

# ICOQ

IRISH COMPLIANCE QUARTERLY

SPRING 2021

DLA PIPER  
GDPR  
DATA BREACH  
SURVEY  
REPORT

COMPLIANCE  
AND THE  
COVID-19  
PANDEMIC

Niall Gallagher  
Scholarship Essay

ETHICAL  
CULTURE

FINANCIAL  
CRIME

5<sup>TH</sup> MONEY  
LAUNDERING  
DIRECTIVE

DATA  
PROTECTION

## Interview With A DPO

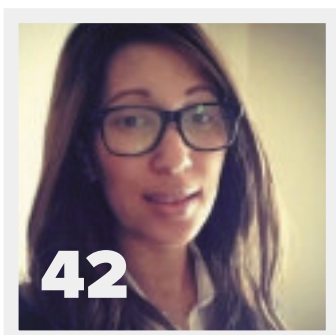
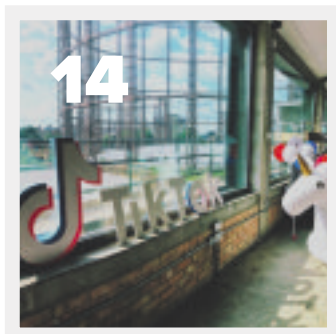
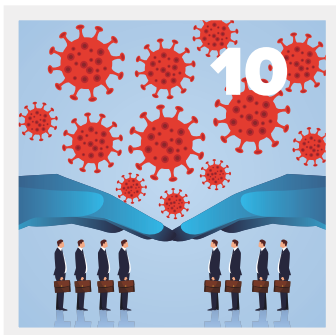
Caroline Goulding  
TikTok

PLUS

ACOI Members' Survey **EVENTS**

ACOI IN THE MEDIA Education Update: Fintech





# CONTENTS

- 02 Contents**

---

- 03 CEO Update:** Michael Kavanagh, Chief Executive, ACOI

---

- 04 President’s Page:** ACOI President, Kathy Jacobs, discusses the compliance issues and topics currently affecting ACOI Members

---

- 06 ACOI in the Media**

---

- 08 ACOI Members’ Survey Results**

---

- 10 Niall Gallagher Scholarship Essay:** Compliance and the COVID-19 Pandemic

---

- 14 DP&IS Working Group:** Interview with a DPO. Caroline Goulding, TikTok

---

- 18 GDPR Data Breach Survey Report:** DLA Piper

---

- 22 Funds Working Group:** CP86 Fund Management Company Guidance & Effectiveness

---

- 26 Financial Crime Compliance Working Group:** 5th Money Laundering Directive

---

- 30 Ethics Committee:** Ethical Culture

---

- 34 Talking Point:** Fintech

---

- 36 Education:** New ACOI Education Programmes

---

- 38 Recruitment:** Robert Walters Recruitment Survey Results

---

- 40 Events**

---

- 42 Member Profile:** Claudette Whyte

---

**ICQ MAGAZINE IS PUBLISHED BY:**

The Association of Compliance Officers in Ireland (ACOI),  
5 Fitzwilliam Square, Dublin 2.

Tel: **+353 778 0200** | Email: [info@acoi.ie](mailto:info@acoi.ie) | [www.acoi.ie](http://www.acoi.ie)

*Production Team:* ACOI Executive.

*Editorial and Production:* Intrepid Media Ltd.

The information contained in these articles should not

be taken as a definitive statement of the law or guidance in relation to the issue of overseas transfers. Appropriate advice should be sought in relation to specific cases. The views and opinions expressed in ICQ are not necessarily those of the ACOI. Copyright of content, except where noted otherwise, is vested in the ACOI.



# CEO UPDATE



Welcome to the Spring edition of the **ICQ** Magazine.

If anything, recent events have demonstrated the importance of your profession and the vital role you play within your organisation. The news that the Central Bank of Ireland has fined J&E Davy €4.1million clearly demonstrates the importance of the compliance function within a financial services organisation and also the massive reputational consequences that result from circumventing or disregarding that compliance function, as appears to have been the case with Davy. Situations such as this reinforce the absolute necessity to involve qualified compliance professionals in any decision-making process such as that that arose in this instance and at an early stage in any scenarios where a conflict of interest may occur. A company's compliance function is there to help to safeguard consumers, clients, employees and the organisation itself. However, it can only discharge its role effectively when it is fully informed and has access to all relevant information. The resignations that have happened so far, the €4.1m CBI fine, the adverse publicity and massive reputational damage to the organisation serve to illustrate the true cost of non-compliance.

## In the News

It was another remarkable quarter from an ACOI profile building perspective. As well as being asked for and having our views published in national media with regards the Davy regulatory matter, we appeared in over 30 articles in a two-month period. I, myself, also did four interviews on regional radio. This demonstrates that the

**“SITUATIONS SUCH AS THIS REINFORCE THE ABSOLUTE NECESSITY TO INVOLVE QUALIFIED COMPLIANCE PROFESSIONALS IN ANY DECISION-MAKING PROCESS SUCH AS AROSE IN THIS INSTANCE AND AT AN EARLY STAGE.”**

demand is there for the voice of compliance to be heard and also the importance of the member surveys that we issue. A summary of the coverage received can be found in various sections of our website and further examples are on page 6.

## Podcasts

We are delighted with the successful launch of our podcast series - The Compliance Files. The podcast series features a broad range of compliance topics and valuable insights from regulators. The feedback so far has been fantastic. There have been over 2,000 downloads of our first four episodes with many more to follow. Keep an eye on our website and social media channels for details of each episode.

## Education

Our new educational offering – the Professional Certificate in Fintech Risk & Compliance – successfully launched in March and is up and running. I am also delighted that our new educational offering – the Professional Certificate in Anti-Money Laundering in a Fintech Environment is scheduled to commence on Wednesday 14th April. ACOI and Professional Accountancy Training (PAT)

have collaborated to provide members of the ACOI with the skills and competencies that supports a culture of AML compliance in this new environment. Further information can be found on page 37.

## AGM and Election to Council

The ACOI AGM took place in January, virtually for the first time and we welcome Claudette Whyte to Council who was elected on the day. An interview with Claudette can be found on page 42.

## Annual Conference 2021

We can confirm that the 2021 Annual Conference will take place on 18th November so please save the date. We look forward to sending you more detailed information about the conference in due course.

## Concluding Remarks

The current vaccine roll-out is welcome but it is clear there are significant challenges ahead. ACOI will continue to provide an extensive schedule of virtual webinars, CPD events and podcasts along with access to accredited educational opportunities for members. **ICQ**

**Michael Kavanagh, CEO.**

# WELCOME TO THE SPRING 2021 EDITION OF THE ICQ



## Dear Member,

You are very welcome to the Spring edition of our **ICQ** magazine.

We are now thankfully well into 'grand stretch' territory and also the milestone of a year of lockdown this past week and the first public holiday of the year, and these markers are hopefully bringing us closer to resuming normal life.

We have seen significant developments ourselves at the ACOI these past weeks which has seen the work and preparation of many months coming to fruition. It has been nerve wracking and exciting at the same time.

The first major deliverable which we have seen come together after a year of work is the Professional Certificate in Fintech Risk and Compliance. We were fortunate to source an excellent partner Professional Accountancy Training (PAT), who shared our vision of delivering a qualification by practitioners for practitioners in this important new field. It was extremely important to get

the syllabus right and it took a number of iterations and fine-tuning to ensure we got the content mix right. The programme will be delivered through a blend of modes including live online tutorials and workshops, prerecorded lectures and demonstrations, directed e-learning content and supported learning materials. There are other innovations such as classroom 'kahoot' - which I have yet to see in practice.

The first introductory evening was held on Tuesday 2nd February and the classes will be weekly until the end of April and the first examination will be on the 1st May. Of course, all will be delivered online due to the continuing restrictions however our partners, PAT are experts in this mode of delivery and not just because of the pandemic - they had pioneered the delivery of online professional training and professional examinations prior to the pandemic.

We have also partnered with PAT to bring the Professional Certificate in AML in a Fintech Environment. This course is designed to provide professionals, practitioners and other stakeholders with the skills and competencies that supports a culture of AML compliance. In the context of the technologically



driven innovation in Financial Services, the course addresses AML requirements from the perspective of a variety of sectors – for example: Credit and Financial Institutions, and Designated Non-Financial Business and Professions (DNFBP's). The course identifies the core requirements and contemporary (technologically enhanced) best practice in the risk assessment, client onboarding, and life cycle management of client accounts from the perspective of both the financial institutions and professional service providers for example: accountants and auditors.

These are really exciting ventures for the ACOI, given the importance of this emerging industry potentially for Ireland's post COVID-19 recovery and the future of financial services in general. I was privileged to be at the introductory meeting to talk to our first cohort of students. I mentioned that I sincerely wished to be among them as I would like to take the course at some point when my schedule allows. It really is a must for anyone who wishes to work in this industry.

The other development in ACOI has been the launch of our podcast series, 'The Compliance Files'. This again is something that took many months to plan and work to deliver. It is a testament to how the last year has brought huge strides and the technologies that connect us and help us communicate with each other, that we have been able to launch this at all during a lockdown. I had bought a couple of books to read up on how to put together a podcast, all written pre pandemic. All of them talked about the need for recording a podcast and a studio with the correct sound equipment. This is obviously impossible during the last year. We were however able to purchase recording technology that enables us to record the podcast remotely almost as if it were a Zoom or Teams call. At the time of writing, we have published our Launch Podcast, with Seána Cunningham about the Central Bank of Ireland priorities for 2021 and we discussed a number of other important topics such as the agenda of the AML and Enforcement Division which Seána leads. Our next podcast was one on the Fintech industry when I was joined by Joe Beashel, Partner in Matheson when Joe talked about the issues facing Fintechs in getting authorized in Ireland, post-authorisation challenges, the importance of the industry to Ireland, and a post-Brexit perspective on the future of the industry in Ireland. I was lucky enough to sit down with three leading female regulators, Mary-Elizabeth McMunn, Director of Credit Institutions Supervision at the Central Bank of Ireland, Jennifer Dolan, Assistant Commissioner for Children's Policy at the Data Protection Commission and Senator Fiona O'Loughlin to talk about their careers, the risks they have taken and the experiences and challenges that

**“ WE HAVE SEEN SIGNIFICANT DEVELOPMENTS OURSELVES AT THE ACOI THESE PAST WEEKS WHICH HAS SEEN THE WORK AND PREPARATION OF MANY MONTHS COMING TO FRUITION.”**



have shaped them into the leaders they are today. A must-listen for everyone starting out in their career – and those at the top of the profession, and beyond compliance too. Also published is a discussion with MB Donnelly, Assistant Commissioner at the Data Protection Commission, Head of Communications, Regulatory Strategy EU Projects and DPO Networks about the highlights of the recently published Annual Report. She gave us a peak behind the scenes as to what it is like to put together the Report as well as the highlights. We have some more currently being edited and will be released over the coming weeks about various compliance topics.

Our vision was that these podcasts will provide an alternative means of connecting with members – especially at this time, and will be informative, and delivered in an accessible format – and I do hope that ACOI members and listeners beyond enjoy the podcasts and find them useful.

That wraps up a very busy Spring for us. Enjoy the lengthening days and the upcoming Easter holidays, and hopefully we are closer to meeting again,

Yours in Compliance,

**Kathy Jacobs, March 2021. ICQ**

# ACOI IN THE MEDIA

The first quarter of 2021 was a busy one for the ACOI and we are delighted to have received extensive media coverage since the start of the year. During this time, the ACOI featured prominently in national and regional media including the Irish Independent, The Examiner, Business World, The Echo, TechCentral, The Business Post and several radio stations as well.

A survey conducted by the ACOI in conjunction with its Data Protection and Information Security working group sought members views regarding Ireland's data protection landscape in 2021. Respondents cited uncertainty as a result of Brexit (32%); an increase in remote working (26%) and the impact of the Schrems II ruling (23%) as the primary drivers behind heightened threats to data protection and mounting challenges for organisations with regard to ensuring compliance.

The ACOI also received more publicity following the release of findings from a survey of over 250 organisations regarding some of the challenges they are facing in 2021. The findings

showed that generating new business is the chief concern for 60% of organisations ahead of managing a remote workforce (30%), while more organisations now believe that Covid-19 is likely to have a bigger impact than Brexit on their success in 2021.

Notwithstanding these challenges, the ACOI sounded a note of cautious optimism within the financial services sector, where almost three quarters of businesses surveyed by the ACOI anticipate job creation this year. ACOI Chief Executive, Michael Kavanagh, commented on the findings, "Amongst the slew of fairly bleak news at the moment, these results shine some positive light on the prospects for Ireland's financial services sector. We were greatly encouraged to find that positive sentiment towards recruitment has improved again since September, when we last put this question to our members, with 10% more respondents believing that the sector would recruit this year up from 64% to 74%.

**Details of all ACOI media coverage can be found on [acoi.ie](http://acoi.ie). ICQ**

Select an area to comment on

**RTE**  
Most financial services firms expect jobs growth, ACOI survey reveals



The survey of 250 organisations, answered by ACOI members with responsibility for compliance in financial organisations throughout the country, revealed that as much as 74% of businesses in the sector will see notable recruitment.

