DILLON EUSTACE

DUBLIN CAYMAN ISLANDS NEW YORK TOKYO

Payments, E-Money and Crypto-Assets

Quarterly Legal and Regulatory Update

Period covered: 1 July 2020 – 30 September 2020

TABLE OF CONTENTS

1. PAYMENTS

1.1 European Commission adopts proposal for codification of Regulation on cross-border payments

On 17 July 2020, the European Commission (**Commission**) adopted a legislative proposal for a Regulation on cross-border payments in the European Union (**EU**).

The purpose of the proposal is to undertake a codification of the current Regulation on cross-border payments (No 924/2009), with the aim of simplifying and clarifying the law. The current Regulation has been amended several times, therefore the new Regulation will supersede the current Regulation and the various acts incorporated in it. No changes of substance will be made.

A feedback period was open from 17 July 2020 to 11 September 2020, during which time the Commission invited stakeholders to submit their views. The proposed Regulation will now be considered by the European Parliament and the Council of the EU. It is expected to come into force on 20 April 2021.

The text of the proposed Regulation can be accessed here, and its accompanying Annexes can be accessed here.

1.2 The Commission publishes communication on a Retail Payments Strategy for the EU

On 24 September 2020, the Commission published a communication on a Retail Payments Strategy for the EU.

The strategy identifies the Commission's objectives in respect of retail payments, namely to make instant payments and EU-wide payment solutions more accessible and cost effective for citizens and businesses across Europe. The Commission will also seek to foster consumer protection and increase consumer trust in instant payments.

To achieve these objectives, the strategy focuses on four key pillars:

- increasingly digital and instant payment solutions with pan-European reach;
- innovative and competitive retail payments markets;
- efficient and interoperable retail payment systems and other support infrastructures; and
- efficient international payments, including remittances.

The Strategy forms part of the Commission's digital finance package, adopted on 24 September 2020.

The text of the communication is available here.

1.3 EBA updates Single Rulebook Q&A on PSD2

During the period 1 July 2020 to 30 September 2020, the European Banking Authority (**EBA**) published an updated version of its Single Rulebook Questions and Answers publication (**Single Rulebook Q&As**) on the Revised Payment Services Directive (2015/2366/EU) (**PSD2**). The Q&As in respect of the following articles have been updated:

- Article 5 - Applications for authorisation;
- Article 96 - Incident reporting;

- Article 97 – Authentication; and
- Article 98 - Regulatory technical standards on authentication and communication.

The updated Single Rulebook Q&A can be accessed here.

2. DIGITAL FINANCE & CRYPTO-ASSETS

2.1 ECB publishes response to Commission consultation on a new digital finance strategy for Europe/FinTech action plan

On 27 August 2020, the European Central Bank (**ECB**) published its response to the Commission's public consultation on a new digital finance strategy for Europe/FinTech action plan (the **Response**).

The Response broadly supported the priority areas identified in the consultation document, noting that while fintech innovation may bring benefits to financial institutions and their customers, due account must be taken of the associated risks.

With regard to the Commission priorities, the Response concluded:

- while the current EU financial services regulatory framework is broadly technology neutral, it should support fair competition in digital financial services and reinforce the need to develop strong risk management at firm level;
- that the ECB fully endorses the mandatory use of unique identifiers;
- that the ECB supports the need for enhanced cooperation throughout the EU on different schemes such as regulatory sandboxes and innovation hubs, while fostering open dialogue between supervisors and supervised entities;
- that the ECB is adapting its supervisory approach in response to open finance, in particular in response to PSD2; and
- that any customer data sharing, particularly with third-party providers, must meet legal requirements and fulfil security standards.

The text of the Response can be accessed here.

2.2 The Commission adopts digital finance package

On 24 September 2020, the Commission adopted a new digital finance package.

The purpose of the package of measures is to boost Europe's competitiveness and innovation in the financial sector and give consumers access to innovative financial products, while ensuring consumer protection and financial stability.

The digital finance package contains the following initiatives:

- a digital finance strategy, setting out in general terms how Europe can support the digital transformation of finance while regulating its risks;
- a retail payments strategy;
- legislative proposals on crypto-assets, namely for a regulation on markets in crypto-assets and for a regulation on a pilot regime for market infrastructures based on distributed ledger technology (**DLT**); and

- legislative proposals supporting the creation of a regulatory framework on digital operational resilience for the financial sector.

