ICLG

The International Comparative Legal Guide to:

Fintech 2018

2nd Edition

A practical cross-border insight into Fintech law

Published by Global Legal Group, with contributions from:

A&L Goodbody
Advokatfirmaet BAHR AS
Anderson Mōri & Tomotsune
Anjarwalla & Khanna
Appleby
ATZ Law Chambers
Bär & Karrer Ltd.
BBA
BonelliErede
Bonn Steichen & Partners
Bredin Prat
De Brauw Blackstone Westbroek
ENSafrica
Erciyas Law Office
Etah-Nan & Co, Attorneys
Evris Law Firm
Galicia Abogados, S.C.
Gilbert + Tobin
Gleiss Lutz
Goldfarb Seligman & Co.
Gorrissen Federspiel
GVZH Advocates
Haiwen & Partners
ISOLAS LLP
Kim & Chang
Lee and Li, Attorneys-at-Law
Mannheimer Swartling
Mattos Filho, Veiga Filho, Marrey Jr e Quiroga Advogados
McMillan LLP
MinterEllisonRuddWatts
QUORUS GmbH
Rahayu and Partners Law Offices in Association with HFW
Romulo
Roschier, Attorneys Ltd.
Shearman & Sterling LLP
Shearn Delamore & Co.
Shook Lin & Bok LLP
Slaughter and May
Trilegal
Udo Udoma & Belo-Osagie
Uría Menéndez
Uría Menéndez – Proença de Carvalho
Wilmer Cutler Pickering Hale and Dorr LLP
WKB Wierciński, Kwieciński, Baehr
Yale Law School

glg
global legal group

Ireland

Claire Morrissey

Peter Walker

A&L Goodbody

1 The Fintech Landscape

1.1 Please describe the types of fintech businesses that are active in your jurisdiction and any notable fintech innovation trends of the past year within particular sub-sectors (e.g. payments, asset management, peer-to-peer lending or investment, insurance and blockchain applications).

Dublin is now a "*booming FinTech hub*". Change in the financial services sector in Ireland is being driven by digitalisation in consumer banking and disruptive technology. New entrants to this sector are developing innovative business models that are testing the parameters of the current financial services framework. These include services relating to electronic money, intermediation of payments and payment channels, the aggregation of financial services data, raising capital through peer-to-peer platforms and crowdfunding, financial cybersecurity, the facilitation of price comparisons in connection with retail financial products, and the emergence of blockchain technology. In recent years we have seen particular disruption in the payments sector with established institutions being bypassed through the use of technology-driven payment processes such as PayPal, Stripe and TransferMate. Notable trends of the past year include innovation in integrated payment services, use of contactless technology, alternative credit models, use of non-traditional data sources and the emergence of data analytics and automated processing being used to price risks and reduce operating costs. The Payment Services Regulations 2018 which came into force in January of this year, and lowered the barrier of entry for third-party service providers and fintechs into the payment services market. It is also likely to bring new fintech business models and innovation in the area of open banking in the year ahead as these businesses capitalise on the new opportunities.

1.2 Are there any types of fintech business that are at present prohibited or restricted in your jurisdiction? (for example cryptocurrency-based businesses)?

There are no prohibitions or restrictions that are specific to fintech or cryptocurrency-based businesses in Ireland. However, these businesses may fall under the regulatory frameworks addressed in question 3.1 below.

2 Funding For Fintech

2.1 Broadly, what types of funding are available for new and growing businesses in your jurisdiction (covering both equity and debt)?

Equity

Venture capital firms and private equity investors continue to focus on high-potential fintech businesses. The Irish Venture Capital Association recently reported that fintech companies raised over €144 million in the first three quarters of 2017. Irish financial services organisations have set up venture funds and a number of fintech incubation and acceleration projects which offer funding in return for an equity percentage (see our answer to question 2.2).

Debt

In addition to traditional lending from financial institutions for small and medium businesses, there are increasing funding options available for fintech businesses in Ireland. Online financing platforms, crowdfunding and peer-to-peer lending platforms are often used in combination with more traditional sources of funding. Peer-to-peer lending is beginning to gain pace through platforms such as LinkedFinance and Grid Finance. The speed at which funds can be raised makes this a particularly attractive option.

2.2 Are there any special incentive schemes for investment in tech/fintech businesses, or in small/medium-sized businesses more generally, in your jurisdiction, e.g. tax incentive schemes for enterprise investment or venture capital investment?