**The Business Post**  
Corporate Governance COMPANY LAW & COMPANY SECRETARIES

Good governance saves companies from

Conflicts of interest and non-compliance can come with a high cost for organisations in any industry, writes **Lorraine Cleary**



The discussion around conflicts of interest in Ireland is the subject of a new book by Lorraine Cleary, a former senior compliance officer and current director of the Institute of Directors. The book, 'Conflicts of Interest: A Practical Guide for Directors', is available on Amazon and is a must-read for all directors. The book provides a clear and concise guide to the rules and regulations surrounding conflicts of interest, and is written in a style that is easy to read and understand. It is a valuable resource for all directors, and is highly recommended.

**BUSINESS WORLD**  
74% OF FINANCIAL SERVICES FIRMS EXPECT RECRUITMENT IN SECTOR IN 2021



A new survey from the Association of Compliance Officers of Ireland (ACOI) finds that 74% of financial services firms expect recruitment in sector in 2021 and 70% say pay and/or benefit cuts are not on the cards.

The survey of 250 organisations – answered by ACOI members with responsibility for compliance in financial organisations throughout the country, sought to gain an insight into the outlook for the sector as it moves further into 2021.

**Echo.ie**  
Your Local Newspaper

74% of financial services firms expect create new jobs in 2021

**Cyber attack top concern for business**


After a poll by the Association of Compliance Officers, spokesman Michael Keating said: "It's apparent remote working is a major issue facing firms this year when it comes to data protection, with 34% of businesses voicing their concerns around the risks associated with it."



Survey of 250 organisations – answered by ACOI members with responsibility for compliance in financial organisations throughout the country, to gain an insight into the outlook for the sector as it moves further into 2021 revealed that as much as 74% of businesses believe the sector will see notable recruitment - up from 64% when the same survey was undertaken by the ACOI in September 2020. 70% say they are not expecting to see cuts to pay and/or benefits in their firms this year – a marked improvement on the 51% who felt the same in September of last year.

**Independent.ie**

Finding new business the biggest concern for firms



This is according to a survey of more than 250 businesses from the Association of Compliance Officers of Ireland (ACOI).

When ACOI carried out the same survey last June, 39pc of firms cited generating new business as their biggest worry, while one in four were concerned about managing working from home.



IRISH TECH NEWS

**REMOTE WORKING AND CYBER ATTACKS ARE BIGGEST DATA PROTECTION THREATS FACING 65% OF IRISH ORGANISATIONS IN 2021**



Remote working and the threat of cyber-attacks are the number one data protection concern for 65% of Irish companies in 2021. This is according to a new survey from the Association of Compliance Officers Ireland (ACO I) which sought to understand the current data protection risks facing companies – 85% of whom have more than 75% of their workforce currently working from home.

**BUSINESS WORLD**  
**IRISH BUSINESSES SAY COVID A BIGGER THREAT THAN BREXIT**



These are some of the headline findings of a new survey from the Association of Compliance Officers of Ireland (ACO I). The survey of more than 250 organisations, answered by ACO I members with responsibility for compliance in financial organisations throughout the country, sought to gain insight into attitudes

around the challenges coming down the line in 2021, and whether they have changed significantly since respondents were last asked the same questions over 6 months ago.

**EchoLIVE.ie**  
**Uncertainty across businesses around data protection**



76% of businesses have experienced growing uncertainty across the data protection spectrum over the last 12 months with no signs of this abating. This is according to a new survey from the Association of Compliance Officers Ireland (ACO I) released for World Data Protection Day.

**TechCentral.ie**  
**Majority of Irish businesses unsure of data protection landscape**

27 January 2021 | 0 More than three-quarters (76%) of Irish businesses have experienced growing uncertainty across the data protection spectrum over the last 12 months with no signs of this abating according to a new survey from the Association of Compliance Officers Ireland (ACO I).

**Irish Examiner**  
**Survey finds cash flow is not a concern for most businesses**



More than 250 financial organisations throughout the country, to the survey from the Association of Compliance Officers of Ireland (ACO I), to gain insight into the challenges.

**siliconrepublic**  
**Data protection landscape more uncertain than last year, survey finds**

Surveying 250 organisations across the country, the Association of Compliance Officers in Ireland (ACO I) found that 76pc of Irish businesses believe the data protection landscape is more uncertain now than it was 12 months ago.

**TECH**  
**90% of businesses say cyberattack risk has increased due to home working**

This is according to a new survey from the Association of Compliance Officers Ireland (ACO I) which sought to understand the current data protection risks facing companies – 85% of whom have more than 75% of their workforce currently working from home.



**Independent.ie**  
**Further action in Davy scandal unlikely Central Bank**



The Association of Compliance Officers in Ireland issued a statement casting Davy's problems as a cautionary tale for financial firms that bypass compliance processes.

**TechCentral.ie**  
**Remote working, cyber attacks | data protection threats facing Irish organisations**



The survey of more than 250 organisations, answered by ACO I in responsibility for compliance in financial organisations throughout the country, has left employers feeling increasingly vulnerable to data protection

**Irish Examiner**  
**Remote working makes firms feel more vulnerable to data breaches**

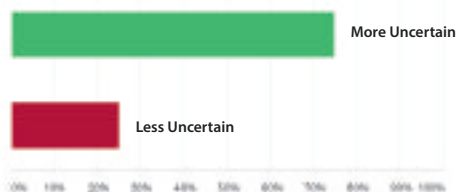


Remote working has left employers feeling increasingly vulnerable to data protection breaches and cyber-attacks, according to a new survey from the Association of Compliance Officers Ireland (ACO I).

# ACOI MEMBER SURVEY DATA PROTECTION IN 2021

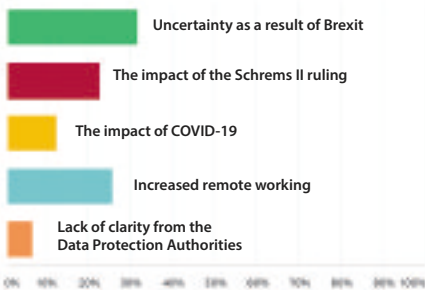


**Q1** Is the data protection landscape in 2021 more or less uncertain than in 2020?



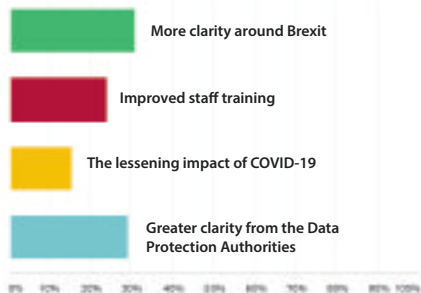
More Uncertain	189	75%
Less Uncertain	63	25%

**Q2** If it is more uncertain, what do you believe is the main reason for this?



Uncertainty as a result of Brexit	74	32%
The impact of the Schrems II ruling	53	23%
The impact of COVID-19	29	13%
Increased remote working	60	26%
Lack of clarity from the Data Protection Authorities regarding GDPR compliance requirements	16	7%

**Q3** If it is less uncertain, what do you believe is the main reason for this?



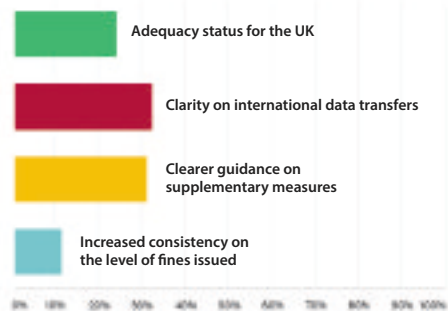
More clarity around Brexit	55	31%
Improved staff training	43	24%
The lessening impact of COVID-19	28	16%
Greater clarity from the Data Protection Authorities regarding GDPR compliance requirements	52	29%

**Q4** What, do you believe, is the number one data protection risk for your company in 2021?



Brexit	19	8%
Remote working	85	34%
Cyber attacks	79	31%
The volume of staff training needed	21	8%
New rules around international data transfers – Schrems II	32	13%
Anti-Money Laundering and Counter Financing of Terrorism obligations	16	6%

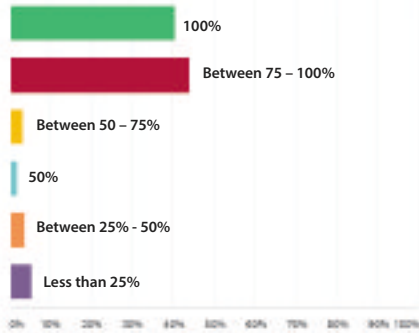
**Q5** What one data protection / compliance outcome or solution would be most beneficial for your company in 2021?



Adequacy status for the UK	61	25%
Clarity on international data transfers	81	33%
Clearer guidance on the supplementary measures required for standard contractual clauses	78	31%
Increased consistency on the level of fines issued for data protection or compliance breaches	29	12%

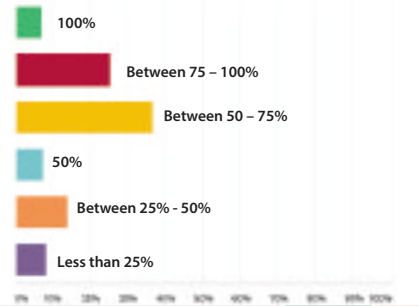


**Q6** Approximately what percentage of your organisation's staff are now working remotely?



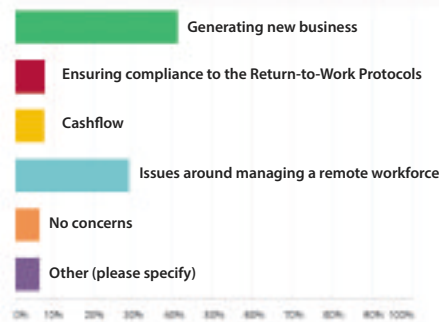
100%	101	41%
Between 75 - 100%	110	44%
Between 50 - 75%	9	4%
50%	5	2%
Between 25% - 50%	10	4%
Less than 25%	14	6%

**Q7** Approximately what percentage of your organisation's staff are likely to be partially or fully working remotely in 12 months?



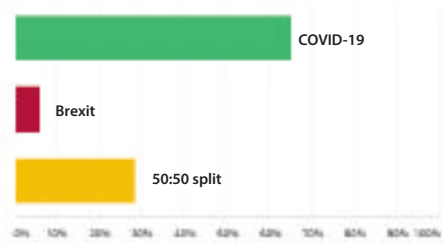
100%	18	7%
Between 75 - 100%	62	25%
Between 50 - 75%	90	37%
50%	19	8%
Between 25% - 50%	35	14%
Less than 25%	21	9%

**Q8** What is the biggest concern for your organisation for the year ahead?



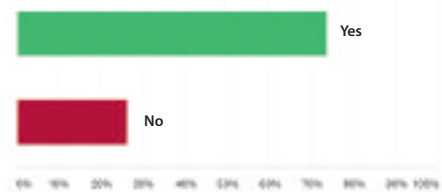
Generating new business	104	41%
Ensuring compliance to the Return-to-Work Protocols	20	8%
Cashflow	20	8%
Issues around managing a remote workforce	73	29%
No concerns	17	7%
Other (please specify)	17	7%

**Q9** What do you think is likely to have a bigger impact on your employer's business in 2021?



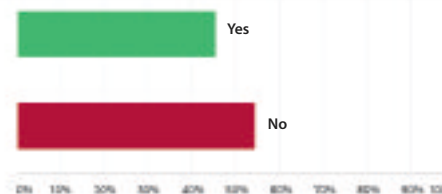
COVID-19	164	65%
Brexit	15	6%
50:50 split	72	29%

**Q10** Do you believe firms in your sector will recruit in 2021?



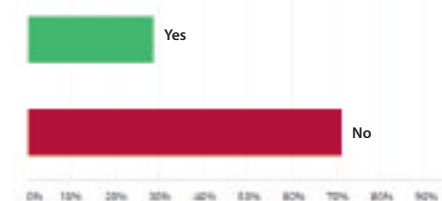
Yes	186	74%
No	66	26%

**Q11** Do you believe firms in your sector will have to make redundancies in 2021?



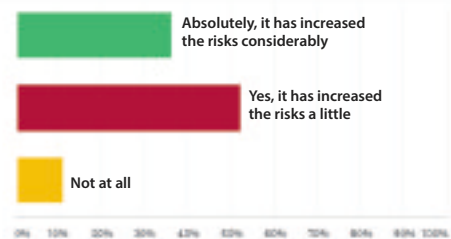
Yes	115	46%
No	137	54%

**Q12** Do you expect pay cuts and/or other cuts in benefits to be implemented in your business in 2021?



Yes	72	29%
No	178	71%

**Q13** Has financial crime and the risk of attack become a greater consideration since some of your workforce have been redeployed to work at home.