The communication setting out the content of the digital finance package in detail can be accessed here.

2.3 The Commission adopts proposal for a Regulation on a pilot regime for market infrastructures based on DLT

On 24 September 2020, the Commission adopted a proposal for a Regulation on a pilot regime for market infrastructures based on DLT, i.e. the use of technology that trades and settles transactions in financial instruments in crypto-asset form.

Existing EU financial services legislation often pre-dates DLT and in some cases this may hinder its adoption or innovation. The purpose of the pilot regime is to allow regulators to gain experience of the use of DLT in market infrastructures and to allow companies to test out solutions using DLT. The pilot regime provides for derogations from existing rules and will allow companies learn more about how existing rules fare in practice.

The proposal seeks to improve legal certainty, support innovation, instil consumer and investor protection and market integrity, and to ensure financial stability.

This proposal forms part of the Commission's digital finance package, adopted on 24 September 2020. Amongst other priorities, the package of measures seek to ensure that the EU financial services regulatory framework is innovation-friendly and is adaptable to the application of new technologies.

The text of the proposal is available here.

2.4 The Commission adopts legislative proposal for a Regulation on markets in crypto-assets

On 24 September 2020, the Commission adopted a proposal for a Regulation on markets in crypto-assets.

The proposed Regulation will replace existing national frameworks applicable to crypto-assets not covered by existing EU financial services legislation and will establish rules for 'stablecoins', including when these are e-money. It will establish uniform rules for crypto-asset service providers and issuers at EU level.

The proposal has four main objectives:

- to provide legal certainty for crypto-assets falling outside existing EU financial services legislation;
- to support innovation and facilitate the development of crypto-asset markets in the EU;
- to instil consumer and investor protection; and
- to ensure financial stability.

The proposal forms part of the Commission's digital finance package, adopted on 24 September 2020. Amongst other priorities, the package of measures seek to ensure that the EU financial services regulatory framework is innovation-friendly and is adaptable to the application of new technologies.

The text of the proposal is available here, and its accompanying annexes are available here.

2.5 The Commission adopts legislative proposal for Regulation on digital operational resilience for the financial sector

On 24 September 2020, the Commission adopted a legislative proposal for a Regulation on digital operational resilience for the financial sector by amending the Credit Rating Agencies Regulation (1060/2009/EU) (**CRA**), European Market Infrastructure Regulation No 648/2012 (**EMIR**), Markets in Financial Instruments Regulation (600/2014/EU) (**MiFIR**) and the Central Securities Depositories Regulation (909/2014) (**CSDR**).

The legislative proposal aims to introduce a harmonised and comprehensive framework on digital operational resilience for European financial institutions. The legislative proposal sets out requirements applicable to:

- financial entities in respect of Information and Communication Technologies (**ICT**) risk management;
- contractual arrangements between ICT third-party service providers and financial entities; and
- the oversight framework for critical third-party service providers and rules on cooperation between competent authorities.

The proposal forms part of the Commission's digital finance package, adopted on 24 September 2020. Amongst other priorities, the package of measures seek to ensure that firms can withstand all types of ICT related disruptions and threats by setting certain minimum standards to prevent and limit the impact of such incidents.

A copy of the legislative proposal can be accessed here.

2.6 The Commission adopts legislative proposal amending existing EU financial services legislation in respect of crypto assets and digital operational resilience

On 24 September 2020, the Commission adopted a proposal for a Directive clarifying and amending existing EU financial services legislation in respect of crypto assets and digital operational resilience.

More specifically, the proposed Directive will:

- amend various operational risk or risk management requirements in a number of Directives by introducing precise cross-references, in order to attain legal clarity. These amendments complement the proposal for a Regulation on digital operational resilience;
- clarify the legal treatment of crypto assets qualifying as financial instruments by amending the definition of a 'financial instrument' in the Markets in Financial Instruments Directive (2014/65/EU) (**MiFID II**); and
- provide for the temporary exemption of DLT market infrastructures from certain provisions in MiFID II in order to enable them to develop solutions for the trading and settlement of transactions of crypto-assets that would qualify as financial instruments. This measure complements the proposal for a Regulation on a pilot regime for DLT market infrastructures.

The proposal forms part of the Commission's digital finance package, adopted on 24 September 2020.

The text of the proposal can be accessed here.

