks we need to regulate AI. Financial Times. January 2020. <https://www.ft.com/content/3467659a-386d-11ea-ac3c-f68c10993b04>

BIG DATA: THE ONLY WAY IS ETHICS

AUTHOR:
JAMES TUCKER, MANAGER,
SMART TECHNOLOGIES, ALLIANZ



Data is everywhere and growing at an exponential rate. According to cloud software firm DOMO, there is forty times the amount of bytes of data than stars in the observable universe.¹

Insurance companies have access to huge amounts of data, but this sector has not been one of the first to leverage its potential.

Data comes from myriad sources (including policy and claims records, social media, credit reference agencies, equipment sensors) but data on its own is useless. It only becomes effective once processed, analysed and/or modelled, and then used for a specific purpose. Making sense of so much information and using it in a timely manner (often near real-time) requires specialist infrastructure and skills. And the skills required are broad – they include IT skills, data science skills and legal/regulatory expertise.

Companies which are able to effectively exploit data can reap diverse benefits, ranging from optimised underwriting to tailored proposition development, better customer segmentation and fraud reduction. Big Data presents huge opportunities for companies to gain competitive advantage, but attention must be paid to the following key subjects: consumer privacy, regulation and data ethics.



CONSUMER PRIVACY AND REGULATION

Many consumers are happy to cede a level of privacy and share personal data if they stand to benefit; a Mulesoft survey revealed that nearly two thirds (62%) of 18-34 year olds stated they would be happy for their insurance provider to use third-party data from social media platforms in return for a more personalised service and better premiums.² This willingness declined as age increased and UK consumers were more cautious about the use of third-party data (36%) than those in Singapore (63%) or the U.S. (49%).

As more and more customer data has become available to businesses, it's no surprise that these businesses have developed inconsistent views about how this data should be managed, and the appropriate level of privacy that should be attached. To address this issue, and to make it easier for EU consumers to understand and control how their personal data was stored and used, the General Data Protection Regulation (GDPR) was introduced in May 2018.

Customers' data is not just protected by GDPR. The Equality Act 2010 exists to protect all individuals from discrimination based on characteristics including age, disability and race. Insurers are forbidden from instigating blanket policies whose terms uniformly disadvantage one such group.

The law does accept that certain exceptions may apply; for example, an insurance provider would be allowed to consider a disability as an influencing factor if the insurance risk was greater as a direct result.

DATA ETHICS

Artificial intelligence (AI) can unlock the power of Big Data. It enables companies to make sense of massive data sets, but the use of AI and machine learning algorithms, which provide much deeper

insight into Big Data, bring ethical challenges. Users must be aware of bias which may exist in the data and know how to minimise its effects on the models they are building. Although machines do not have human bias, they use data which does, so "AI models can embed human and societal biases and deploy them at scale".³

One oft-quoted example of an algorithm with embedded bias is within the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) software used in the U.S. criminal justice system by some states to predict the likelihood of criminals reoffending. COMPAS has come under criticism for its alleged bias against minority ethnic groups.⁴

Insurance, an industry based on risk profiling, must also guard against risks of bias in the data, whether in relation to age, demographic factors, or even some random factors where there may be a chance correlation to risk but no rational explanation, or causation – such as drivers called 'David' being more risky than those named 'Peter'.

AI can help improve data transparency and highlight bias where a process is continually tested, with a view to examining and explaining decisions made. This 'explainable AI' can help expose vulnerabilities and flaws and ultimately feed into data ethics models. For now, at least, it seems that a combination of AI and human involvement is the ideal approach.

The growing use of AI has prompted the Government to set up the Centre for Data Ethics and Innovation (CDEI) which advises on best practice for responsible use of data-driven technology. Further, in April 2019, the European Union High Level Expert Group on Artificial Intelligence presented the [Ethics Guidelines for Trustworthy Artificial Intelligence](#). This states that machine learning models should be lawful, ethical and robust. This seems likely to be an area in which regulation will continue to evolve and develop.

Insurance, an industry based on risk profiling, must also guard against risks of bias in the data, whether in relation to age, demographic factors, or even some random factors where there may be a chance correlation to risk but no rational explanation, or causation – such as drivers called 'David' being more risky than those named 'Peter'.