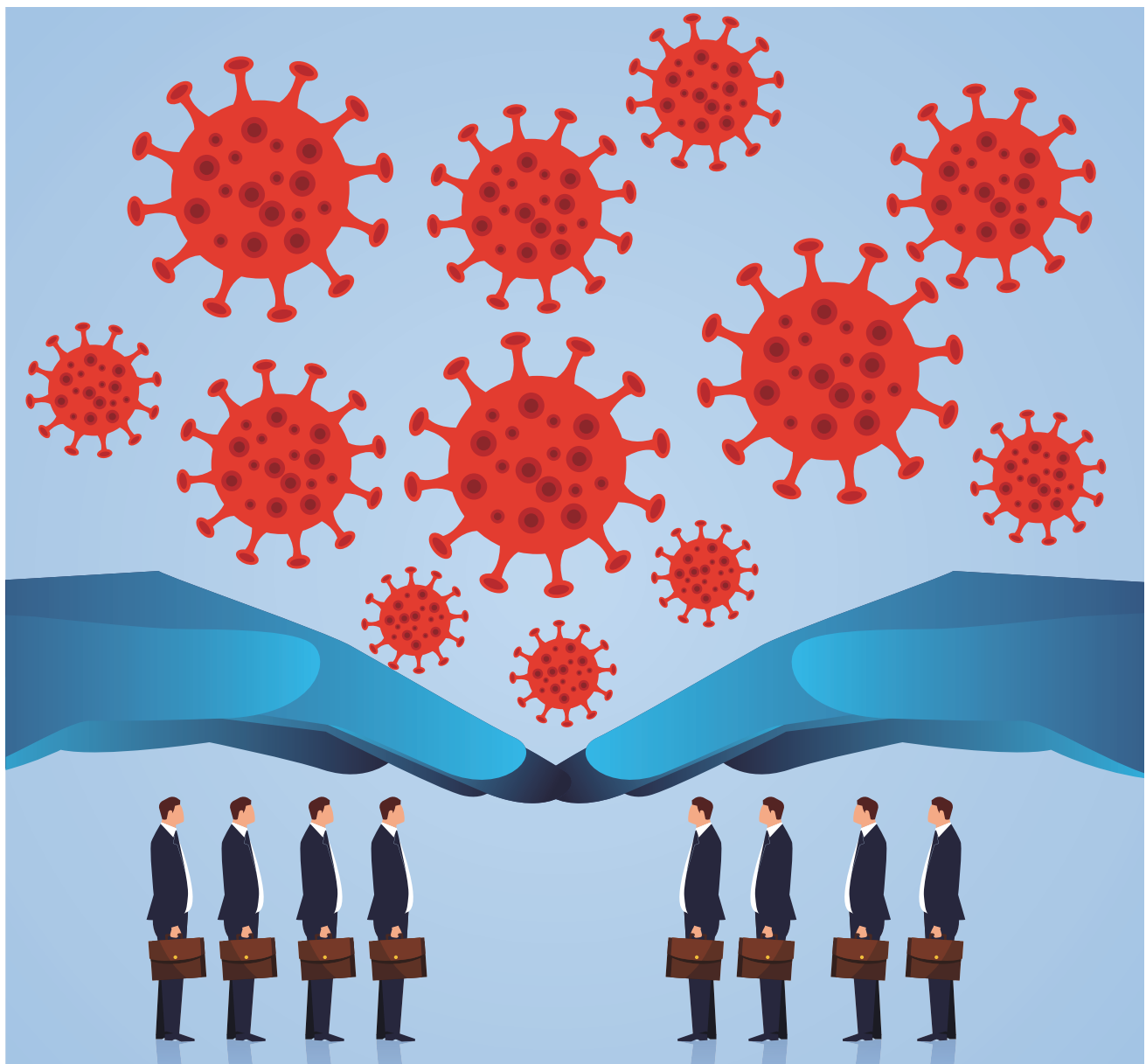


Absolutely, it has increased the risks considerably	91	36%
Yes, it has increased the risks a little	131	52%
Not at all	28	11%

# Compliance & the COVID-19 Pandemic

The compliance professional's role in promoting a consumer-focused culture and protecting the firm in these difficult times.

**AUTHOR:** Michael Siwiec, 1<sup>st</sup> place winner of the Niall Gallagher Professional Diploma in Compliance Scholarship.



**T**hese two aspects of the compliance professional's role in the times of the COVID-19 pandemic, i.e. 1) promoting a consumer-focused culture, and 2) protecting the firm, are inextricably linked, and therefore will be analysed jointly, with differences highlighted if required.

While it is commonly understood in the three lines of the defence model that compliance staff manage compliance risk, but strictly speaking this is not correct. The sole and primary responsibility for management of compliance risk (or any other risk) rests with the first line of defence (and ultimately the board of the company). Compliance officers do not create risk – they do not approve card or loan applications, mis-sell products, process payments, make decisions about debt collections or switching clients away from tracker mortgages to boost company profits. Compliance risk arises in the front line and in a healthy organisation, must be managed in the front line. The existence of the compliance function cannot be an excuse for abdicating the responsibility for risk management. The compliance team's role is to challenge and enable the first line to manage the compliance risk and to provide assurance on the design and effectiveness of the compliance risk management.

If the compliance risk management framework (and programme) is adequately designed, the emergence of COVID-19 should have triggered only changes to individual compliance programme elements, but should not have caused any major changes of the programme itself (that would mean the programme was inadequate). It is best to follow the principle of managing the risk in the best of times, to stand tall in the worst of times (Greener, 2020), i.e. be always ready.

**“IT IS BEST TO FOLLOW THE PRINCIPLE OF MANAGING THE RISK IN THE BEST OF TIMES, TO STAND TALL IN THE WORST OF TIMES (GREENER, 2020), I.E. BE ALWAYS READY.”**

Depending on the scale and complexity of the organisation, it should have the following elements in its compliance programme (names may vary): policies, procedures, training, risk assessment (annual), targeted risk assessments (audits), risk reporting, training, risk appetite statement, risk appetite metrics, risk appetite metrics reporting, risk appetite breach escalation, issue identification and reporting, regulatory inventory, regulatory change management, compliance related loss reporting, external compliance loss/fines monitoring, training, monitoring, testing and surveillance.

While no major changes are required to the overall compliance programme, the COVID-19 pandemic requires adjustments or a fresh approach to some elements of the programme, to address the need for wellbeing of customers and employees, as well as respond to changes in work practices, e.g. the move to work from home posture or the more pervasive use of remote technology, and the additional risks which these entail. What follows are insights and recommendations for compliance professionals during the current pandemic on how to protect the clients and the firm, categorised under broad headings: Compliance Programme, Empathy, Conduct, Connection, and Question & Challenge.

## Compliance Programme Elements

The compliance professional should review the risk appetite asking the question if it is

still adequate. From this, a re-assessment of risks should follow, to understand if the risk profile changed, especially in areas such as customer protection, information security, privacy, or fraud. Compliance teams should also check for any new or revised regulatory guidance, such as the Central Bank of Ireland's new rules relating to consumer credit payment breaks or the Central Credit Register (CBI, 2020). This may require performing additional scenario analysis to understand or quantify the impacts of the changed risk profile. After evaluation of the risk re-assessment results, the compliance team may decide to enhance monitoring and reporting of compliance risk (e.g. in relation to personal loan payment breaks, or postponing, in line with the CBI guidance, of recording of credit payment delays in the Central Credit Register) to verify that a consumer-focused approach is in place. Also, the increased use of technology in the pandemic may boost the use of the technology for compliance purposes (for risk identification or subsequent compliance monitoring and testing – say hello to artificial intelligence and robotics).

## Empathy

The COVID-19 pandemic caused significant hardship to many groups in society. However, the concept 'we are all in this together' contributed to strengthening of a trend where focus shifts from shareholders to a governance model where the 'health and resilience of the company' is paramount (Paine, 2020). More broadly, this relates to

putting people first and looking after both customers and associates. Customers are humans with feelings, and the corporate machine has the potential to hurt individuals, as we know from the tracker mortgage scandal (CBI, 2019). The role of the compliance professional is to be vigilant and to promote (through training, as well as targeted assessments, monitoring and testing) the right behaviours within the firm to ensure that the company has a customer focused culture. This will not only prevent the firm from being featured on front pages of newspapers (in a negative light) but will mitigate the risk of regulatory fines (thus protecting the bottom line). Regulators increasingly take a hard line against systemic risk management breakdowns (including in compliance risk management), such as the substantial recent fine from the Central Bank of Ireland levied at Bank of Montreal Ireland for breaches of banking licence conditions (CBI, 2019).

## Conduct

Working with regulations, not against them (Thorne, 2020) is vitally important, and this attitude must come down from the very top – the whole board and the executive management must have the right compliance risk mindset. Compliance function needs to assess that the right risk mindset permeates from every corner of the organisation (this applies to all risks). Associates in a company with high conduct standards will do the right thing when nobody is watching (Geffroy, 2019). Such constantly reinforced message (from the Board, executives and the compliance function) about the commitment to uphold high standards in compliance risk management will make people think twice before committing a compliance breach. The role of the compliance professional is to keep reinforcing this message (unfortunately 'ad nauseam') until it sinks in – Brian Moynihan, the CEO

of Bank of America, once said that he repeats his messages (including in relation to risk management) until staff feel tired of hearing it, at which point he knows the message got through (Moynihan, 2019). Investing in risk management pays – by avoiding regulatory fines, such as the recent Citibank fine from the US Comptroller of the Currency for risk management (including compliance risk) deficiencies (OCC, 2020).

## Connection

The pandemic caused a change in work posture (work from home). This brings certain challenges. Compliance team members need to stay connected with the rest of their team to be able to continue to adequately evaluate the risks. Compliance should also stay connected (or even increase interactions) with the first line to avoid the situation of being side-lined. Employee engagement is an important parameter to gauge the level of satisfaction and motivation of staff (lack of which typically results in lowering of the compliance standards). In addition, the business should communicate with both associates and clients to reduce their uncertainty (Cleaveland, et al., 2020). The compliance team's role is to re-assess and communicate those risks, but also to assess the design and operating effectiveness of controls to mitigate those risks (through e.g. targeted risk assessments, but also through compliance monitoring and testing, to ensure that clients and staff are kept in the loop).

## Question & Challenge

Because of the prevalent work from home posture, increased risk of internal and external fraud, and new regulatory guidance issued, compliance officers should be vigilant through the application of intellectual curiosity (Gallinek, 2019) to detect non-compliant practices or increased compliance risk. While being

mindful of the negatively changed circumstances of clients and associates as a result of the pandemic, compliance staff should maintain dispassionate objectivity (Greener, 2019), so that their judgment is not compromised. Compliance officers should also strive to avoid the 'function trap' (Kaplan & Mikes, 2020) – everybody is responsible for risk management (first line primarily) and the silo-mentality must be avoided (to prevent compliance breaches). This links to the previous paragraphs as well - compliance officers have to talk to the business (connection) and prevent things falling through the cracks due to a fragmented approach (conduct), as well as educate the first line about those risks and have adequate compliance monitoring routines in place to establish adherence to ensure that clients' and firm's interests are protected.

## Conclusion

The compliance professional's role in promoting a consumer-focused culture and protecting the firm in the context of the COVID-19 pandemic will look different in each firm. A robust compliance risk management programme is essential and this would typically already be in place in a healthy organisation, but the elements of the compliance programme may still require re-assessment or re-focusing. Numerous practical steps, based on the author's experience, were proposed in this essay under several broader headings: Compliance Programme, Empathy, Conduct, Connection, and Question & Challenge, with the caveat that the existence of the compliance function cannot guarantee compliance, but it is a necessary condition for the organisation to thrive, while also looking after its clients and employees. **ICQ**



## REFERENCES

CBI, 2019. Central Bank of Ireland: Enforcement Action: Bank of Montreal Ireland plc. reprimanded and fined €1,246,189 by the Central Bank of Ireland for breach of banking licence condition. [Online] Available at: <https://www.centralbank.ie/news-media/press-releases/enforcement-action-bank-of-montreal-ireland-plc.-reprimanded-and-fined-1-246-189-by-the-central-bank-of-ireland-for-breach-of-banking-licence-condition> [Accessed 14 October 2020].

CBI, 2019. Central Bank of Ireland: Tracker Mortgage Examination. [Online] Available at: <https://www.centralbank.ie/consumer-hub/tracker-mortgage-examination> [Accessed 15 October 2020].

CBI, 2020. Central Bank of Ireland: Consumer Hub: COVID-19 (Coronavirus). [Online] Available at: <https://www.centralbank.ie/consumer-hub/covid-19> [Accessed 12 October 2020].

Cleveland, A., Cussins Newman, J. & Weber, S., 2020. The Art of Communicating Risk. [Online] Available at: <https://hbr.org/2020/09/the-art-of-communicating-risk> [Accessed 18 October 2020].

Gallinek, E., 2019. Bank of America Employee Townhall. s.l.:s.n.

Geffroy, O., 2019. Bank of America Employee Townhall. s.l.:s.n.

Greener, G., 2019. Bank of America Employee Townhall. s.l.:s.n.

Greener, G., 2020. Bank of America Employee Townhall. s.l.:s.n.

Kaplan, R. S. & Mikes, A., 2020. Managing Risks: A New Framework. [Online] Available at: <https://hbr.org/2012/06/managing-risks-a-new-framework> [Accessed 11 October 2020].

Moynihan, B., 2019. Bank of America Employee Townhall. s.l.:s.n.

OCC, 2020. OCC Assesses \$400 Million Civil Money Penalty Against Citibank. [Online]

Available at: <https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-132.html> [Accessed 17 October 2020].

Paine, L. S., 2020. Covid-19 Is Rewriting the Rules of Corporate Governance. [Online] Available at: <https://hbr.org/2020/10/covid-19-is-rewriting-the-rules-of-corporate-governance> [Accessed 10 October 2020].

Thorne, R., 2020. Bank of America Employee Townhall. s.l.:s.n.

# Interview With A DPO

## Caroline Goulding, TikTok



**Caroline Goulding, Director and Data Protection Officer at TikTok** talks communication, upskilling and the importance of integrity.



### **Q** What are the biggest challenges for DPOs in 2021?

**A** We're living through an unprecedented time that, among everything else, has surfaced new data protection challenges. As the pandemic rumbles on, implementing appropriate protocols, which includes safeguarding workforce health related data will continue to feature as a priority for DPOs, particularly if we see a major return to offices.