The attractively low corporate tax rate in Ireland of 12.5% in respect of trading profits is a major incentive for start-ups or companies looking for a location for their business investments. Some other attractive features of Ireland's tax code for relevant companies include the R&D tax credit regime, the stamp duty exemption available on the transfer of a wide range of IP, the key employee reward mechanism, Ireland's Double Taxation Agreement network (currently 73 agreements signed and in effect) and the potential 6.25% tax rate under Ireland's Knowledge Development Box on profits arising from certain IP assets which are created as a result of qualifying R&D activity carried out in Ireland or the European Economic Area (the **EEA**).

Enterprise Ireland (the state agency responsible for supporting the development of manufacturing and internationally traded services companies) offers a number of supports:

- **Competitive Start Fund (CSF)**: This fund offers €50,000 equity investment in return for a 10% equity stake. Calls are made throughout the year for specific sectors, and in June 2017, a specific fintech CSF was announced which was open to companies in payments, banking, regtech, security, insurtech and other fintech solutions leveraging blockchain, the internet of things, artificial intelligence and data intelligence.
- **Innovative High Potential Start-Up (HPSU) Fund**: Enterprise Ireland offers equity investment to HPSU clients on a co-funded basis (similar to a venture capital approach). The funding goes towards the achievement of an overall business plan, rather than funding towards discrete elements of a business plan, such as R&D or employment creation.

Other Government-backed schemes include:

- **StartUP Refunds for Entrepreneurs (SURE)**: an initiative which allows individuals to obtain a refund from the Government of up to 41% of the capital they invest in establishing their own company over a six-year period; and
- **Employment and Investment Incentive (EII) Scheme**: a scheme which allows individual investors to claim tax relief of up to 40% on investments they make in other companies. The EII scheme is available to unquoted micro, small and medium-sized trading companies, subject to certain exceptions.

2.3 In brief, what conditions need to be satisfied for a business to IPO in your jurisdiction?

The first step in an Irish IPO is to decide which market to list in and this essentially depends on the scale of the business and the funding required by the company. The precise listing rules differ in respect of different markets. The Irish Stock Exchanges (**ISE**) offers four markets: the Main Securities Market (**MSM**), which is suited to large companies and requires a minimum of 25% of its shares to be placed in the public and requires a three-year trading record; the Enterprise Securities Market (**ESM**), which suits smaller companies (minimum market capitalisation of €5,000,000) in the early stages as no trading record is required; the Global Exchange Market (**GEM**), which is a specialist debt market; and finally, the Atlantic Securities Market (**ASM**), which is a market dedicated to companies who wish to dual list in both the EU and the US.

General requirements for listing securities on the MSM (the principal market in Ireland) include the following:

- an issuer must be duly incorporated or otherwise validly established and operating in conformity with its constitutional document;
- securities must conform with applicable laws of the place of incorporation and be duly authorised;
- securities must be freely transferable; however, the ISE may permit securities that are partly paid if there is no restriction;
- the expected aggregate market value of all securities must be at least €1,000,000 for shares and €200,000 for debt securities;
- the whole class of securities must be listed; and
- an approved prospectus must be published for the securities.

2.4 Have there been any notable exits (sale of business or IPO) by the founders of fintech businesses in your jurisdiction?

Examples of notable exits include:

- the founder of Realex Payments, an Irish online payment technology, exiting the business in 2015 following a €115 million acquisition by US company Global Payments; and
- the Irish financial compliance solutions company Kyckr listing on the Australian stock exchange in October 2016.

It is expected that 2018 will see increased M&A activity within the fintech space. In particular, consolidation within the emerging payment and regulatory solutions sector is anticipated.

3 Fintech Regulation

3.1 Please briefly describe the regulatory framework(s) for fintech businesses operating in your jurisdiction, and the type of fintech activities that are regulated.

Ireland does not have a specific regulatory framework for fintech businesses. In some cases, fintech businesses will fall outside of the regulatory ambit as they do not involve the provision of services or undertaking of activities which fall within a regulated activity (as defined in legislation). However, fintech businesses providing regulated activities (as defined in legislation) which cannot avail of an exemption will fall within the existing body of financial regulation and so require prior authorisation from the Central Bank of Ireland (**CBI**) to conduct business. If authorised, the firms will be subject to Irish legislation and various ongoing CBI requirements.