3. CYBERSECURITY

3.1 The Commission conducts review of NIS Directive

On 7 July 2020, the Commission launched a public consultation on the Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the EU (**NIS Directive**). The consultation formed part of the Commission's review of the NIS Directive, which is expected to be concluded by the end of 2020.

The NIS Directive is the first piece of EU-wide legislation on cyber-security. It provides legal measures to boost the overall level of cybersecurity in the EU.

In light of the fast moving nature of the cyber-security landscape, the consultation sought to collect views on the implementation of the NIS Directive and on the impact of potential future changes. It gave stakeholders an opportunity to inform the Commission on the state of the cybersecurity preparedness of companies and propose ways to further improve it.

The consultation period closed on 2 October 2020. The results of the consultation will be used for the evaluation and impact assessment of the NIS Directive. The Commission will likely adopt a new legislative initiative in respect of the NIS Directive, for example a proposal for a Directive, before the end of 2020.

The feedback received during the public consultation can be viewed here.

Further information on the Commission's review of the NIS Directive can be accessed here.

4. THE CENTRAL BANK OF IRELAND

4.1 The Central Bank publishes statement on use of electronic signatures

On 24 August 2020, the Central Bank of Ireland (**Central Bank**) published a statement on the use of electronic signatures in regulatory documents and forms, arising out of increased instance of remote working arising from the Covid-19 pandemic.

In its statement, the Central Bank confirms that, in the absence of any specific legal provisions to the contrary, regulated firms may use electronic signatures in submitting regulatory documents and forms to the Central Bank.

The Central Bank emphasised that those signing regulatory documents and forms in electronic form will be accountable for the content of the document in the same way as if they had signed the document in 'wet ink'.

The statement is available here.

4.2 Central Bank Act 1942 (Section 32D) Regulations 2020 [S.I. No. 345 of 2020]

On 4 September 2020, the Central Bank Act 1942 (Section 32D) Regulations 2020 (S.I. No. 345 of 2020) (**Regulations**) came into operation.

Each year, the Central Bank sets out the framework for that year's levying process and the basis on which the individual financial supervisory providers' levies will be calculated.

From 4 September 2020, all financial service providers are liable to pay an annual levy as specified in the Regulations. The Schedule to the Regulations prescribes the amount of the levy contribution and, where applicable, any supplementary levy contributions due in respect of each authorisation held during a relevant levy period.

A regulated entity is liable to pay the levy contribution prescribed whether or not a levy notice has been issued by the Central Bank.

In particular, at Category N, the Schedule address the amount of the levy contribution for Payment Institutions and E-Money Institutions.

The text of the Regulations can be accessed here.

5. ANTI-MONEY LAUNDERING (AML) AND COUNTERING THE FINANCING OF TERRORISM (CFT)

5.1 FATF publishes report on stablecoins

On 7 July 2020, the Financial Action Task Force (**FATF**) published a report to the G20 Finance Ministers and Central Bank Governors on so-called stablecoins.

The report sets out the FATF's analysis of the anti-money laundering (**AML**) and counter terrorist financing (**CFT**) issues relating to so-called stablecoins, particularly 'global stablecoins' (those with potential for mass-adoption). The report found that stablecoins share many of the same money-laundering and terrorist financing risks as some virtual assets. Features such as their potential for anonymity, global reach and layering of illicit funds present money-laundering and terrorist financing vulnerabilities.

The FATF confirmed that its revised standards on virtual assets apply to stablecoins, noting that a range of entities in any stablecoin arrangement will incur AML and CFT obligations under the revised standards, for example customer-facing exchanges and transfer services and custodial wallet providers, depending on the design of the stablecoin and what activities the entity undertakes.

The report addresses:

- what the characteristics of so-called stablecoins are (Section 1);
- what the money laundering and terrorist financing risks of stablecoins are (Sections 2 and 4);
- how the FATF Standards apply to stablecoins and the different businesses involved (Section 3); and
- how the FATF plans to enhance the global AML and CFT framework for virtual assets and so-called stablecoins (Section 5).

The report can be accessed here.

5.2 FATF publishes 12-month review of revised AML and CFT standards on virtual assets and VASPs

On 7 July 2020, the FATF published its 12 month review of the revised FATF standards on virtual assets and virtual asset service providers.

In June 2019, the FATF finalised its global Standards to place AML and CFT requirements on virtual assets and virtual asset service providers (**VASPs**).