Then of course we have the ongoing challenge of data transfers discussed below. And for some DPOs, coming to grips with emerging technologies such as AI will be high on their agendas.

### **Q** Is the outlook for DPOs in 2021 more or less uncertain than last year?

**A** Technology changes rapidly, so a degree of adjustment will always be part of a DPO's job. However, right now the current landscape has never been more certain for DPOs. Driven in part by higher privacy expectations from the general public, we are seeing and can expect: greater levels of enforcement, additional



**“ THE MODERN DPO NEEDS A VARIETY OF SKILLS. FIRST AND FOREMOST IS INTEGRITY, AS THE DPO IS IN A POSITION OF TRUST WITH ACCESS TO CONFIDENTIAL AND SENSITIVE INFORMATION.”**



guidance from regulators; more engagement and attention from senior business leaders than ever before; all of which is taking place in an increasingly globalised data protection environment.

**Q How do you think the role has changed in recent years?**

**A** Since GDPR and the increase of data protection awareness among business hierarchies, the job has shifted from its legalistic focus on compliance, to a more strategic and cross-functional role. Data protection is no longer a niche issue devolved to IT and Legal departments - it now cuts across all departments and you'd struggle to find a serious executive who didn't acknowledge its importance in terms of reputation, customer journey and business performance.

**Q What skills should a successful DPO possess?**

**A** The modern DPO needs a variety of skills. First and foremost is integrity, as the DPO is in a position of trust with access to confidential and sensitive information. Second comes diplomacy, as we tend to have numerous stakeholders across an organisation; being able to understand and balance their competing needs and priorities is key.

Also DPOs need a certain degree of humility. The challenges we face are complicated and ever-evolving. It's important to acknowledge when you need a second opinion in order to be in an even better position to advise the business.

**Q What advice would you give to a DPO starting out in their career?**

**A** Learn from those that came before you - taking on the role in 2021 is quite different to those who

were contemplating becoming DPOs in 2017 during the pre-GDPR readiness era. Nurture relationships with DPOs from a variety of sectors who can act as a sounding board.

Develop your soft skills especially communication, influencing and people management. These skills are equally as important to the modern DPO as knowledge about privacy, security and compliance. Lastly, expect the unexpected...It's a career with lots of interesting challenges to overcome. Our profession has changed rapidly and so have the problems we need to solve. This is why it's important to stay humble to new ways of doing things.

**Q Have you found any qualifications particularly beneficial to your role?**

**A** Qualifications certainly play a role and there are some useful ones





out there to get you up to speed. However, the key is to stay curious during your career and take every opportunity to keep learning, which has never been easier with conferences and webinars going virtual. Things change quickly so you need to stay on top of what's happening in data protection right now - rather than rely on what you learnt in years past.

**Q In your opinion, will Brexit or Schrems II have more impact on Irish companies' data protection activities?**

**A** Now that the European Commission has issued a draft adequacy decision, essentially accepting that the UK data protection regime affords adequate protections for EU data subjects, there may have been a collective sigh of relief among certain companies. While an EDPB opinion is yet to issue

and the draft decision will need the green light from representatives of the EU Member States, it provides some assurance about the continuing free flow of data between the EU and UK.

Nevertheless the implications of Schrems II endure. How that impacts Irish companies depends on how they are structured and the extent of their international footprint. The true impact of Schrems will become clearer when the EDPB release their final recommendations. This is one we'll all be watching closely.

**Q Do you think the Schrems II decision will result in fewer companies using Standard Contractual Clauses or seeking alternative options?**

**A** It's difficult to say...when you consider what are the viable alternatives?

Companies generally appear to be considering all options and willing to actively engage while also seeking confidence in a measure that will have a certain degree of longevity. Recent comments of the judge rapporteur of the CJEU who was involved in the Schrems II case and the final paragraph of that judgment itself suggests that Article 49 derogations may have a broader role to play. Finally, US-EU engagement on data sharing arrangements at a political level is crucial and will influence the next stage of developments.

**Q What does an effective data protection culture look like within an organisation?**

**A** A strong data protection culture is one in which employees connect privacy risks to their own roles and personal lives. They understand how to operationalise data protection policies





**“CONSISTENCY IS CRITICAL WHEN IT COMES TO DATA PROTECTION, SO MAKE SURE YOU’RE REGULARLY REMINDING YOUR COLLEAGUES ABOUT ITS IMPORTANCE.”**



and adhere to the organisation’s security measures. If things go wrong - and they will in every business from time to time - they know how and when to surface potential issues.

It also means support from the top. At TikTok, it’s something our senior leaders take very seriously. One such recent example, when my proposal to convert Data Protection Day into a month long internal Privacy Awareness Month was fully supported and encouraged.

### **Q How can DPOs create greater awareness of data protection within their business?**

**A** Consistency is critical when it comes to data protection, so make sure you’re regularly reminding your colleagues about its importance. Traditional methods really do work - breaking down the message into bite size

chunks and infographics via different company channels - IM, resource hubs, newsletters - and securing speaking slots in company wide or department level meetings to explain key processes, new developments and remind everyone of best practice. Executive video testimonials can also be powerful.

Get creative. At TikTok, we regularly use the platform to explain important issues to both our community and our colleagues. For example, we launched an educational video series - ‘You’re in Control’ - using top creators to present TikTok’s safety and privacy controls in an accessible and engaging fashion. The videos can also be accessed directly in-app @TikTokTips.

### **Q Does remote working make the job of DPO more challenging?**

**A** Fundamentally yes. It’s much

harder to build trust and maintain relationships across the company, especially with those from different departments, without the organic discussions that can happen in person and which are often crucial for DPOs to leverage for insights. It takes a deliberate effort to prioritise scheduling virtual coffees.

### **Q If you had one data protection wish for 2021, what would it be?**

**A** An ever greater expansion of two crucial concepts enshrined in GDPR; data protection by design and by default, which not only benefits society as a whole at a macro level, it also makes the job of a DPO much easier when data privacy features and data privacy enhancing technologies are embedded directly into the design of projects at an early stage. **ICQ**

# DLA Piper GDPR Fines and Data Breach Survey: 2021

**T**he EU General Data Protection Regulation (GDPR) has applied across the European Union since 25 May 2018. In what was an extraordinary year for many reasons, Europe's data protection supervisory authorities and those they regulate have been grappling with the tough requirements imposed by GDPR and the legal questions it leaves unanswered.

**“REGULATORS HAVE BEEN TESTING THEIR NEW POWERS THIS YEAR, ISSUING EURO158.5M (USD193.4M / GBP142.7M)<sup>4</sup> IN FINES SINCE 28 JANUARY 2020. BUT THEY HAVEN'T HAD IT ALL THEIR OWN WAY, WITH SOME NOTABLE SUCCESSFUL APPEALS AND LARGE REDUCTIONS IN PROPOSED FINES.”**



With thanks to the many different contributors<sup>1</sup> and supervisory authorities who make this report possible, our third annual survey covers key GDPR

metrics across the European Economic Area (EEA)<sup>2</sup> and the UK<sup>3</sup> since GDPR first applied and for the year to 27 January 2021.

<sup>1</sup> This publication has been prepared by DLA Piper. We are grateful to Batliner Wanger Batliner Attorneys at Law Ltd., Glinska & Miskovic, Kamburov & Partners, Kyriakides Georgopoulos, LOGOS, Mamo TCV Advocates, Pamboridis LLC, Schellenberg Wittmer Ltd and Sorainen for their contributions in relation to Liechtenstein, Croatia, Bulgaria, Greece, Iceland, Malta, Cyprus, Switzerland, Estonia, Latvia and Lithuania respectively.

<sup>2</sup> The EEA includes all 27 EU Member States plus Norway, Iceland and Liechtenstein.

<sup>3</sup> The UK left the EU on 31 January 2020. The UK has implemented GDPR into law in each of the jurisdictions in the UK (England, Northern Ireland, Scotland and Wales), which as at the date of this report is the same in all material respects as GDPR.

<sup>4</sup> In this report we have used the following exchange rates: EUR1 = GBP0.9 / USD1.22.

## SUMMARY AND KEY FINDINGS

### Significant increase of breach notifications

It has been more than two and half years since GDPR first applied on 25 May 2018. For the period from 28 January 2020 to 27 January 2021 there were, on average, 331 breach notifications per day (a 19% increase on the previous year average of 278 notifications per day), so the current trend for breach notifications continues to see double digit growth.

### Testing new powers and successful appeals

The supervisory authorities responsible for enforcing GDPR<sup>5</sup> have not been idle; some notable fines have been imposed relating to a wide variety of infringements. The UK left the EU on 31 January 2020. The UK's supervisory authority, the Information Commissioner's Office (ICO), has, however, been active, issuing several large fines.

Regulators have been testing their new powers this year,

issuing a total of EUR158.5m (USD193.4m / GBP142.7m)<sup>6</sup> in fines since 28 January 2020. But they haven't had it all their own way, with some notable successful appeals and large reductions in proposed fines.

The Austrian supervisory authority had a bad end to the year when its headline EUR18m (USD22m / GBP16.2m) fine imposed on Austrian Post was overturned by the Austrian Federal Court on 2 December 2020. Similarly, the two fines issued by the ICO in the UK were reduced from the originally proposed GBP189.39m (EUR210.4m / USD256.7m) and GBP99.3m (EUR110.3m / USD134.6m) to GBP20m (EUR22.2m / USD27.1m) and GBP18.4m (EUR20.4m / USD24.9m) respectively.

In percentage terms, the reductions secured were 90% and 80% of the originally proposed fines. The ICO noted in its final penalty notices that the originally proposed fines had been discounted in part in light of the financial hardship caused by COVID-19.

Nevertheless, it evidently pays to appeal and to mount robust challenges to proposed regulatory sanctions.

### Highest individual fine league table

**#1** France's data protection supervisory authority, the CNIL, retains pole position, having fined Google Inc EUR50m (USD61m / GBP45m) in January 2019 for breaching GDPR transparency requirements, and for failing to have an adequate legal basis for processing in relation to personalised advertising (breach of Articles 6, 12 and 13 GDPR).<sup>7</sup>

**#2** The Hamburg data protection supervisory authority is in second place, having fined a global retailer EUR35.26m (USD43m / GBP31.7m) in October 2020 for failing to have a sufficient legal basis for processing (breach of Articles 5 and 6 GDPR).

**#3** In third place, Italy's data protection supervisory authority, the Garante, fined a telecommunications operator EUR27.8m (USD33.9m / GBP25m) in January 2020 for a number of breaches of GDPR, including breaches relating to transparency obligations, failing to have a sufficient legal basis for processing personal data, and inadequate technical and organisational measures, and breach of the principle of privacy by design (breach of Articles 5, 6, 17, 21 and 32 GDPR).

<sup>5</sup> All references in this report to infringements or breaches of GDPR are to findings made by relevant data protection supervisory authorities when issuing fines. In a number of cases, the entity subject to the fine has disputed these findings and the penalty notices are subject to appeal. DLA Piper makes no representation as to the validity or accuracy of the findings made by relevant supervisory authorities.

<sup>6</sup> Not all supervisory authorities publish details of fines. Some treat them as confidential. Our report is, therefore, based on fines that have been publicly reported or disclosed by the relevant supervisory authority. It is possible that other fines have been issued on a confidential basis.

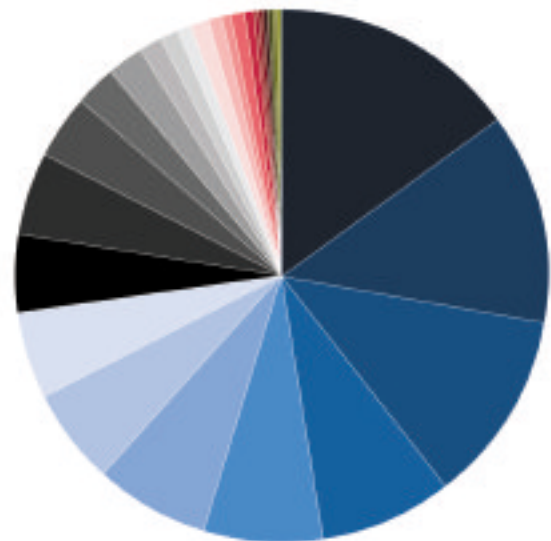
<sup>7</sup> The CNIL was in the news again in December 2020, having imposed another fine on Google entities for a total of EUR100m. However, these fines related to alleged violations of e-privacy laws rather than GDPR infringements, so are not included in the metrics in this report.



DLA PIPER GDPR FINES AND DATA BREACH SURVEY: 2021

Per capita country ranking of breach notifications\*  
 Number of data breaches per 100,000 people for the period 25 May 2018 to 27 January 2021  
 Change compared to last year's ranking

Per capita country ranking of breach notifications*	Number of data breaches per 100,000 people for the period 25 May 2018 to 27 January 2021	Change compared to last year's ranking
Denmark	155.6	+3
Netherlands	150	-1
Ireland	127.8	+1
Slovenia	80	+3
Finland	71.8	No change
Iceland	69.1	-2
Luxembourg	59.6	-1
Liechtenstein	51	+1
Germany	50	+2
Sweden	48.1	-2
Norway	37.9	-1
Malta	23.8	No change
Poland	22.6	+1
United Kingdom	12.7	-1
Estonia	11.2	+1
Austria	9.8	-1
Belgium	9.8	No change
Hungary	8.5	+1
Cyprus	7.3	+1
Lithuania	7	+1
Latvia	5.4	-3
Spain	3.2	+2
Czech Republic	2.9	-1
France	2.8	-1
Croatia	2.7	Information not publicly available
Italy	2.5	-1
Greece	1.3	No change



\*Per capita values were calculated by dividing the number of data breaches reported by the total population of the relevant country multiplied by 100,000. This analysis is based on census data reported in the CIA World Factbook (July 2020 estimates).