Payment institutions, electronic money institutions (**EMIs**), investment companies, money transmission businesses and payment initiation and account information service providers are examples of business models which may require authorisation. The legislation which is most likely to apply to fintech businesses is the Electronic Money Regulations 2011, which authorises an undertaking to issue E-money and the Payment Services Regulations 2018, which governs payment institutions and third-party payment services providers providing payment initiation and account information services.

Fintech business may also be subject to consumer protection legislation, the CBI codes of conduct including the Consumer Protection Code, as well as anti-money laundering and data protection legislation, depending on the services that they are offering.

3.2 Are financial regulators and policy-makers in your jurisdiction receptive to fintech innovation and technology-driven new entrants to regulated financial services markets, and if so how is this manifested?

The CBI is becoming increasingly aware of the positive impact financial services can have on a country as a whole and the regulatory environment surrounding this area is therefore positive. The CBI encourages fintech development, but does recognise and warn against the potential to blur lines between regulated and

unregulated activities and the challenges this may present. The CBI has sought to develop a clearer picture of fintech activity in Ireland with a view to better understanding the implications for regulatory policy and supervisory activity. It has identified a number of areas, including payments, regtech, markets and exchanges, deposits and lending, investment and advice, insurance, analytics, capital raising and the start-up support ecosystem. The CBI continues to review the sector and is closely following and actively contributing to the European Supervisory Authority's approach to fintech.

The CBI's focus is on the risks to consumers from fintech developments and on protecting consumers where activity is not yet regulated. In its 2017 Consumer Protection Outlook Report, the CBI observed that in line with the increasing use of technology in the delivery of financial products and services, the need for focus on the consumer and delivering fair consumer outcomes through sound product oversight and governance arrangements as new products and services are being developed and rolled out is critical. The CBI's Director of Consumer Protection has recently said that "*there is an exciting opportunity for Fintech firms to contribute in a positive way to protecting consumers and enabling greater access and availability of financial products and services*".

In June 2017, the CBI published a Discussion Paper which sought feedback on a number of specific points aimed to inform the CBI's view of whether the Consumer Protection Code adequately protects consumers in the environment of the digitisation of financial services. Within the Discussion Paper, the CBI noted its intention to bring a consultation paper in 2018 if it determined to advance any specific policy proposals as a result of that feedback.

In 2015, the Irish Government launched its strategy for Ireland's International Financial Services Sector for the following five years (**IFS2020**), which seeks to consolidate and grow Ireland's position as the global location of choice for specialist international financial services. A key element of this strategy is the recognition and promotion of fintech as a rapidly expanding area of innovative financial services. To this end, the Irish Government Industrial Development Authority (**IDA**) is working with its clients to determine what role Ireland can play as they plan their future technology requirements. Furthermore, the start-up rate for Irish-owned fintech companies is accelerating rapidly, and in 2017, Enterprise Ireland launched its competitive start-up fund which aims to support early stage companies active in the fintech sector.

IFS2020 aims to develop and maintain an effective ecosystem which addresses the needs of start-ups and scaling companies in terms of funding, skills, mentors, accelerators, an innovation-friendly regulatory environment, and access to key markets, while at the same time addressing the needs of foreign-owned international financial services (**IFS**) companies. A key strategy objective is facilitating the collaboration between large IFS companies and the indigenous base to create disruptive solutions based on innovative products and services. Multinational corporations (**MNCs**) in Ireland will be able to access products and services from a growing cluster of indigenous start-up firms in software, payments, peer-to-peer and analytics, all of which are looking to revolutionise the way technology is used in financial services.

IFS2020 has identified three key actions to be implemented over the course of the strategy in relation to fintech: enhancing IFS and information and communications technology (**ICT**) through sectoral collaboration while engaging both Irish-owned and foreign-owned SMEs and MNCs; sourcing funding for fintech; and supporting fintech accelerators through partnership with Enterprise Ireland, for example, the Accenture fintech Innovation Lab which is now in its fourth year. IFS2020 has also led to the publication of a yearly action plan in line with the overall strategy in order to execute its particular goals each year.

The IDA, Enterprise Ireland, the CBI and the Department of Finance participate in a working group coordinated by the Fintech & Payment Association of Ireland. The group also includes industry stakeholders and has recently published a strategy report on the future for Ireland's Fintech industry (available at https://fpai.ie/downloads/FPAI_FinTech_Report.pdf).