In this review, the FATF measures the implementation of the revised Standards by jurisdictions and the private sector, as well as monitoring any changes in the typologies, risks and market structure of the virtual assets sector.

The review finds that, overall, both public and private sectors have made progress in implementing the revised FATF Standards. However, the review emphasises that while more than half of reporting jurisdictions have implemented the revised Standards, the effectiveness of the revised Standards is contingent on all jurisdictions implementing the standards, and the private sector implementing their obligations.

The review concludes that, at this point in time, there is no clear need to amend the revised FATF Standards, and the FATF undertook to continue its enhanced monitoring of virtual assets and VASPs.

The review can be accessed here.

5.3 EBA publishes response to the Commission call for advice on the future of EU AML and CFT framework

On 10 September 2020, the EBA published its response to the Commission's call for advice, issued 3 March 2020, on the future of the EU's AML and CFT framework. The response comprises an opinion together with a report.

In its response, the EBA recommends that the Commission establish a single rulebook to:

- harmonise the EU's legal framework where evidence suggests divergence of national rules, in particular with respect to CDD measures and AML/CFT systems and controls requirements that determine what financial institutions do to tackle money laundering and terrorist financing;
- strengthen the EU's legal framework where current provisions are insufficiently robust, particularly in relation to the powers AML/CFT supervisors have at their disposal to monitor and take the measures necessary to ensure financial institutions' compliance with their AML/CFT obligations and in relation to financial institutions' reporting requirements;
- review of the scope of the EU's AML/CFT legislation to ensure the list of obliged entities is sufficiently comprehensive and in line with international AML/CFT standards; and
- clarify provisions in sectoral financial services legislation to ensure that they are compatible with the EU's AML/CFT objectives.

The opinion, which gives a high-level overview of the EBA's advice, may be accessed here.

The report, which sets out the EBA's detailed response, may be accessed here.

5.4 FATF publishes report on Virtual Assets – Red Flag Indicators of Money Laundering and Terrorist Financing.

On 14 September 2020, the FATF published its report on 'Virtual Assets - Red Flag Indicators of Money Laundering and Terrorist Financing'.

In its report, the FATF warns that the distinct features of virtual assets and related services create new opportunities for money launderers, terrorist financiers and other criminals to launder their proceeds and finance their illicit activities by their ability to acquire and move assets digitally, often outside the regulated financial system, and obfuscate the origin or destination of the funds.

The report highlights the most important red flag indicators that could suggest whether virtual assets are being used for criminal activity. The report emphasises the existence of a single indicator is not necessarily a basis for suspicion of money laundering or terrorist financing, however the presence of one or more such indicators could prompt further monitoring and examination.

The report aims to facilitate reporting entities in identifying and reporting potential money laundering and terrorist financing activity involving virtual assets. The report can also assist reporting entities application of a risk-based approach to their customer due diligence (**CDD**) requirements.

Key indicators in this report focus on:

- Technological features that increase anonymity - such as the use of peer-to-peer exchanges websites, mixing or tumbling services or anonymity-enhanced cryptocurrencies;
- Geographical risks - criminals can exploit countries with weak, or absent, national measures for virtual assets;
- Transaction patterns - that are irregular, unusual or uncommon which can suggest criminal activity;
- Transaction size – if the amount and frequency has no logical business explanation;
- Sender or recipient profiles - unusual behaviour can suggest criminal activity; and
- Source of funds or wealth - which can relate to criminal activity.

The report can be accessed here.

5.5 Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Bill 2020

On 22 September 2020, the Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Bill 2020 (**Bill**) commenced Dáil Éireann, Second Stage. The purpose of the Bill is to transpose the criminal justice elements of the Fifth EU Anti-Money Laundering Directive (**AMLD 5**) by amending the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 in line with AMLD 5. The Bill seeks to:

- improve the safeguards for financial transactions to and from high-risk third countries;
- bring a number of new 'designated persons' under the existing legislation (notably virtual currency providers and custodian wallet providers);
- improve the transparency of beneficial ownership of legal entities. Where a designated person is entering a business relationship with another entity, the designated person must take steps to obtain the relevant information from the appropriate register of beneficial ownership prior to commencing the business relationship;
- provide for a new defence in relation to 'tipping off' where the designated person can prove that the entity to whom the information was disclosed was a specified financial institution, which is connected to the designated person or part of the same group structure;
- enhance existing CDD requirements;
- set new limits on the use of anonymous pre-paid cards. A person supplying such an instrument will now be required to conduct CDD when the value of the requested card is €150 or higher;
- broaden the definition of a politically exposed person (**PEP**) to include 'any individual performing a prescribed function';
- provide for Ministerial guidance which will clarify domestic 'prominent public functions' that will give rise to a person being designated as a PEP; and
- make a number of technical amendments to other provisions of Acts already in force.