¹ Data Never Sleeps 7.0. DOMO, Inc. July 2019. <https://www.domo.com/news/press/data-never-sleeps-7>

² Mulesoft: Consumer Connectivity Insights 2018.

³ McKinsey: <https://www.mckinsey.com/featured-insights/artificial-intelligence/tackling-bias-in-artificial-intelligence-and-in-humans>

⁴ ibid.

BIG DATA CHALLENGES



In 2014 the Information Commissioner's Office ("ICO") produced a guidance note on Big Data, recognising the challenges that such technologies present to data protection compliance, nevertheless stating that there was no exception to data protection compliance, and organisations would have to deploy such technologies within the boundaries placed in data protection law.

Rhiannon Webster is head of information law at DAC Beachcroft.

[She was the legal expert on the ICO and Turin Institute's citizens jury, looking at explaining AI decisions.](#)

Nearly 6 years on, we have a new data protection law and the big data guidance has been updated to also cover the challenges faced in the fields of artificial intelligence and machine learning.

Meanwhile many insurance firms are immersed in data analytics within data lakes and moving towards machine learning and artificial intelligence to predict propensity to claim and pricing models. However, the essence of the challenges and indeed the compliance message from the ICO remains the same. Such automated and large-scale processing of data, if it involves personal data, can be hard to reconcile with the data protection principles.

NEVERTHELESS, COMPLIANCE MUST BE ACHIEVED. THE PARTICULAR CHALLENGES ARE:

- Any repurposing of data (i.e. collecting it for one purpose and then using it for another purpose) needs to comply with the purpose limitation principle. Often organisations have little idea of the power of the data they collect, when it is collected, but then have a team of data scientists who recognise its potential and wish to harness it, long after the opportunity to inform individuals of the uses of their data has passed.
- Organisations require ever larger datasets in order to train artificial intelligence, and to create meaningful response. This needs to be balanced against an organisation's obligation under the GDPR to only process personal data which is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation).
- Meeting the transparency requirement of the GDPR, in that organisations need to explain the processing of personal data that will occur. It is anticipated that, as machine learning and AI get more sophisticated, it

will not be possible to explain the decisions that are being made in automated form. This is a topic explored by the ICO and Turin institute through its project ExplAI and resultant guidance on explaining AI.

LEGAL POINT

A key focus area for the ICO, in February, the ICO launched its consultation on a self-auditing framework for organisations' use of AI, which forms a useful checklist for anyone in the insurance market looking at AI and machine learning solutions, to ensure that data protection compliance is considered at the outset. Although currently in consultation form, those in the insurance sector dipping their toes into the world of AI would be advised to review this guidance. It contains advice on how to understand data protection law in relation to artificial intelligence (AI) and recommendations for organisational and technical measures to mitigate the risks AI poses to individuals.

Aimed at both technology specialists developing AI systems and risk specialists whose organisations use AI systems, this guidance is designed to assess the risks to rights and freedoms that AI can cause; and the appropriate measures you can implement to mitigate them.

AUTHOR:
RHIANNON WEBSTER,
HEAD OF INFORMATION LAW,
DAC BEACHCROFT



PREPARING FOR A DRIVERLESS FUTURE?

AUTHOR:
PETER ALLCHORNE,
PARTNER, DAC BEACHCROFT LLP



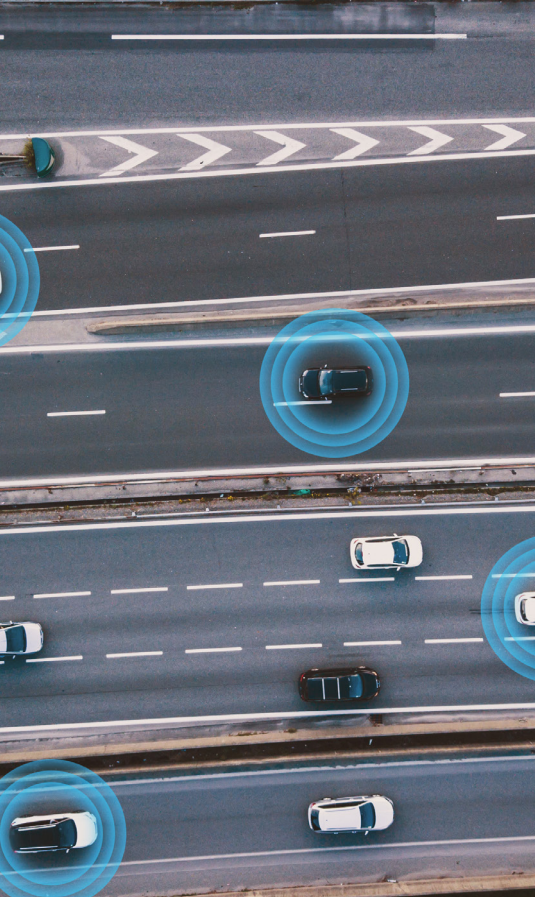
Peter Allchorne is a DAC Beachcroft Partner and a member of the firm's Connected and Autonomous Vehicles team.