3.3 What, if any, regulatory hurdles must fintech businesses (or financial services businesses offering fintech products and services) which are established outside your jurisdiction overcome in order to access new customers in your jurisdiction?

A fintech business wishing to provide regulated services in Ireland, regardless of whether the business is based in Ireland or not, must either obtain authorisation from the CBI, avail of an exemption or "passport" into Ireland from another EU Member State.

- Firms wishing to establish a regulated fintech business in Ireland must engage in the CBI's authorisation process. The CBI's key principle is that the firm's "heart and mind" must be in Ireland, as shown by the firm having its principal place of business in Ireland, sufficient senior management presence and demonstrating a high level of decision-making. It is expected that key leadership positions will operate from Ireland, including roles such as chief executive, head of finance, head of operations and head of compliance. A board of directors should meet in Ireland quarterly. A business must have at least two directors, one of whom is an EU resident. The CBI will require at least one independent non-executive director and such role is often filled by an Irish resident. There is no set minimum number of staff – headcount will be driven by the levels of business activity planned and is to be discussed with the regulator. Outsourcing arrangements are permitted but must be documented in clear legal agreements.
- The CBI also requires firms applying for authorisation to be adequately capitalised. The amount will vary depending on the precise nature and scope of services in respect of which authorisation is required. Finally, the CBI will require the applicant to submit a business plan and summary details of all the key policies, processes and procedures which will be put in place in the new business, including detailed anti-money laundering policies.
- Various exemptions apply to the performance of regulated services. These exemptions can be general or apply to a specific area.
- Alternatively, a fintech business authorised to provide regulated services in another EU Member State can notify the CBI (via its home stake regulator) that it intends to rely on the EU "passporting" regime to provide those activities in Ireland.

4 Other Regulatory Regimes / Non-Financial Regulation

4.1 Does your jurisdiction regulate the collection/use/transmission of personal data, and if yes, what is the legal basis for such regulation and how does this apply to fintech businesses operating in your jurisdiction?

The Data Protection Acts 1988 and 2003 (**DPA**) govern the control and processing of personal data in Ireland. The DPA implement

the EU Data Protection Directive 95/46/EC. The DPA regulate the processing of personal data and apply to data controllers if (i) they are established (e.g. as a body incorporated, branch or agency) in Ireland and process in the context of that establishment, or (ii) the data controller is neither established in Ireland or the EEA but makes use of equipment in Ireland for processing data.

In addition, the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (S.I. 336 of 2011) which implement Directive 2002/58/EC (as amended by Directive 2006/24/EC and 2009/136/EC) (the **ePrivacy Regulations**) deal with data protection issues in relation to phone, email, SMS and internet use and will generally apply to data controllers which fall within the scope of the DPA. The ePrivacy Regulations will likely be repealed when the European Commission's proposed Regulation on Privacy and Electronic Communications is passed.

General Data Protection Regulation 2016/679 (GDPR)

The DPA will be superseded by the GDPR from 25 May 2018. The GDPR, as a regulation, will be directly applicable in Ireland and will broadly not require national implementing measures. However, the General Scheme of the Data Protection Bill (the **Data Protection Bill**) which is expected to come into force in the coming months is designed to give effect to, and provide derogations from, the GDPR under Irish law. A notable derogation is that the digital age of consent in Ireland will be set at 13.

The Data Protection Bill includes a mechanism for fines imposed by the Office of the Data Protection Commission (**ODPC**) under the GDPR to be confirmed by a court. The profile and influence of the ODPC will increase under the GDPR as it is expected to become the lead data protection regulator for many of the world's largest multinational tech companies under the GDPR's one-stop-shop mechanism.

4.2 Do your data privacy laws apply to organisations established outside of your jurisdiction? Do your data privacy laws restrict international transfers of data?

Yes to both questions.

The DPA apply to organisations not established in the EEA that use equipment to process personal data in Ireland. The GDPR goes further, and will apply to data controllers and processors outside the EEA who offer goods and services to, or monitor, EEA residents.