The Bill's progress can be tracked here.

6. DATA PROTECTION

6.1 Implications of Schrems II Ruling

On 16 July 2020, the CJEU published its much anticipated ruling in the Schrems II case1 in which it considered whether the transfer of personal data by Facebook Ireland to Facebook Inc, which is located in the U.S., under the EU-U.S. Privacy Shield or through the use of standard common contractual clauses (**SCC**) was permissible.

The CJEU ruled that: (i) the Privacy Shield was no longer a valid mechanism by which to transfer personal data to the US on the basis that it did not ensure EEA data subjects the same protections they are afforded under Regulation (EU) 2016/679 (**General Data Protection Regulation** or **GDPR**); and (ii) although the SCC remained valid, upon assessment of the data controller, *'supplementary measures'* may be required to ensure that the adequate level of protection is given to data subjects.

The ruling has significant implications for personal data transfers between EEA member states and third countries whose data protection regimes have not yet been assessed by the Commission as offering an equivalent level of protection to data subjects. Notably, the United Kingdom (**UK**) will become a 'third country' for data protection purposes on 31 December 2020.

6.2 Data Protection Commission statement on Schrems II ruling

On 16 July 2020, the Data Protection Commissioner (**DPC**) published its response strongly welcoming the Schrems II ruling. The DPC's case was that data transfers between the EU and the USA were highly problematic in light of the Court of Justice of the EU's (**CJEU**) decision in the Safeharbour case of 2015 and the structure of the US legal system.

The DPC indicated that it had brought these proceedings, and resisted objections from both Facebook and Mr Schrems, *"specifically in order to secure a decisive statement of position from the CJEU in relation to the key issues of principle at stake when an EU citizen's personal data is transferred to the United States"*.

The DPC indicates that the CJEU's decision in the Schrems II case endorses *"the substance of the concerns expressed by the DPC (and by the Irish High Court) to the effect that EU citizens do not enjoy the level of protection demanded by EU law when their data is transferred to the United States"*. The DPC also indicates that whilst the SCCs transfer mechanism used to transfer data to countries worldwide is, in principle, valid, *"it is clear that, in practice, the application of the SCCs transfer mechanism to transfers of personal data to the United States is now questionable"*.

The DPC also welcomes the clarity provided by this judgment with regard to the allocation of responsibility between data controllers and NSAs. The DPC looks forward to cooperating with its fellow EU supervisory authorities in giving effect to this judgment.

The DPC statement can be accessed here.

6.3 Frequently Asked Questions on the Schrems II case

On 23 July 2020, following the ruling in the Schrems II case, the European Data Protection Board (**EDPB**) published a Frequently Asked Questions (**FAQ**) document. In this FAQ, the EDPB confirmed that the Privacy Shield was invalidated with immediate effect. Therefore data exporters which relied on the Privacy Shield as a legitimate means of transferring personal data from the EEA to the U.S. will need to consider an alternative mechanism for any future transfers.

The EDPB FAQ can be accessed here.

The decision of the CJEU is available here and the press release of the CJEU, here.

1 Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems

6.4 Guidance for Data Controllers who Lose Control of Data to a Third Party

On 27 August 2020, the DPC published guidance on its website highlighting the steps that should be taken by data controllers in the event of the loss of control to third parties.

The GDPR and the Data Protection Act 2018 are the primary pieces of legislation governing the control of data and list the responsibilities of data controllers. In a situation where personal data is revealed to a third party, the possibility of that party retaining this information could be damaging to the data subject.

In most scenarios, the third party will return or dispose of the personal data upon request but where this is not the case, the data controller is responsible for rectifying the situation. The breach and all relevant information should be reported to the DPC and the following steps are recommended:

- Advise the third party that retention of this data is unlawful;
- If necessary, contact An Garda Síochána; and
- Consult with legal advisers regarding possible remedies, including injunctions.

The guidance can be accessed here.