Here he asks leading transport planning consultant, Martin Wedderburn, for his views on the AV development roadmap amid a global pandemic.

The journey to vehicle automation is well under way, but there is much more to be done to enable the safe deployment of driverless cars. Technology continues to outpace regulation; issues of data sharing and cyber security remain unresolved for example.

While the UK's current network infrastructure is not yet capable of sustaining connected and automated vehicles on a mass scale, it is widely anticipated that the Covid-19 crisis will act as a catalyst for change, accelerating the pace of digitisation across the world. But what does this mean for the connected and automated vehicle development agenda?





I asked Martin Wedderburn to give us his opinion on the subject.

A RAPIDLY CHANGING POLICY AND REGULATORY ENVIRONMENT

The competition is tough and all major car manufacturing nations are seeking to create the conditions to attract investment. One way to get ahead in the global race is to create an appropriate regulatory and insurance framework that allows vehicles with increasing levels of automation to be tested and gradually released to market.

While the push for autonomous vehicles is largely driven by industrial strategy, the transport planning profession is slowly coming to terms with the potential pros and cons of a world of autonomous mobility. Both the Department for Transport and Transport for London have formulated policy in terms of 'guiding principles' to steer the deployment of Connected and Automated Vehicles (CAVs). From a policymaker's perspective, CAVs present the opportunity to significantly reduce road danger and provide accessible transport for all groups in society. Yet they also pose risks if they discourage people from walking, thus reducing everyday physical activity, and increasing the number of vehicles on the road.

We have all witnessed the global impact of the movement started by a Swedish teenager calling for action on climate change. The wider public policy landscape in the UK has shifted dramatically with numerous organisations declaring a climate emergency. Looking forward, there is now increasing political pressure for

more fundamental changes to transport policy. Previously marginalised debates about reforms to land use planning, the creation of powerful devolved transport authorities, and even replacing fuel duty with national road pricing are increasingly becoming mainstream. Autonomous vehicles may yet emerge into a different world of mobility than we know today.

WILL CONSUMERS ACCEPT THE TECHNOLOGY? AND WHAT MODEL WILL THEY ADOPT?

Much of the hype around CAVs and their benefits is being generated by the industry promoting them, and there remain very real questions about the extent to which consumers want or will accept the technology.

Consumers will likely also have a choice of how to use autonomous vehicles. Industry analysts distinguish between the ownership model of Car-as-a-Product (CaaP) and the automated robo-taxi model of Car-as-a-Service (CaaS). There is some debate about whether older generations will still feel more comfortable with the vehicle ownership model. But younger generations who never experienced CDs, encyclopaedia or photo albums appear more inclined to see mobility as a digital service. But ultimately both models may co-exist.

DRIVERLESS FREIGHT

Businesses are already trialling CAVs in many stages of the supply chain, from connected lorries on motorways to neighbourhood takeaway delivery pods.

In recent times as supermarket shelves were laid bare, the media spotlight shone briefly on our Just-in-Time supply chains. Working to keep stock to a minimum and to meet ever decreasing delivery windows, our supply chains are driven by increasing automation through the entire production and distribution process. Driverless freight can be seen as just one step in this trend towards greater automation, where CAVs would function in the road network like in one huge automated distribution centre.

PROPERTY DEVELOPMENT: BUILDING IN FLEXIBILITY

The million dollar question being asked by property developers is about the volume of parking required in the future, and building in a degree of flexibility to future parking will be crucial.