The DPA restrict the transfer of personal data to countries outside the EEA unless the third country provides an adequate level of protection for the privacy of an individual. Accessing personal data from a third country amounts to transferring the personal data outside the EEA. Businesses wishing to transfer personal data outside the EEA must invoke one or more of the factors that legitimise transfers outside the EEA. The options include:

- the use of legally enforceable privacy/data protection codes of practice ("**binding corporate rules**") by MNCs;
- Privacy Shield (for transfers to the US): a standard by which US companies can self-certify the adequacy of their data protection measures; or
- Model Clauses: Irish data controllers may put in place EU-approved contractual provisions (known as Model Clauses). The validity of the Model Clauses is currently being questioned in the context of the ODPC's application to the Irish High Court to make a reference to the Court of Justice of the European Union as to the validity of this mechanism (*Data Protection Commissioner v. Facebook Ireland Limited & Maximillian Schrems Record Number 2016/4809P*). For the time being, however, the Model Clauses remain valid for data transfers outside the EEA.

Data transfers to countries outside the EEA will continue to be prohibited under the GDPR unless that country ensures an adequate level of protection. The GDPR will retain the existing transfer mechanisms set out above and will provide for additional mechanisms, including approved codes of conduct and certification mechanisms, together with binding and enforceable commitments of the data controller or processor in the non-EEA country to apply the appropriate safeguards.

4.3 Please briefly describe the sanctions that apply for failing to comply with your data privacy laws.

Regulatory Action

The ODPC is responsible for the enforcement of the DPA and the e-Privacy Regulations. The ODPC has a proactive approach to identifying data protection issues and regularly engages with public and private sector organisations on these issues. The ODPC has, for example, a specific unit which focuses on issues that arise for Irish-based tech multinationals.

Under the DPA, the ODPC has no power to issue administrative fines but has broad investigative and enforcement powers including the power to:

- carry out announced and/or on the spot audits;
- compel compliance with the DPA, require the deletion of data and/or prohibit the transfer of personal data from the State; and
- prosecute – the ODPC has actively pursued prosecutions in respect of electronic marketing in recent years.

Criminal liability can arise for breach of specific provisions of the DPA. These include: (i) failure of a data controller or data processor to register; (ii) disclosure of personal data which was obtained without authority; and (iii) failure to comply with an enforcement notice. Persons found guilty of these offences under the DPA may be liable on summary conviction (before a district judge sitting alone) to a fine not exceeding €4,000; or on conviction on indictment (before a judge and jury) to a fine not exceeding €100,000. The e-Privacy Regulations also prescribe criminal liability for failure to report data breaches, inadequate security measures and sending of unsolicited communications (spam) with regard to electronic communication networks and services.

Under the GDPR, there is potential for the imposition of significant administrative fines on data controllers and processors for non-compliance. Two maximum thresholds for fines are provided for under the GDPR, which apply depending on which data protection obligation has been breached. Businesses may face administrative fines of up to: (a) €10m or 2% of the total worldwide annual turnover of the preceding financial year; or (b) €20 million or 4% of the total worldwide annual turnover of the preceding financial year. Fines can be imposed in addition to, or instead of, any corrective measures such as reprimands or warnings.

Damages

Damages may be recovered by a data subject for a breach of their data protection rights. In order for a data subject to be awarded compensation, it must be shown that the data subject suffered loss or damage arising from the breach. To date, the Irish courts have held that actual damage must be proved and damages for distress are not recoverable unless extreme distress results in actual damage, such as a recognisable psychiatric injury. Under the GDPR, however, data subjects can sue both data controllers and processors for compensation for pecuniary and non-pecuniary damage suffered as a result of a breach.

4.4 Does your jurisdiction have cyber security laws or regulations that may apply to fintech businesses operating in your jurisdiction?

The obvious growth in the fintech sector, while considered to be mainly positive, also increases the need for regulation to avoid the abuse of online financial payments.