6.5 EDPB adopts guidelines on the concepts of controller and processor in the GDPR

On 2 September 2020, the EDPB adopted guidelines entitled *'Guidelines 07/2020 on the concepts of controller and processor in the GDPR'* (**Guidelines**).

The Guidelines seek to provide guidance on the concepts of controller and processor by clarifying the meaning of these concepts and clarifying the different roles and the distribution of responsibilities between these actors. The Guidelines specifically address the extent to which the GDPR brought changes to these concepts, including the implications of joint controllership under Article 26 GDPR and the relationship between controller and processor under Article 28 GDPR.

The Guidelines replace the previously issued Article 29 Working Party guidance on these concepts (Opinion 1/2010 (WP169)). The new Guidelines aim to give more developed and specific guidance in order to ensure consistent application of the rules throughout the EEA.

The EDPB is now seeking feedback on the Guidelines in the form of a public consultation. The closing date for receipt of comments is October 19 2020.

The Guidelines are available here, and the public consultation can be accessed here

6.6 EBF publishes response to EDPB on the Guidelines on the interplay of PSD2 and the GDPR

On 16 September 2020, the European Banking Federation (**EBF**) published its response to the EDPB consultation on the Guidelines on the interplay of PSD2 and the GDPR.

The EBF welcomed the EDPB's efforts to clarify uncertainties that existed between the two legislative frameworks. In their response, the EBF advised:

- that the EDP Guidelines should ensure coherence with existing legislation and should not result in new technical measures;

- a clear distinction should be made between the GDPR responsibilities for each of the payment service providers, based on the roles described in PSD2;

- the Guidelines should recognise that Article 9(2)(g) GDPR provides a legal basis for the processing of special categories of personal data for account servicing payment service providers (**ASPSP**), payment initiation service provider (**PISP**) and account information service provider (**AISP**);

- on further processing under PSD2, the Guidance should be amended to clarify that AISPs and PISPs can process personal data relating to payments on other Article 6 bases, provided this is linked to the provision of core account information service (**AIS**) and payment initiation service (**PIS**), and subject to meeting other GDPR requirements; and

- the Guidelines should take into account that it is the responsibility of each payment service provider (**PSP**), as the data controller, to respect the principal of data minimisation, particularly with respect to the recommendation on digital filters.

The EBF response can be accessed here.

7. COVID – 19

7.1 Companies (Miscellaneous Provisions) (COVID-19) Act 2020

The Companies (Miscellaneous Provisions) (COVID-19) Act 2020 (**Act**) was signed into law on 1 August 2020. The Act provides relief to companies which have faced difficulties in complying with certain statutory requirements as a result of the COVID-19 pandemic by way of temporary amendments to the Companies Act 2014.

Please see Dillon Eustace's briefing concerning the temporary amendments made with effect on 21 August 2020 to the Companies Act 2014 by the Act. A copy of the Dillon Eustace briefing can be accessed here.

8. BREXIT

8.1 The Commission published a stakeholder preparedness notice on readiness at the end of the transition period for the electronic commerce and payment services industry

During the period 1 July 2020 to 30 September 2020, the Commission published an updated stakeholder preparedness notice for the electronic commerce industry and for the payment services industry on readiness at the end of the transition period.

In the notices, the Commission reminded these industries of the need to take appropriate action in good time ahead of the UK's transition period, coming to an end on 31 December 2020. The Commission has also updated its webpage on getting ready for the end of the Brexit transition.

The updated notice can be accessed here.

If you have any questions in relation to the content of this update, to request copies of our most recent newsletters, briefings or articles, or if you wish to be included on our mailing list going forward, please contact any of the team members below.

Keith Waine
E-mail: keith.waine@dilloneustace.ie
Tel : + 353 1 673 1822
Fax: + 353 1 667 0042

Karen Jennings
E-mail: karen.jennings@dilloneustace.ie
Tel : + 353 1 673 1810
Fax: + 353 1 667 0042

Enda McGeever
E-mail: enda.mcgeever@dilloneustace.ie
Tel : + 353 1 673 1751
Fax: + 353 1 667 0042

Seán Mahon
E-mail: sean.mahon@dilloneustace.ie
Tel : + 353 1 673 1707
Fax: + 353 1 667 0042

DISCLAIMER:

This document is for information purposes only and does not purport to represent legal advice. If you have any queries or would like further information relating to any of the above matters, please refer to the contacts above or your usual contact in Dillon Eustace.