A recent Centre for London report on designing for new urban mobility in residential developments explored practical ways to future-proof sites for alternative scenarios. Basement parking areas are easier to convert to other uses if they have light wells, an open structure and slightly higher ceilings. Surface parking and multi-storey structures can be positioned and designed to retain future development potential as stand-alone sites.

This material is provided by Martin Wedderburn. He manages a specialist transport planning consultancy offering strategic advice, research, and forecasting/appraisal studies. He has wide-ranging experience in transport planning, policy and analysis, and has worked for a wide range of public, private and third sector clients around the world.

With UK car manufacturing facing numerous challenges, developing a world-leading R&D capability in vehicle automation technologies is recognised as one crucially important factor in retaining jobs and investment in the UK.

CYBER AND THE LEGAL LANDSCAPE

Cyber attacks are increasing in both complexity and frequency, with almost half of businesses (46%) suffering a cyber security breach or attack over the last twelve months.¹

Rapid digitalisation of businesses coupled with organisations holding significant amounts of sensitive data has led opportunistic cyber criminals to steal information. Regulation is therefore continually evolving in order to keep pace with new and emerging cyber and data security threats.

CYBER AND COVID-19

Fears around the potential for cyber security incidents intensified during the Covid-19 (coronavirus) pandemic as many businesses were required to rapidly adopt widescale remote working for their employees. Companies were suddenly faced with balancing a need to keep their workforce online while ensuring systems and networks remained secure, particularly where personal, non-corporate devices were used. Video conferencing apps such as 'Zoom' experienced a steep increase in usage during lockdown and consequently became a target for hackers. In response, the National Security Cyber Centre issued [guidance for individuals and organisations](#), warning of cyber criminals exploiting the pandemic for commercial gain through activities such as social engineering methods and phishing emails.

DIRECTORS' RESPONSIBILITIES

While the pandemic shone a further spotlight on cyber security, company directors had already been reminded of their data security duties during the implementation of the General Data Protection Regulation (GDPR) in May 2018. Sitting alongside the UK's Data Protection Act, GDPR placed ultimate responsibility upon directors and officers for GDPR compliance, leading many to review their cyber security measures and consider the benefits of D&O insurance.

CODE OF PRACTICE FOR CONSUMER IOT SECURITY

In October 2018 the Government published a [Code of Practice for Consumer Internet of Things \(IoT\) Security](#) aimed at updating laws relating to the manufacture and sale of consumer smart devices in the UK. With predictions of 75 billion internet-connected devices worldwide by 2025², it's recognised that compromised IoT devices could present a significant threat, especially when connected to other appliances. The new law is designed to ensure such devices are built to communicate securely and that personal data is protected. It's possible insurers will need to design new products and services for the IoT industry in line with this new legislation.

AUTHOR:
CHRISTIAN SIMPSON, SENIOR CYBER
UNDERWRITER, ALLIANZ



INSURERS AND CYBER

Of course, insurance companies are themselves not immune from cyber attacks. Cyber criminals know that insurers hold vast amounts of data and personal information on policyholders and this information can be extremely lucrative. However, financial and insurance businesses are also more likely to have some sort of insurance cover against a breach and to monitor potential supplier risks.³

SUMMARY

Cyber remains a relatively new risk and so regulation is still largely playing 'catch-up'. As the landscape evolves, insurers and brokers must keep abreast of such regulation to support their role in designing suitable insurance solutions and also in their capacity as risk management advisors.

¹ Cyber Security Breaches Survey 2020: Department for Digital, Culture, Media & Sport. Available at: <https://www.gov.uk/government/publications/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020>

² Statista. Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025. <https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/>

³ Cyber Security Breaches Survey 2020, Department for Digital, Culture, Media & Sport. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/875573/Main_report_-_Cyber_Security_Breaches_Survey_2020.pdf

5G AND CONNECTED CARS

5G will fundamentally change the world we live in. Boasting record speeds, increased capacity and improved network efficiency, 5G is the new generation of wireless technology.