In the rankings of the total value of all GDPR fines issued to date, the data protection supervisory authority in Italy tops the table, having imposed fines totalling EUR69,328,716 (USD84,581,033 / GBP62,395,844). The data protection authorities in Germany and France are in second and third place with fines totalling EUR69,085,000 (USD84,283,700 / GBP62,176,500) and EUR54,436,000 (USD66,411,920 / GBP48,992,400) respectively.

### Total amount of fines

Last year, the total (reported) fines for the full 20-month period since the introduction of GDPR on 25 May 2018 was just over EUR114m (USD139m / GBP103m), which we had noted in our previous report was quite low, given that supervisory authorities enjoy the power to fine organisations up to 4% of their total worldwide annual turnover for the preceding financial year. The total (reported) fines since 25 May 2018 has more than doubled to just over EUR272m (USD332m / GBP245m), with EUR158.5m (USD193.4m / GBP142.7m) over the last 12 months alone, a 39% increase on the previous 20-month period since GDPR came into force.

### Many open legal questions

There are many open legal questions relating to GDPR, including whether fines should be assessed against the consolidated global revenue of the organisation being fined, or just against the revenue of the specific legal entity responsible for the infringement.

The clear intent of the non-legally binding recitals in GDPR supports the former broad interpretation, which is also supported by the influential European Data Protection Board.<sup>8</sup> However, the legally binding articles of GDPR conflict with the recitals and appear to limit the assessment of fines to the revenues of the specific entity being fined. This is a critical point of interpretation, as it potentially significantly limits the maximum fine that regulators can impose under GDPR.

It is also open to interpretation whether fines for breach of Article 5(1)(f) and Article 32 (the integrity and confidentiality principle and the related requirement to ensure the security of processing personal data) should be capped at 2% or 4% of total worldwide annual turnover. Having considered this issue when imposing two headline-grabbing fines last year, the UK ICO concluded in its penalty notices that the higher 4% maximum fine applied to breaches of security. That said, this is far from being settled law, and we expect the point to be argued in future appeals of fines, given the significant amounts involved.

The many open legal questions and uncertainties in the interpretation and application of GDPR perhaps explain, in part, why the fines imposed to date by supervisory authorities have been at the lower end of the scale of potential maximum fines.

As was the case in last year's report, fines certainly aren't the only exposure for organisations that fall short of

**“THE MANY OPEN LEGAL QUESTIONS AND UNCERTAINTIES IN THE INTERPRETATION AND APPLICATION OF GDPR PERHAPS EXPLAIN, IN PART, WHY THE FINES IMPOSED TO DATE BY SUPERVISORY AUTHORITIES HAVE BEEN AT THE LOWER END OF THE SCALE OF POTENTIAL MAXIMUM FINES.”**

GDPR's exacting requirements. The continuing fallout of the Schrems II<sup>9</sup> judgment, handed down in July 2020 by Europe's highest court, is a reminder of the broad range of other sanctions supervisory authorities can impose. Maximilian Schrems has, through his organisation *My Privacy is None of Your Business*, issued 101 complaints to lead supervisory authorities.<sup>10</sup> These complaints demand, in addition to fines, the immediate suspension of alleged illegal transfers of personal data from the EU to third countries. There is also an increased risk of "follow-on" compensation claims, including US-style "opt-out" class action in a number of EU Member States and the UK, fuelled by billions of euros invested in litigation funds looking for claims to support. **ICQ**

<sup>8</sup> *The European Data Protection Board is made up of representatives from all 27 EU Member States and the European Data Protection Supervisory Authority. The supervisory authorities of the EFTA EEA States are also members with regard to the GDPR-related matters (without the right to vote or be elected as chair or deputy chairs).*

<sup>9</sup> *Data Protection Commissioner v Facebook Ireland Limited, Maximilian Schrems (Case C-311/18).*

<sup>10</sup> See <https://noyb.eu/en/101-complaints-eu-us-transfers-filed>

# CP86 Fund Management Company Guidance & Effectiveness

**AUTHOR:** **Laura Wadding,**  
**Partner, Risk Advisory,**  
**Deloitte LLP**

Ireland has a long and well-established reputation as a fund-friendly domicile. Its pragmatic regulatory environment benefits from the passports available under the UCITS Directive and AIFMD. These frameworks allow funds to be sold and marketed into the EU and beyond under various regulatory regimes, while the portfolio management can be performed outside of Ireland in jurisdictions such as the UK, US and Asia.

The introduction of AIFMD in July 2013 started a process of change in relation to managing the business affairs of the funds under management. Unlike the UCITS regime, which is largely a product directive but also enshrines principles around the management of UCITS, AIFMD focuses on the regulation and ongoing supervision of the Alternative Investment Fund Manager (AIFM).

Although AIFMD permits both an internally managed Alternative Investment Fund (AIF) structure, as well as the appointment of an external AIFM, the rules around governance, supervision and the extent to which an AIFM can delegate duties were far more prescriptive than the UCITS regime. This made the concept of an internally managed AIF (similar to the SMIC model under the UCITS regime) far more challenging.

Furthermore, Article 82(1)(d) of the Level 2 AIFM Directive sets out in significant detail the rules around delegation and includes both quantitative and qualitative criteria around what can be delegated and what can be retained. Article 82(2) also provides that the EU Commission may review AIFMD delegation models to ensure that the AIFM does not become a 'letter-box entity'. Article 82(3) further provides that

the European Securities and Markets Authority (ESMA) may issue guidelines to ensure a consistent assessment of delegation structures across the EU. This prompted the CBI to consider the effectiveness of the delegation structures by Irish management companies.

The first consultation on fund management company effectiveness in Ireland, CP86, was published in July 2014. The resulting feedback was accompanied by a mini consultation in 2015 and it was then decided to use CP86 in relation to the third consultation in June 2016. The Central Bank published its Guidance in December 2016, concluding a three-part CP86 consultation process. Existing FMCs were expected to comply with the relevant provisions introduced under CP86 by 1 July 2018. At that point, the Central Bank signalled to industry that it would carry out a body

“THE FIRST CONSULTATION ON FUND MANAGEMENT COMPANY EFFECTIVENESS IN IRELAND, CP86, WAS PUBLISHED IN JULY 2014.”

of work to assess implementation of the requirements and the Guidance by FMCs.

Other jurisdictions followed suit, mostly notably Luxembourg produced CSSF Circular 698 in 2018 which include much of the same principles as CP86.

CP86 has remained on the CBI's agenda since finalised in 2016. The CBI has maintained its focus on fund governance and has raised the bar with regard to substance and governance, most notably for new applicants setting up an Irish fund management company as a result of Brexit. In 2019, the CBI began a thematic review of the implementation of CP86. This concluded in 2020 and resulted in a “Dear Chair” letter, dated 20 October 2020. The Central Bank expects all FMCs to critically assess their day to day operational, resourcing and governance arrangements against

all relevant rules and guidance. The analysis should be completed and an action plan discussed and approved by the Board by the end of Q1 2021.

### Overview of the Fund Management Company Guidance

The objective of CP86 was to introduce initiatives “designed to underpin the achievement of substantive control by FMCs, acting on behalf of funds, over the activities of their delegates.” The guidance applies to UCITS management companies (“ManCos”), authorised Alternative Investment Fund Managers (“AIFMs”), self-managed UCITS and internally managed Alternative Investment Funds (“AIFs”) that are authorised as AIFMs.

It provides guidance on seven key areas:

1. **The Rationale for Board Composition**
2. **Directors’ Time Commitments**

3. **Organisational Effectiveness**
4. **Six Managerial Functions**
5. **Delegate Oversight**
6. **Operational Issues**
7. **Procedural Matters**

### Dear Chair Letter

In 2019, the CBI began a thematic review of the implementation of CP86 when it wrote to over 300 Irish management companies (ManCos) and self-managed investment companies (SMICs) asking questions of their governance structures, level of delegate oversight, detailed analysis of director time commitments, and how organisational effectiveness was being achieved. After this industry-wide outreach, the CBI began a series of desktop reviews of a sample of FMCs in late 2019. This concluded in 2020 and resulted in a “Dear Chair” letter, dated 20 October 2020. In this letter, the CBI highlighted



“THE PLAN NEEDS TO BE FORWARD LOOKING TO TAKE INTO ACCOUNT PLANS FOR GROWTH OR INCREASED COMPLEXITY IN THE PRODUCT RANGE OF THE FMC.”

concerns and recommendations in relation to the following areas:

### 1. Resourcing

- All FMCs should have a minimum of 3 FTE (suitably qualified and senior) or more depending on the nature, scale and complexity of operations.
- FMCs must appoint locally based persons to act as Designated Persons (DPs) and sufficient staff to fulfil duties including oversight of delegated activity.
- In larger firms DPs are expected to be full time roles.
- All but the smallest FMCs should have a CEO.
- Resourcing to be kept under review as business scale and complexity increases.

### 2. Designated Persons

- Evidence of constructive challenge and interrogation by DPs as an indicator of good management.
- DPs to commit enough time to carry out their role thoroughly and to a high standard.

### 3. Delegate Oversight

- Due diligence reviews to be conducted at take on and then annually. If relying on a delegates Policy and Procedure there must be a formal process to review same.
- Documented SLA to be in place in respect of third party arrangements.

### 4. Risk Management Framework

- Robust, Board approved, entity specific RMF (incl. Risk Register and Risk Appetite Statement).

### 5. Board approval of new funds

- Evidence of robust discussion and challenge by the Board. Early involvement when formulating strategy of new funds.

### 6. The role of the Organisational Effectiveness Director

- To fulfil role in monitoring adequacy of resourcing must have meaningful, regular and documented interaction with DPs and Board at least on quarterly basis.

- Report to Board at least annually.
- Ensure Board effectiveness evaluation conducted annually.
- Consider conflicts of interest and personal transactions on an ongoing basis and report to the Board.
- Consider tenure of INEDs & rotation.
- Consider gender diversity.

## Risk Mitigation Programmes

In addition to the *Dear Chair letter*, some firms received direct instruction from the CBI in the form of a Risk Mitigation Programme ('RMP') and these included specific requirements for action by those entities. In general, these RMPs are consistent with the recommendations outlined by the CBI in the letter, however, some specific requirements have been imposed on firms to undertake certain activities within an agreed timeframe such the following:

- Complete a board effectiveness review
- Complete an organisational effectiveness review





- Review the designated persons time commitments
- Enhance the risk management framework
- Develop a risk appetite framework and corresponding risk appetite statements

## Preparing a Board Approved Plan

Regardless of whether an FMC receives a specific risk mitigation requirement or not, the Central Bank expects all FMCs to critically assess their day to day operational, resourcing and governance arrangements against all relevant rules and guidance.

## The Assessment and Implementation Plan should at a minimum consider the following:

- The time commitment, skills and expertise of available resources;
- The FMC's retained and delegated tasks, including how ongoing independent challenge of all

- delegates can be ensured;
- The tasks required by the framework, including those that must be completed on a fund by fund basis;
- How resources and operational capacity will need to increase to take account of any increase in the nature, scale and complexity of the funds under management since authorisation or the last time the FMC critically assessed its operations;
- How resources and operational capacity will need to increase to deal with a market and/or operational crisis.

The analysis should be completed and an action plan discussed and **approved by the Board by end Q1 2021.**

The plan needs to be forward looking to take into account plans for growth or increased complexity in the product range of the FMC. Latest indications from the CBI suggest that plans should not run into 2022, which could be a challenge for many firms, especially if the action required includes applying

for an extended or additional licence e.g. where a SMIC intends to establish a Management Company into which it will put the required substance.

The plan itself does not need to be submitted to the CBI, but indications are that the CBI will perform a round of inspections in 2022 which will test the robustness of those plans and the manner in which they have been implemented. So the plan needs to be reasonably detailed, with clear rationale for decisions made, and a clear roadmap for its implementation. It should be accompanied by a risk and issues tracker, with due consideration being given to how to mitigate those risks. In addition to approving the plan, the Board should be kept abreast of its progress on a regular basis. Where an FMC develops a plan for its longer term strategy that flows into 2022, it may need to consider some tactical steps to satisfy the requirements of CP86 in the medium term, but certainly the expectation is that all FMCs will have made significant progress on their plan by the end of 2021. **ICQ**

# Dear CEO Letter - Schedule 2 Firms



**AUTHORS:** [Joe Beashel](#), Partner and Head of the Regulatory Risk Management and Compliance, Matheson, and [Karen Reynolds](#), Partner and Co-Head of the Regulatory and Investigations Team, Matheson. With the support of the ACOI Financial Crime Compliance Working Group.

**T**he Central Bank of Ireland (“CBI”) issued a “Dear CEO Letter” in December 2020 (the “Letter”), outlining the anti-money laundering/terrorist financing (“AML/CTF”) compliance issues that firms who are designated as ‘Schedule 2 firms’ must adhere to and monitor on an ongoing basis. Schedule 2 firms would include, for example, Irish SPVs that are involved in activities such as lending, debt factoring or finance leasing, unregulated lenders and others.