- **Data Protection Legislation**: The DPA require data controllers and data processors to take "appropriate security measures" to protect personal data and to ensure that staff and "other persons at the place of work" are aware of, and comply with, security measures. The GDPR contains enhanced security measures, and will require data controllers and data processors to implement "appropriate technical and organisational measures" to ensure a level of security appropriate to the risks that are presented by the processing of the data. These measures, where appropriate, should include: (i) pseudonymisation and encryption of the data; (ii) integrity and resilience of processing systems; (iii) the ability to restore availability and access in the event of a physical or technical incident; and (iv) regular testing of security measures.
- **Payment Services Regulations**: The Payment Services Regulations 2018 which came into force 13 January 2018 enhance regulation in this area by: (i) increasing reporting obligations applicable to providers offering payment services; (ii) applying new authorisation requirements for providers offering payment services (payment initiation and account information service providers now require authorisation); and (iii) requiring that all remote and online payment transactions meet strong customer authentication requirements. The issue of strong customer authentication will also be subject to regulatory technical standards that will be published by the European Banking Authority and will come into effect 18 months after entry into force.
- **Criminal Law**: It is an offence under the DPA to access or obtain and disclose to another person personal data without the prior authority of the data controller or data processor. The Criminal Damage Act creates two basic computer crime offences: that of causing criminal damage to a computer; and that of unauthorised access. The unlawful operation of a computer with the intent of making gain is a criminal offence under the Criminal Justice (Theft and Fraud) Offences Act 2001.
- **Duty of Care**: A duty of care may arise in relation to data compromised during a cybersecurity incident. Both data controllers and processors owe individuals whose data they process an express statutory duty of care under the DPA. As such, they may be subject to a claim for damages where a cybersecurity incident arises in connection with a breach of that duty.
- **Regulatory Guidance**: In June 2015, guidance on internet payments and the necessary security required were published by the European Banking Authority (the **EBA**) and, subject to the EBA's PSD2 regulatory technical standards coming into effect, the CBI would expect any authorised firms to comply with these. Fintech businesses regulated by the CBI need to comply with the CBI's 2016 cross-industry guidance in respect of IT and cybersecurity risks (available at: https://centralbank.ie/docs/default-source/Regulation/how-we-regulate/policy/cross-industry-guidance-information-technology-cybersecurity-risks.pdf?sfvrsn=2).
- **Cybercrime**: The Criminal Justice (Offences relating to Information Systems) Act 2017 came into force on 12 June 2017. The Act creates a number of new cybercrime offences including unauthorised access of information systems (e.g. hacking), interference with information systems or data and use of tools to facilitate commission of these offences.
- **Proposed Legislation**: The EU's Network and Information Systems Directive sets out legal measures to boost the overall level of cybersecurity in the EU, including imposing security requirements and incident notification obligations on banks and other "operators of essential services" together with certain digital service providers. This Directive must be enacted into Irish law by 10 May 2018.

An organisation which suffers a data security incident may also be subject to a number of separate incident notification obligations including under financial and payment services regulations, data protection and/or information security regulations.

4.5 Please describe any AML and other financial crime requirements that may apply to fintech businesses in your jurisdiction.

Ireland's key anti-money laundering and terrorist financing legislation is the Criminal Justice Act 2010 (**CJA 2010**). Designated persons under the CJA 2010, including all financial institutions authorised by the CBI or businesses conducting certain activities, have statutory obligations to comply with the CJA's 2010 provisions. The CJA 2010 involves a combination of risk-based and rules-based approaches to the prevention of money laundering and terrorist financing. Designated persons must apply customer due diligence, report suspicious transactions and have specific procedures in place to prevent money laundering and terrorist financing. Failure to comply with the CJA 2010 is an offence.

At the time of publication, similar to other EU Member States, Ireland had not implemented the EU Fourth Anti-Money Laundering Directive. Once implemented, it is likely that the new regime will be more prescriptive than is presently the case, and a more detailed analysis and evaluation of the risks of a business from this AML perspective may be required.

Bribery and corruption are criminalised in Ireland under the Prevention of Corruption Acts 1889 to 2010. However, there are weaknesses in the legislation which have sometimes made it difficult to enforce. Revised legislation is expected to be introduced shortly.

4.6 Are there any other regulatory regimes that may apply to fintech businesses operating in your jurisdiction?

There is no fintech-specific regulatory regime in Ireland. The applicable regimes and legislation are described above. Any other applicable regulatory regimes would probably be specific to the sector in which a particular fintech business operates.

5 Accessing Talent

5.1 In broad terms, what is the legal framework around the hiring and dismissal of staff in your jurisdiction? Are there any particularly onerous requirements or restrictions that are frequently encountered by businesses?

Hiring and Recruitment

Employers must comply with equality legislation not only in the context of existing employees, but also in all aspects of recruitment, including job advertisements and candidate selection. Employers must ensure that in advertising and interviewing for a particular position they do not give rise to an inference of discrimination on one of the nine protected grounds (gender, civil status, family status,

sexual orientation, religion, race, age, disability, or membership of the traveller community). The maximum compensation available to non-employees who bring a claim in relation to a job application is €13,000.