5G is set to enable smart cities and pave the way for connected cars. Transport networks and other public bodies could use it to improve public services, such as parking and street lighting. In the insurance space, companies could even use the technology for loss adjusters to tour damaged property and inspect vehicles remotely, capitalising on better quality video feeds.²

CONNECTED CARS

Although autonomous cars are still a little way off, connected cars are very much in the present. The newest models are becoming sensor laden IoT devices. 5G will allow for a more flexible network that can support vehicle capabilities which have previously been impractical.³

The 5G in Automotive and Smart Transportation Report, produced by ABI research⁴ predicts that globally, there will be 41 million 5G connected cars on the road by 2030, rising to 83 million by 2035. It also claims that by using 5G in vehicles, fuel consumption can be reduced by one third. This could help the country's ambition to reduce emissions to zero by 2050.

5G will give rise to greater opportunities to collect data from the vehicle, such as vehicle location, driver behaviours, engine diagnostics and weather

conditions – all directly from the vehicle. In-vehicle infotainment will also be a possibility, particularly if the vehicle is fully automated.

We should find that roads become safer due to real-time alerts on driving hazards and road conditions, such as closures, up ahead. Smart motorways will potentially be able to work alongside connected vehicles to improve the flow of information to the driver. The sharing of sensor data between vehicles and the highway infrastructure of the future will likely help to create a safer driving environment for all road users. Analytics company Gartner forecasts that by 2023, the automotive industry will be the largest market opportunity for 5G IoT solutions.⁵ When you combine this with data analytics, machine learning and artificial intelligence – this brings many opportunities for mobility in the near and distant future.

IOT AND SECURITY

With the increased amount of data and third parties involved in IoT devices, 5G poses an elevated security threat. This is partly because there are more ways through which vehicles can be attacked. It's likely to bring some challenges with regard to protecting customer data and privacy. Constantly connected IoT technology,

such as cars connecting to the cloud, will transmit large volumes of data – a temptation for cyber criminals. Examples of such exposure already exist, for example when ethical hackers managed to exploit a vulnerability in the in-car web browser and take control of the infotainment system.⁶

In October 2018, the Code of Practice for Consumer Internet of Things (IoT) Security was published by the Government. The aim is to ensure IoT devices are built to operate securely and that data is protected. Security doesn't fundamentally change with 5G, however, the breadth and depth of it does and connected cars and other IoT devices will push its boundaries.

¹ Ericsson mobility report – <https://www.ericsson.com/en/press-releases/2/2018/11/5g-estimated-to-reach-1.5-billion-subscriptions-in-2024--ericsson-mobility-report>

² AT&T WHITEPAPER https://www.business.att.com/content/dam/attbusiness/reports/5G_for_Business.pdf

³ <https://www.intel.co.uk/content/www/uk/en/communications/5g-connected-vehicle.html>

⁴ https://www.abiresearch.com/market-research/product/1033746-5g-in-automotive-and-smart-transportation/?utm_source=media&utm_medium=email

⁵ <https://www.gartner.com/en/newsroom/press-releases/2019-10-17-gartner-predicts-outdoor-surveillance-cameras-will-be>

⁶ McKinsey - <https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/the-race-for-cybersecurity-protecting-the-connected-car-in-the-era-of-new-regulation>



AUTHOR:
GERRY ROSS, HEAD OF
COMMERCIAL MOTOR, ALLIANZ

BIBA GUIDES

**Here are just some of BIBA's guides,
provided in association with DAC
Beachcroft LLP and Allianz:**

- Sustainability
- BIBA Broker Legal Round-Up
- Claims Inflation Trends
- Employers' Liability Insurance
- Business Interruption Insurance
- Security Measures In Today's World
- The Future of Motor Insurance

Member Helpline:
Tel: **0344 7700266**
enquiries@biba.org.uk
www.biba.org.uk

**British Insurance
Brokers' Association**
8th Floor, John Stow House
18 Bevis Marks, London EC3A 7JB

Allianz Insurance plc
57 Ladymead, Guildford
Surrey GU1 1DB

DAC Beachcroft LLP
25 Walbrook,
London EC4N 8AF

Produced by **SandisonPay**
01329 835135
www.sandisonpay.co.uk

The information in this guide is of a general nature and is not intended to address the circumstances of any particular individual or entity. BIBA, Allianz and/or DAC Beachcroft cannot accept any responsibility for any loss occasioned to any person or entity as a result of action or refraining from action as a result of any item herein.

Allianz Insurance plc (registered in England number 84638) is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority. Financial Services Register number 121849.