The Letter also sets out the CBI’s findings from its supervisory engagements with firms in accordance with Part 4 of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (as amended) (the “2010 Act”), which includes conducting inspections and holding ad hoc meetings with registered firms, as well as the CBI’s expectations in this regard. The CBI’s expectations addressed to Schedule 2 firms are, in our experience, entirely consistent with the regulator’s approach to AML/CTF compliance in other sectors and for compliance professionals with responsibility for AML/CTF nothing contained in the Letter will be a surprise.

## Board Oversight and Governance

As with many “Dear CEO” letters, the CBI’s first observation was addressed to boards. This is particularly relevant for the SPVs which were the focus of the CBI’s review given that these vehicles have no staff so it falls on the boards to ensure compliance. Firms are expected to ensure that AML/CTF is a regular agenda item at board meetings, and ensure a framework is in place to identify and adopt updates in the relevant legislation for ongoing compliance.

It is not mandatory for a Schedule 2 firm to appoint a Money Laundering Reporting Officer but it is considered to be best practice. If appointed, they (or their equivalent who has been clearly allocated AML responsibilities by the firm) should actively report to the Board on a frequent basis. It is recommended that this would include on relevant outsourced arrangements, where the Board does not have direct oversight, and the firm must be able to evidence that they are monitoring the progress of management action points arising from these arrangements. It may be that contracts with service providers will need to be revised to provide the support necessary to meet the applicable AML/CTF obligations.

## Risk Assessments

Where a firm relies on a third party, or another entity within a group of companies, to carry out its AML/CTF business wide risk assessment on its behalf, it must relate to risks and controls associated with the firm specifically, rather than focus on those of the wider group. The objective should be a focussed risk assessment not a generic one. This risk assessment should be refreshed annually, and approval by the board must be formally evidenced.

## Policies and Procedures

Firms must ensure to have documented AML/CTF policy and procedures in place, that are tailored to the specific business activities and associated risk factors of the firm, and which are consistent with Irish legislative requirements. Similar to the point on risk assessments, this finding comes from the CBI finding too many firms using “cookie cutter” precedents derived from group with not enough adapted to the specific circumstances of the Schedule 2 firm itself.

**“AS WITH MANY ‘DEAR CEO’ LETTERS, THE CBI’S FIRST OBSERVATION WAS ADDRESSED TO BOARDS. THIS IS PARTICULARLY RELEVANT FOR THE SPVS WHICH WERE THE FOCUS OF THE CBI’S REVIEW GIVEN THAT THESE VEHICLES HAVE NO STAFF SO IT FALLS ON THE BOARDS TO ENSURE COMPLIANCE.”**

## Customer Due Diligence (“CDD”)

Firms must consider the identity of their customers and must conduct appropriate due diligence in accordance with the level of risk involved with their customers. The Letter noted that many firms were inconsistent in determining who were their customers. This comment seemed particularly focussed on firms that raise capital from investors through loan notes and then subsequently lend that capital to third party borrowers as part of an investment strategy. There are broad obligations in Section 54 of the 2010 Act to prevent and detect money laundering and terrorist financing but the detailed due diligence obligations in section 33 only apply to customers. It is critical for firms to correctly distinguish between customers and others in order to correctly understand their obligations under the 2010 Act.

**“AT THE TIME OF WRITING, THE CRIMINAL JUSTICE (MONEY LAUNDERING AND TERRORIST FINANCING) (AMENDMENT) BILL 2020 (THE “BILL”) HAD ALMOST FINISHED ITS PASSAGE THROUGH THE OIREACHTAS AND WE CAN EXPECT IT TO BE FINALISED VERY SOON.”**

## Politically Exposed Persons (“PEPs”) and Financial Sanctions (“FS”)

Firms should ensure that the policies and procedures are in place to identify and escalate PEP and FS alerts, including the process and appropriate reporting lines to be followed. Where screening tools are relied upon, firms should ensure appropriate oversight and ongoing assurance testing and monitoring is in place to ensure they are fit for purpose. Suspicious Transaction Reporting (“STR”) Firms should ensure their policies and procedures include details for the escalation of suspicions, including the personnel to whom suspicions should be raised / reported. If AML responsibilities are outsourced to third parties, the firm should ensure the third party is subject to the appropriate level of oversight. The level of STRs being made by the firm should be regularly reported to the Board of Directors.

## Training

Training materials should be tailored to the business of the firm and be

reflective of the standards and practices the firm should be exhibiting to meet its obligations. These materials should be kept up-to-date and in line with Irish legislative requirements.

## Conclusion

The focus of the CBI’s guidance and expectations in the Letter centres around Irish SPVs, who have registered as Schedule 2 firms and have failed to put in place bespoke AML policies and procedures, an AML business-wide risk assessment, or relevant tailored outsourcing agreements for AML. Firms using generic, ‘off the shelf,’ policies and outsourcing agreements fail to take into account the specific business activities and risk factors faced by the firm, and will face CBI scrutiny in the event of any investigation conducted following registration as a Schedule 2 firm. These firms should carefully take time to design more tailored AML compliance arrangements prior to registration with the CBI, and ensure these arrangements are updated and under constant review. For SPVs the support of third party service providers will undoubtedly be critical in enabling boards to demonstrate compliance in a way which meets the expectations of the CBI.

## Virtual Asset Services Providers – 5AMLD

The Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Bill 2020 (the “Bill”) is expected to become law at the beginning of April (at the time of writing the precise date was not clear). The purpose of the Bill is to give effect to certain parts of the 5th Anti-Money Laundering Directive (Directive (EU) 2018/843) (“AMLD5”), and to transpose those parts into national law. Notably, the Bill proposes to bring virtual asset service providers (“VASPs”) within the

scope of Ireland’s AML regime for the first time and also creates a bespoke regulatory framework for such firms. These changes, including the definition of “Virtual Asset Service Provider” used in the Bill, go further than the minimum requirements of AMLD5 and seeks to bring Irish law on VASPs into line with the FATF Recommendations on the regulation of virtual asset service providers first published in June 2019.

The Bill introduces a number of new definitions into the existing AML regime, such as:

- 1 **Virtual Asset**, meaning a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes, but does not include digital representations of fiat currencies, securities or other financial assets;
- 2 **Virtual Asset Service Provider**, meaning a person who by way of business carries out one or more of the following activities for, or on behalf of, another person:
  - exchange between virtual assets and fiat currencies;
  - exchange between one or more forms of virtual assets;
  - transfer of virtual assets, that is to say, conduct a transaction on behalf of another person that moves a virtual asset from one virtual asset address or account to another; and/or
  - participation in, and provision of, financial services related to an issuer’s offer or sale of a virtual asset or both;
  - but does not include a designated person that is not a financial or credit institution and that provides virtual asset services in an incidental manner and is subject to supervision by a national competent authority, other than the CBI; and
- 3 **Custodian Wallet Provider**, meaning



an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies.

Section 25 of the Bill will seek to insert a Section 106E into the 2010 Act, requiring VASPs to register with the CBI for AML purposes in order to carry on activities as a VASP, such as an exchange between virtual assets and fiat currencies or acting as a custodian wallet provider. This will mean that the VASP or Custodian Wallet Provider will be subject to the same AML requirements as other designated persons, such as monitored transactions and customer due diligence.

### Other relevant provisions

Section 106F of the Bill provides that a firm carrying out virtual asset services immediately prior to the enactment of the provisions will be taken to be registered to carry on such services until the CBI is in a position to grant / refuse an application to register the firm, provided that the firm seeks registration for AML purposes no later than 3 months following the enactment of these provisions. This “grandfathering” allows existing VASPs to continue to provide these virtual asset services following the passage of the Bill into law, without any business interruption

suffered by the firm before the CBI’s acceptance of the its registration.

The Bill also outlines the factors the CBI may consider in deciding to refuse a firm’s registration application. These include a failure to satisfy the CBI: of the firm’s ability to comply with its obligations as a designated person; the firm will have in place sufficient resources and procedures to carry on business as a VASP; and the firm can manage and mitigate the risks of engaging in activities that involve the use of anonymity enhancing technologies or mechanisms that obfuscate the identity of the sender, recipient, holder or beneficial owner of a virtual asset.

Furthermore, a registered VASP will be required to include a regulatory disclosure statement in all of its advertisements for services, stating that the holder of the registration is registered and supervised by the CBI for anti-money laundering and countering the financing of terrorism purposes only.

### Who does the registration requirement apply to?

Section 106E of the Bill extends the registration obligation to “all persons carrying on business” as a VASP. Interestingly, the Bill does not make any express exception for firms that

may already be authorised by the CBI under other legislative frameworks (for example as e-money institutions or payment institutions). Accordingly, until the CBI issues guidance on the registration requirement following the entry of the Bill into law, it is unclear if the CBI will seek only to require otherwise unregulated firms to register as VASPs under this new framework.

### Other Developments

The developments proposed by the Bill comes at a time of other significant regulatory developments for crypto-asset service providers in the European Union. In September 2020, the European Commission published its proposal for the establishment of an EU-level regime for crypto-assets, the Market in Crypto-Assets Regulation (“MiCA”). MiCA will seek to bring all crypto-assets within the remit of EU financial services regulation for the first time. This regime will likely involve the creation of a more formal authorisation process for unregulated subsidiaries that are providing virtual asset services, and importantly, enable the passporting of these rights across the EEA. It is therefore likely that many firms requiring registration as a VASP under Irish law will eventually seek to obtain an authorisation under the more useful MiCA framework once it is finalised at EU level in the coming years. **ICQ**



# Culture, Ethics, Values, Beliefs - Which Comes First?

**AUTHOR:** Ed McDonald, FCOI, MA in Ethics (Corporate Responsibility), MBS.  
Part 1 of a 2-part series.

**O**ver the last few years the concept of corporate culture has become a major focus across many sectors in wider society, including industry and not least in financial services. Various corporate scandals and misconduct have shone a spotlight on the kind of culture that an organisation has that seems to permit, allow for, generate, even tolerate, misconduct that results in the harm of some kind to a range of parties (consumers, employees, communities, shareholders, taxpayers, and others), and to what extent are the misconduct behaviours somehow facilitated (not necessarily deliberately) by the way that organisation is structured and overseen. In this case, I use the term “overseen” to refer to people at the top in the organisation who set the tone for the organisation. And in Ireland it has become a significant focus for the Central Bank which is demanding financial service businesses improve their corporate cultures, hence why we are talking about it so much because it seems to have a touch of mystery about it.

### So, what is “culture”?

Corporate Culture, that is, the culture in companies and organisations, is a topic that has been extensively researched and written about. Just think about companies who have been reported as having culture issues and what went wrong in them. There are various definitions of what “culture” covers, or more specifically, corporate culture, but two will suffice for this paper.

The famous American management writer, Edgar Schein, saw organisational culture as having three elements – Artifacts (logos, images, posters, dress codes, workplace and office designs – aspects that one can readily see), Espoused Values (what the organisation says about itself and its ways of working and its desired standards) and Underlying beliefs

**“MANY ORGANISATIONS HAVE HAD HIGH-SOUNDING STATEMENTS ABOUT THEIR VALUES OR CODES OF CONDUCT BUT HAVE STILL HAD MAJOR MISCONDUCT PROBLEMS, REMEMBER ENRON AND ARTHUR ANDERSEN IN THE USA, BOEING, VOLKSWAGEN, DEUTSCHE BANK, WELLS FARGO? NOT TO MENTION A NUMBER OF PROMINENT IRISH COMPANIES.”**

(the attitudes, beliefs and behaviours that really underlie the way it acts inside itself and may not be always displayed). McKinseys probably have the most concise definition, one that many people are aware of – “Culture is the way we do things around here”. Maybe the reality is one or the other or a mix of both, but they paint a picture of what this mysterious concept called “culture” might be in practice.

Many organisations have had high-sounding statements about their Values or Codes of Conduct but have still had major misconduct problems (remember Enron and Arthur Andersen in the USA, Boeing, Volkswagen, Deutsche Bank, Wells Fargo? Not to mention a number of prominent Irish companies, including financial services). There are lots of cultures at various levels and scales and they’re not necessarily bad or defective in themselves, at least at the theoretical level – but some can be and are at the practice level, the “how we actually do things” level.

**“ I WAS BORN INTO A CULTURE. YOU WERE BORN INTO A CULTURE. BUT AT NO STAGE DID ANYONE EVER SAY THAT I WAS NOW ENTERING, OR PART OF THIS CONCEPT CALLED ‘CULTURE’. I DIDN’T ASK TO BE BORN INTO THAT CULTURE AND LIKEWISE YOU DIDN’T.”**

## Varied Cultures

I was born into a culture. You were born into a culture. But at no stage did anyone ever say that I was now entering, or part of this concept called “culture”. I didn’t ask to be born into that culture and likewise you didn’t. We each entered our respective culture with no knowledge of it. And as we went through our infancy and then our early childhood we were taught things and learned aspects of being in that culture, what it was like to be part of it, a member of it. The first culture we each (or most of us) experienced was the culture of our family, and probably our first culture influencers were our parents and related family members. Our parents in turn probably carried with them influences or views about parenting that they got from their families and then from their practical life experiences. My family lived in a village where there was probably some kind of

village culture, e.g., a commitment as part of the village, so my family could be said to be a sub-culture within the village culture. My village was part of a county and in turn it might have had something akin to a village culture. And when I went to school (be it primary or secondary) it in turn had a culture where I was taught things and learned how to work in that situation. Then at University I realised university was different and had a culture of its own (though at the time I didn’t think of it as having a “culture”), where I had to study, more at my own pace than being driven by a teacher as had been the case in primary and secondary school. As I subsequently joined clubs and organisations and took up different jobs on my career path, I encountered slightly different cultures, all of them with their own way of doing things, and which involved working out how to work with others, play as a team player,

develop a sense of competitiveness because of playing in competitions. And all of them were within the context of there being what was called a “national culture”, the Irish culture (or whatever your nationality), a broad notion of what being Irish involved, what marked Irish people out as being a bit different from the people of other nationalities. And then I travelled overseas a lot and saw the ways things were done in other places. And I worked in England and later lived and worked in New York, experiencing different kinds of cultures. I didn’t overly think about them being called “cultures” though I was told that the New York culture was aggressive, assertive, get on with it, hit the targets. But I found my way through them all and the differences they brought to my life. I adapted and fitted in. And I could have left any of them if I didn’t like it or feel comfortable in it. Did they change me? Did I change?