Dismissing Staff

The Unfair Dismissals Acts 1977 to 2015 (the **UD Acts**) govern the dismissal of staff. The UD Acts provide that every dismissal is deemed to be unfair unless it is based on one of six fair grounds for dismissal:

- capability;
- conduct;
- qualification;
- redundancy of the role;
- competence of the employee;
- statutory prohibition; or
- some other substantial reason justifying dismissal.

The UD Acts provide that the onus is on employers to show the following: (i) substantial grounds justifying the dismissal based on one of the grounds set out above; and (ii) that fair procedures were followed in effecting the dismissal. The extent of fair procedures to be followed will depend on the circumstances and the reason for effecting the dismissal. The UD Acts apply to employees who have obtained one years' service (there are limited exceptions to the one years' service rule). Employees may also bring a claim for discriminatory dismissal under the Employment Equality Acts 1998 to 2015 (the **EE Acts**) where their dismissal is connected with one of the nine protected grounds listed above but they have not obtained the requisite one years' service to bring a claim under the UD Acts.

The maximum compensation available under the UD Acts (and the EE Acts for discriminatory dismissal) is: (i) two years' remuneration (five years' remuneration in the case of dismissal resulting from the making of a protected disclosure); (ii) re-engagement; or (iii) re-instatement.

Redundancy

In a redundancy situation, fair procedures require employers to consult with employees on the proposal prior to the decision to go ahead with the change with a view to looking for alternatives to the redundancy.

Irish law entitles employees (with over two years' service) to a statutory redundancy payment which is tax-free. It is calculated on the basis of two weeks' pay per year of service, plus a bonus week, and a week's pay is capped at €600 per week. It is the practice in many redundancies for the employer to make a severance payment greater than the statutory level to the employees.

Employers also have certain statutory obligations in respect of consultation when effecting a collective redundancy. A collective redundancy will arise where an employer dismisses a specified number of employees within a 30 day consecutive period.

Notice Period

Employees are entitled to certain minimum statutory notice periods depending on length of service. An employee who does not receive this notice period may bring a claim for wrongful dismissal and loss of earnings during the notice period.

5.2 What, if any, mandatory employment benefits must be provided to staff?

Under Irish law, an employer can engage employees on such terms as it deems appropriate provided the following mandatory benefits are protected:

- **Annual Leave**: the statutory minimum annual leave entitlement for full time employees is four working weeks.
- **Rates of Pay**: the minimum wage for employees in Ireland is €9.55 per hour. However, this rate may vary in certain sectors of employment.
- **Pension**: an employer in Ireland is not required to contribute to a pension for an employee; however, it is required to provide their employees with access to a pension scheme.
- **Protected Leave**: Ireland has the following protected leaves:

Leave	Entitlement	Obligation to Pay
Maternity Leave	Up to 42 weeks (26 weeks' basic leave (paid by the State) and 16 weeks' unpaid leave).	No obligation to pay. However, many employers pay the basic 26 weeks' entitlement to employees.
Adoptive Leave	Up to 40 weeks (24 weeks' basic leave (paid by the State) and an additional 16 weeks' unpaid leave).	No obligation to pay. However, many employers pay the basic 24 weeks' entitlement to employees.
Paternity Leave	Up to two weeks' leave (paid by the State).	No obligation to pay. However, many employers pay the entitlement to employees.
Carer's Leave	Up to a maximum of 104 weeks' unpaid leave.	No obligation to pay.
Parental Leave	18 weeks' unpaid leave per child.	No obligation to pay.

5.3 What, if any, hurdles must businesses overcome to bring employees from outside your jurisdiction into your jurisdiction? Is there a special route for obtaining permission for individuals who wish to work for fintech businesses?

All EEA nationals have the right to work in Ireland. Non-EEA nationals must have a valid employment permit in order to work in the State. Permits are administered by the Employment Permit Section of the Department of Business, Enterprise and Innovation.

Special route for obtaining permission for individuals who work for fintech businesses:

As part of a highly skilled workforce, many employees in the fintech industry can apply for a Critical Skills Employment Permit. In order to be eligible for such permits the employee must have:

- a job offer of at least two years within the State; and
- an annual salary of €60,000 or more.