## Who Creates ‘Cultures’?

I paint the somewhat long-winded picture above to show that I and many other people, including you, inter-act and have inter-acted with a variety of other cultures, each with their particular sense of focus. But who set each of those separate cultures? Was there somebody (or somebodies, plural) who decided or exerted influence on creating each of those cultures? Or were there many people who contributed to them and at varying levels in any given organisation? For the purposes of this paper, let’s interpret those organisations as being in the financial services industry. And if they are really big organisations, have they got the same Corporate Culture, Mission statements, Values and Codes of Practice for every part of the organisation, every department, every branch, every subsidiary, every location, everyone in the organisation at all levels? And is that realistic?

As the US magazine Compliance Week (15 June 2020) commented “Establishing a culture based on values and transparency is more effective at preventing misconduct than a robust set of rules, and it quotes the LRN (a major US corporate behavioural research company) 2020 survey: “An organization’s ethical culture determines whether its rules and procedures will be followed, ignored, or circumvented, no matter how thick the rule book may be.” The clear indication in its findings is that how a company does things in practice (its culture) is the critical element in acting and behaving, and that it will regularly outweigh any grand policy statements. They are all necessary in developing a right focus but as is often said “Actions speak louder than words”. Setting up, running, managing, doing the tasks of any organisation, is done by people, people who make decisions and choices about what to do. And those people can be at

varied levels in the organisation. So if there is an organisational culture problem, then it’s for the people in it to decide what should be done about it. The question is “Who are those people who can do something about it?”

While not specifically talking about corporate culture, the famous Albert Einstein very aptly said: “The world we have created is a product of our thinking. It cannot be changed without changing our thinking.... If we want to change the world, we have to change our thinking.... no problem can be solved from the same consciousness that created it”. **ICQ**

**IN THE NEXT ISSUE:**  
**The second part of this Article dealing with Ethics and Values.**

# Compliance in the Age of Digital Finance

AUTHOR: **Andrew Quinn**, Director, PAT Fintech



- Client Onboarding
- Know Your Customer (KYC)
- Transition Monitoring
- Suspicious Transaction Reports (STR)

For RegTech vendors, the providers of 'solutions' to the AML compliance function within financial service providers, from first principles, the critical question they must address is what is the business (compliance) problem they are solving? Is it providing a product/service that reduces the so-called 'burden' of AML compliance and regulatory reporting, or is it building a product/service that actually prevents financial crime?

Is it constructing/implementing systems and processes that improve a financial institution's knowledge of its existing and new clients, or is it putting in place systems and processes that effectively identify money laundering and fraud?

Are the RegTech companies working on their own, or are they working in collaboration (building consortiums) with other vendors, financial institutions, and government agencies to build a better overall solution?

The easiest way to address the business problem from a technology perspective is to distill it down to the two key business challenges that the RegTech is trying to address: knowing your customer (KYC) and anti-money laundering (AML), and related to this is another critical question:

In September 2020, the European Commission published its Digital Finance Package, consisting of a Digital Finance Strategy, a Retail Payments Strategy, and two legislative proposals, on crypto-assets and on digital operational resilience. The goal is to develop a competitive EU financial sector that gives consumers access to innovative financial products, while ensuring consumer protection and financial stability.

In this digital age of financial services, in an environment of Fintech innovation, the Central Bank of Ireland will play an increasingly active role in the evolving European framework of regulation and supervision, and technology will become ever more important in managing the challenges inherent in the contemporary compliance function.

This article examines how regulatory technology (RegTech) solutions can be utilised to meet these challenges, specifically related to the core elements of AML/CFT compliance.

## First of all, a definition

RegTech can be thought of as an intersection where the horizontals of underlying technologies and innovations meet the verticals of financial services compliance. In its simplest forms, RegTech is the application of technology to improve the efficiency of regulatory compliance.

Focusing on KYC and AML, RegTech solutions can typically be applied across the following stages of the compliance cycle:

- **Business/Customer Risk Assessment**

are KYC and AML separate or linked? In truth, like much else in the provision of basic financial services, for example payments, neither KYC or AML are new concepts. Criminals, and the proceeds of crime and money laundering, have existed since the beginnings of anything resembling a banking system, if not before.

The issue is that whilst from a conceptual definition perspective the two concepts are undoubtedly linked - did you really perform accurate KYC processes if it turns out that the client is subsequently identified as a money launderer? - from a technology perspective there are important differences between the two.

For example:

KYC can be viewed as a static entity – the information on a form (digitised or not) is accurate at a certain fixed point in time.

AML on the other hand is dynamic, and therefore, in many ways, much more elusive to control – money laundering cannot be identified on a digitised form at a point in time - it is a process flow.

To clarify this, as with all the best technology solutions, RegTech solutions must have as their basis a clearly defined business (compliance) problem. Identifying that business (compliance) problem should lead to a high-level systems' requirements specification from which engineers then build the solution.

From a technology perspective, it is one thing to digitise and update the up to the minute details on anyone engaging in financial transactions, but the real challenge is how do you deploy technology to identify and potentially stop something that is happening in 'real-time'? This is a formidable

## “FOR REGTECH VENDORS, THE PROVIDERS OF ‘SOLUTIONS’ TO THE AML COMPLIANCE FUNCTION WITHIN FINANCIAL SERVICE PROVIDERS, FROM FIRST PRINCIPLES, THE CRITICAL QUESTION THEY MUST ADDRESS IS WHAT IS THE BUSINESS (COMPLIANCE) PROBLEM THEY ARE SOLVING?”

challenge, and the solutions are only just becoming potentially viable.

One could argue that while significant progress has been made in KYC over the last number of years, *real AML is still in its infancy*, and considerable work needs to be done if RegTech solutions can materially impact the effectiveness of AML/CFT detection and enforcement.

To create an environment where RegTech solutions can effectively manage the compliance and regulatory risks in an age of digital finance, the ecosystem of stakeholders in the Irish (EU) financial services industry must come together to address the serious barriers that remain in the evolution of the AML/CFT framework.

For example:

- **Addressing the concerns of civil liberty groups and harmonising data privacy laws;**
- **Establishing cross-jurisdictional data exchanges and the legal standards;**
- **Increasing the transparency of offshore tax havens; and**
- **Incentivising the sharing of data by banks and other repositories of customer data.**

The implementation of the EU's Action Plan for a comprehensive, harmonised, policy on AML/CFT creates

an opportunity, but to innovate, and create better solutions for business (compliance) problems, RegTechs must be a welcomed vocal stakeholder in the Irish financial services ecosystem.

The recently published Ireland for Finance 2021 Action Plan recognises the direction of digital finance, specifically the *'opportunities for digital finance (or 'fintech') and in particular for SupTech (the use of financial technology by supervisory authorities) and the thriving RegTech (the application of financial technology for regulatory and compliance requirements and reporting by regulated financial institutions) sub-sectors in Ireland.'*

We are now unequivocally living in the digital age of financial services.

Compliance and regulation provide valuable protection for consumers and ensure the safety and integrity of the financial system so they will always remain core to the provision of financial services.

Deploying technological solutions and fostering our indigenous RegTech sector is essential to maintaining, and enhancing, Ireland's (the EU's) reputation as a well-regulated financial centre capable of attracting further investment in this exciting new age of digital finance. **ICQ**

# New ACOI Education Programmes

ACOI in partnership with Professional Accountancy Training (PAT), have developed 2 new qualifications designed for the financial services industry and compliance professionals of the 2020's. The ACOI has always anticipated developments in regulation and associated risks and these new qualifications continue that mission. Ireland is an important location for the fintech industry and not just because of Brexit. These qualification will contribute to our strong fintech ecosystem, ensuring that Ireland remains attractive to those seeking to develop a fintech business.

## Professional Certificate in Fintech Risk & Compliance

### Programme Overview

Compliance is core to the provision of regulated Financial Services and the risk management of those services. The evolution of technologically driven innovation in Financial Services (Fintech) presents new challenges for the contemporary compliance function. Fintech's focus on the application of innovative technological solutions and enhanced data analytics to deliver an optimal (customised) user experience needed to be balanced by appropriate governance, control, and oversight. For Fintech companies – whether they are 'new' Fintech companies and/or an 'incumbent/traditional' Financial Institution that is providing technologically enabled Financial Services/products - the strategic priority is to balance the foundations of compliance and control with the flexibility to capitalise on technological innovation.

The ACOI and its education partner, Professional Accountancy Training

(PAT) have collaborated to develop a contemporary practitioner focused course that translates the traditional compliance function in the evolving Fintech environment. This course has been designed to address industry-wide challenges by providing professional training in Fintech Risk and Compliance. The programme provides participants with the knowledge and skills required to conduct and manage evolving compliance functions within the Financial Services industry.

### How you will benefit

On successful completion of the Professional Certificate in Fintech Risk and Compliance, graduates will be able to:

- Understand the structure of the International, European, and Irish regulatory environment from a Fintech perspective and identify areas of EU & Irish legislative and regulatory focus ;
- Analyse from an operational perspective the AML/CFT compliance and regulatory reporting risks in a Fintech operating environment;
- Assess the compliance risks associated with data protection and the ethical

- use of personal data in a Fintech data driven operating model;
- Identify the contemporary compliance risks in the safeguarding arrangements of payment and electronic money institutions;
  - Evaluate the regulatory focus upon compliance risks related to outsourcing of critical services by financial service providers;
  - Demonstrate an awareness of fitness, probity, conduct, and authorisation risks in an evolving Fintech environment;
  - Identify the compliance risks related to regulated and non-regulated cryptocurrencies and crypto-assets services;
  - Examine the compliance, and ethical, risks of an increasingly data - driven Fintech product development cycle; and
  - Contextualise the importance of a compliance culture in the provision of financial services in the Fintech ecosystem.

#### Award

The course is approved by ACOI and participants will receive a Professional Certificate in Fintech Risk and Compliance on successfully passing the continuous assessments and final exam.

## Professional Certificate in Anti-Money Laundering in a Fintech Environment

#### Programme Overview

The course is designed to provide professionals, practitioners and other stakeholders with the skills and competencies that supports a culture of AML compliance that in turn establishes Ireland as a centre of both European and global AML/CTF excellence and innovation.

In the context of the technologically driven innovation in Financial Services (Fintech) the course addresses AML requirements from the perspective of a variety of sectors – for example: Credit and Financial Institutions ('Firms') and Designated Non-Financial Business and Professions (DNFBP's).

The course identifies the core requirements and contemporary (technologically enhanced) best practice in the risk assessment, client onboarding, and life cycle management of client accounts from the perspective of both the financial institutions and professional service providers for example: accountants and auditors.

#### How you will benefit

On successful completion of the Professional Certificate in Anti-Money Laundering in a Fintech Environment, graduates will be able to:

- Assess the evolution of EU AML Directives and their transposition into Irish (national) legislation;
- Evaluate the role of FATF and the national FIU's in investigating and implementing effective AML/CTF enforcement;
- Identify the critical elements of a contemporary AML programme in an evolving Fintech (digital) environment;
- Contextualise the importance of culture and collaboration in the Irish AML Compliance Framework;
- Evaluate the critical inter-related stages of the AML Compliance Cycle and the perspective of the key stakeholders in the Irish AML Framework;
- Assess the AML/CTF regulatory requirements, Central Bank of Ireland's guidance, and contemporary best

practice for the risk assessment of new counterparties and customers;

- Demonstrate contemporary best practice in the onboarding, and lifecycle management of new counterparties/clients in an evolving regulatory and technological Fintech environment;
- Analyse the effectiveness of transaction monitoring processes, the quality of STR information, and the potential of technologically enabled solutions in the AML Compliance Framework;
- Identify the challenges (regulatory, information sharing, and optimising resources) in investigating STRs and enforcing AML sanctions; and
- Contextualise the importance of stakeholder co-operation and analyse the potential for technologically enhanced solutions to enhance the effectiveness of the AML prevention and enforcement.

#### Award

The course is approved by ACOI and participants will receive a Professional Certificate in Anti-Money Laundering in a Fintech Environment on successfully passing the continuous assessments and exam. **ICQ**

**You must be a current member of the Association of Compliance Officers in Ireland, or become a member, to register for the programmes listed. Membership is currently €150 per year. For further information on the programmes please email [info@acoi.ie](mailto:info@acoi.ie)**

# Recruitment Market in Compliance



**Overview of the Robert Walters 2021 Recruitment Survey Results: Brexit, regulatory change, substance requirements and confidence.**  
**AUTHOR: Michael Nolan, Manager, Compliance, Robert Walters.**

**T**he first quarter of 2021 has been a whirlwind for the compliance community. It has seen substantial fines being issued and a seismic shift within the retail banking and broking world that is raising the bar of firms' attitudes towards compliance. The catch up on 2020's recruitment agenda has played a big part in the volume of new roles opening up since the start of the year given sign off constraints and some unreadiness to hire and onboard remotely last year.

## Brexit

Brexit and its impact on the Irish regulated financial services industry continues to be a driving force in the compliance recruitment market. Initially we saw 140+ firms across asset management, banks, broking and insurance acquire a licence in Ireland and hire the required PCF designated persons to meet their regulatory requirements. Now, a further wave of licence applications have appeared to include many fintech payments firms and some ManCo's seeking to elevate their authorisation status to include investment permission (SuperManCo).

**“WHILE THE LANDSCAPE OF THE RETAIL BANKING MARKET IS IN FLUX AND VOLUNTARY REDUNDANCIES HAVE BEEN COMMONPLACE THIS YEAR, OTHER INDUSTRIES SUCH AS ASSET MANAGEMENT, BROKING, CORPORATE BANKING, INSURANCE AND PAYMENTS HAVE HAD A SIGNIFICANT LEVEL OF HIRING AT ALL LEVELS.”**

## Substance Requirements

The call for substance across authorised firms has been an ongoing feature, raising demand at the compliance analyst level in particular. Having the right entrance points to the compliance market from graduate to analyst level, coupled with formal qualifications will play an important role in building home grown talent, in particular as we reach the saturation point of full employment within the profession. Needless to say, some firms and professional bodies are doing excellent work by decree or design, which is putting in the groundwork to bring through the next generation of compliance officers.

## Returning Confidence

While the landscape of the retail banking market is in flux and voluntary redundancies have been commonplace this year, other industries such as asset management, broking, corporate banking, insurance and payments have had a significant level of hiring at all levels. Ultimately confidence has returned to the market both from a stability and operational standpoint. This confidence leads to movement which in turn creates a domino effect and the cycle of new and replacement roles coming to the market continues. Sentiment across the market is that changing roles while being onboarded



**COMPLIANCE IRELAND**

Role	Permanent Salary Per Annum EUR (€)	Contract Rate Per Day (PAYE) EUR (€)
	Range	Range
Chief Compliance Officer	160,000 - 220,000	800 - 1200
Head of Compliance	120,000 - 160,000	600 - 1000
Senior Compliance Manager	90,000 - 130,000	400 - 600
Compliance Officer/Manager	65,000 - 90,000	250 - 400
Compliance Analyst	45,000 - 65,000	200 - 300
Compliance Administrator	35,000 - 45,000	135 - 190
MLRO/Head of Financial Crime	100,000 - 150,000	500 - 750
AML/Financial Crime Manager	80,000 - 100,000	250 - 425
AML/KYC Analyst	45,000 - 60,000	175 - 250
AML Administrator	30,000 - 45,000	120 - 175
Fraud Manager	65,000 - 90,000	250 - 400
Data Protection Officer	90,000 - 120,000	350 - 500
Data Protection Executive	60,000 - 80,000	230 - 320

NR: All figures represent basic salaries exclusive of benefits/bonuses, unless otherwise specified.

remotely is relatively seamless now compared to at the start of the pandemic. In most cases, organisations are better prepared to interview, train, onboard, connect and communicate through online resources than ever before.

### Increased Salary Levels

We have seen an increase in salary levels which was initially related to an uplift in demand and authorisation requirements. These increases are now justified by the pending introduction of the Senior Executive Accountability Regime (SEAR). Enforcement action from the regulator serves as a stark reminder to the industry that compliance officers offer the support and protection needed to manage the strategic tension between a firm’s financial success and its adherence to regulatory requirements. Combined with the increase risk and responsibility taken on by PCF role holders, we expect to see a continued increase in compensation.

### Emerging Trends Driving Recruitment in Compliance:

- An increase in claims and focus on consumer protection in insurance;
- Influence of the CP86 thematic review in asset management;
- Market abuse and integrity within MiFID firms;
- Regulatory transformation

- programmes in corporate banking;
- Schedule 2 firms coming further into scope;
- Authorisations and growth of the fintech space;
- Financial crime within institutional and corporate banking, payments, fintech and gaming;
- Employer and candidate confidence. **ICQ**

**MICHAEL NOLAN**  
**MANAGER**  
**COMPLIANCE DIVISION**

DL: +353 (0)1 6730821  
 Mobile: +353 (0)87 6598178  
 E-mail: Michael.Nolan@RobertWalters.com

**ROBERT WALTERS SALARY SURVEY 2021**

**DIVERSITY & INCLUSION STRATEGY REPORT**

**ROBERT WALTERS**

**1** On **TUESDAY, 19<sup>TH</sup> JANUARY**, we were delighted to have Jan De Spiegeleer, CEO and Founder of RiskConcile deliver a webinar on the upcoming PRIIPs regulation. The webinar was case-study based and explored some practical real-world examples and simulations. RiskConcile illustrated some caveats in the current regulation that impact the Key Information Documents (KIDs) provided to the retail public.



**2** On **THURSDAY, 21<sup>ST</sup> JANUARY** Grace Guy from the Pensions Authority joined us and shared the Authority's key findings following inspections of trustees of master trusts and defined benefit schemes under the 2020 engagement programme. Grace discussed areas where good compliance was demonstrated and on the flip side where failings were identified and what the issues were as well as the actions to be taken to rectify instances of non-compliance. In addition, Grace also discussed the IORP II Directive.

**3** This webinar was the third in a series that explored the traditional compliance function in the technologically driven Fintech environment. This webinar examined the scale and evolution of Fintech providers and evaluated the EU Commission's strategy of optimising the benefits of Fintech with appropriate compliance and regulatory frameworks. The webinar provided a range of perspectives from financial service providers and compliance professionals.





**4** On **THURSDAY 4<sup>TH</sup> MARCH** Laura Wadding and Maggie Nugent, Deloitte delivered a webinar that delved into the background and changing regulatory environment, provided an overview of the Fund Management Company guidance and the latest Dear Chair as well as explored the nature of RMPs being issued and what is required in preparing a plan for Board approval.

**ACO I**  
The Association of Compliance Officers in Ireland

## Thank you for attending

### Fund Management Companies (CP86)

Laura Wadding Partner, Regulatory Risk, Deloitte  
Maggie Nugent Manager, Regulatory Risk, Deloitte  
4<sup>th</sup> March 2021

CPD Code: TBC

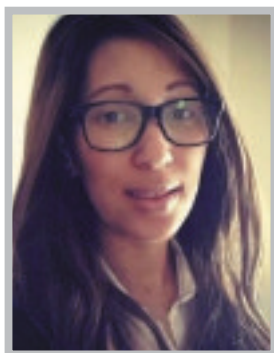
**5** With direct reference to the recently published Finance for Ireland Action Plan 2021, this webinar brought together practitioners, RegTechs, academics and researchers. This panel led discussion focused upon facilitating the interactions between the underlying technologies and innovations of Financial Services compliance that can support the development of RegTech ecosystem. **ICQ**

**ACO I**  
The Association of Compliance Officers in Ireland

## Innovation in RegTech Solutions & Research

Andrew Quinn Head of Fintech & Financial Services, Professional Accountancy Training  
Devraj Basu Senior Lecturer in Finance in the Accounting and Finance department at Strathclyde Business School  
Sharadha V Tilley Lecturer in Finance at Technological University Dublin  
Gerald Murphy Industry advisor to Encompass Corporation  
Rachel Woolley Global Director of Financial Crime @ Fenergo  
9<sup>th</sup> March 2021

CPD Code: TBC



## “EMBRACING DIVERSITY AND INCLUSION IS VERY IMPORTANT TO ME.”

In this issue, we would like to introduce **Claudette Whyte**, who works in **Financial Crime & Compliance Assurance** at **Barclays Ireland**. Claudette is a **Fellow and Director of the Association of Compliance Officers in Ireland**, a **Certified Data Protection Officer** and a **Certified Financial Crime Prevention Practitioner**.

### Where is your favourite place in Ireland?

I love the medieval town, Kilkenny. It's a vibrant town with so many things to do. It possesses so much history which celebrates arts, culture and the community. I love the festivals, food and museums and when I visit, I make sure to explore the historic buildings, gardens and art galleries.

### What did you want to do when you left school?

I grew up wanting to be a Human Rights lawyer. I was raised in a country where the unfair and inhumane treatment during the apartheid era stirred a passion within myself to restore and become a voice to the people. Anti-apartheid lawyer, the late George Bizos, who has represented Nelson Mandela and fellow anti-apartheid activists, is someone I drew inspiration from.

### How did you enter the world of Compliance?

I had planned on pursuing compliance studies in South Africa so when I moved to Ireland, I immediately started the ACOI Certificate in Compliance followed by the Diploma in Compliance and then the MSc in Compliance. I enjoy compliance and my legal and forensic investigation background has equipped me with the necessary skills to excel in the field.

### What's the most valuable advice you have been given?

My parents taught me to have humility, to never stop trying to achieve my goals and to always have an enduring passion for knowledge. I live by the quote of the late Nelson Mandela "What counts in life is not the mere fact that we have lived. It is what difference we have made to the lives of others that will determine the significance of the life we lead".

### How do you relax and unwind?

I am a family-orientated person and pride myself on spending every Sunday with my family. I feel passionately about taking care of myself mentally, spiritually and physically so I go for a run daily, listen to music and read the Bible. I started learning to play the violin last year as well. Pre-COVID, I enjoyed travelling to discover countries and have an understanding of different cultures.

### What is your favourite restaurant?

I have two! I absolutely love the Lady Helen Restaurant at Mount Juliet in Kilkenny as well as The Saddle Room at The Shelbourne in Dublin.

### An interesting fact about you?

I did foil fencing when I was at university in South Africa and for a number of years thereafter.

### What is your biggest accomplishment?

One of my biggest accomplishments is completing the MSc in Compliance whilst working. It is also one of the biggest sacrifices I made, allocating my time between studies and work but always bearing in mind, the end goal. I also recently won a Recognition Award for my involvement in Diversity & Inclusion and feel proud of the hard work I've put into a number of projects I'm involved in. Embracing diversity and inclusion is very important to me personally. It is not just the right thing to do to move society forward, it strengthens our compliance culture, differentiates us and is a major factor in our future success as an association. Whether it's race, ethnicity, sexual orientation, ability, gender or life-stage, I will be committed to the ACOI being a place where everyone feels included and where everyone is given the opportunity to realise their potential. **ICQ**

# CALLING ALL SMEs

## PROJECT ARC – AN AWARENESS RAISING CAMPAIGN FOR SMEs, FUNDED BY THE EU COMMISSION, REC PROGRAMME

In May 2018, Europe introduced the General Data Protection Regulation (GDPR). This harmonised law replaced existing data protection regulations in each country, enhanced the data protection rights of individuals, strengthened the enforcement powers of Data Protection Authorities and increased the obligations of accountability and transparency on organisations that process personal data as part of their business. Since that time, SMEs have been seeking reliable guidance on how best to meet those obligations and ensure that they are in compliance with the requirements of the GDPR.

As part of the EU Commission's efforts to provide that guidance, Project ARC (AWARENESS RAISING CAMPAIGN FOR SMEs) has been funded by the EU Commission with the expressed purpose of providing that guidance

and engaging with SMEs. The project - which commenced at the end of March 2020 - is being steered by a partnership between the Croatian and Irish Data Protection Authorities and Vrije University in Brussels. Over the course of the next two years, the project team will be engaging with SMEs on an ongoing basis to develop the resources SMEs need to drive GDPR-compliance.

Having just one law benefits businesses and promotes responsibility when dealing with personal data, but ensuring compliance requires work on the part of organisations of all sizes. In recognition of this, the ARC Project has been convened to work with small and medium enterprises who may not have access to extensive resources and consequently struggle with compliance issues. By gaining greater insight into the climate in which SMEs operate, the

ARC project aims to assist the sector to grow and prosper in an efficient and compliant way.

The purpose of this survey is to gain insights into the way in which Data Protection is incorporated into the daily workings of SMEs across Europe and, in particular, the challenges faced by them in their efforts to comply with the GDPR.

The aim of the survey is to provide guidance to the ARC project so that it can tailor its guidance to better suit the needs of the sector and reduce the burden associated with compliance.

The survey is conducted on an anonymous basis and the results will be based on aggregate data. Information from these surveys will not be shared with Data Protection Authorities for the purposes of regulatory enforcement.

A long-exposure photograph of the Dublin skyline at night. The Samuel Beckett Bridge is the central focus, its illuminated arch and cables reflected in the water. The city lights and buildings in the background are also reflected, creating a vibrant, colorful scene. The sky is a deep blue, and the water is dark with bright reflections.

**The ACOI provides an authoritative voice  
on regulatory compliance and business ethics  
and is the premier provider of  
compliance education and professional  
development in Ireland**

**The Association of Compliance Officers in Ireland**

5 Fitzwilliam Square East | Dublin 2 | D02 R744

T: +353 1 779 0200 | E: [info@acoi.ie](mailto:info@acoi.ie) | W: [acoi.ie](http://acoi.ie)

Follow us on LinkedIn and Twitter