Jobs with annual salaries of €30,000 or more may also be eligible provided they are one of the occupations listed on the Highly Skilled Occupations List.

The permits are valid for two years, and on expiration, the employee may apply for a "Stamp 4" permission to remain and work in the State without an employment permit. This permission is renewable on an annual basis. Once the applicant has legally resided in Ireland for five years, they may then be eligible to apply for long term residence permission.

Depending on the circumstances, the following permits may also be applied for in the context of fintech workers:

- **Intra-company Transfer Employment Permit**: Key management staff and management, as well as qualifying trainees, of a multinational company can be transferred to an Irish branch of the company with this permit.

- **General Employment Permit**: This may be used where the job in question fails to satisfy the salary requirements of the Critical Skills Employment Permit. However, as applications for this permit must satisfy a "labour market means test", it is not a particularly common form of work permit.
- **Contract for Services Employment Permit**: This enables the transfer of non-EEA employees to work in Ireland whilst remaining employed under their contract of employment outside of the State.
- **Internship Employment Permit**: This permit is available to full-time students enrolled in third level education outside of the State who have been offered an internship or work experience in Ireland.

Legally resident dependents of employees with permits may also apply for Dependent/Partner/Spouse Employment Permits.

Employers and contractors in the fintech industry may also sign up to the Trusted Partner Initiative. Under this scheme, employers can apply for "Trusted Partner" status in order to fast-track the permit application process.

Certain senior roleholders in fintech businesses providing regulated activities would also need to obtain the CBI's approval prior to taking up that position, under the "Fitness and Probity" regime.

6 Technology

6.1 Please briefly describe how innovations and inventions are protected in your jurisdiction.

The Irish legislative framework gives significant comfort to companies creating and managing their IP assets in Ireland. Patents, copyright, design rights, trade marks and confidential information can be used to protect inventions and innovations. All of the core Irish legislation in relation to these forms of protection has been introduced in the relatively recent past. The Commercial Court, a division of the Irish High Court, deals with major commercial and IP cases on an expedited basis and offers an effective way for fintech businesses to enforce their IP rights.

Copyright: Typically, copyright is the most useful protection for the kind of IP generated by fintech businesses, e.g. copyright protects the underlying code in software and computer programs. There is no system of registration for copyright protection in Ireland as copyright attaches automatically on the creation of an original work. Trade secrets can also be useful in protecting software.

Patents: There are two types of patent protection available under Irish patent legislation: a full term patent and a short term patent. In order for an invention to be patentable it must: (i) be new; (ii) involve an inventive step; and (iii) be capable of industrial application.

Trade marks and designs: Trade marks may be registered to protect the branding of fintech products and companies. Designs which are new and have individual character can be registered to protect the appearance of products.

6.2 Please briefly describe how ownership of IP operates in your jurisdiction.

Under Irish law, ownership of a patent rests with the inventor. If the invention is made by an employee in the course of their employment, the right to a patent will usually belong to the employer. In relation to copyright, the author of a work is the first owner. Similar to patent ownership, if a copyright work is made by an employee in the course of employment, the first owner of the work will be the employer, subject to any agreement to the contrary. Ownership of registered trade marks and designs will vest in the person who has applied for registration.

6.3 In order to protect or enforce IP rights in your jurisdiction, do you need to own local/national rights or are you able to enforce other rights (for example, do any treaties or multi-jurisdictional rights apply)?

Copyright: Ireland is a party to and incurs obligations under the Berne Convention (**Paris Act**), the Rome Convention, the TRIPs Agreement, the World Intellectual Property Organisation (**WIPO**) Copyright Treaty, and the WIPO Performances and Phonograms Treaty. These international agreements provide for automatic reciprocal protection for Irish copyright works in the territories of the signatories.

Patents: Patent protection may be secured by applying for (i) national protection in the Irish Patents Office, (ii) protection via the European Patent Convention (**EPC**), or (iii) protection under the Patent Cooperation Treaty (**PCT**) which provides for an international search and examination system. The outcome of an EPC or PCT application will, depending on the results of the search and examination process and application of national patent rules, result in national patents being granted which may be enforced in the jurisdictions in which they are registered.

Plans are at an advanced stage for the introduction of the EU Unitary Patent Package (**UPP**) which would provide: (i) a single unitary patent offering protection across EU Member States; and (ii) a Unified Patent Court (**UPC**). A referendum in Ireland is expected to be scheduled on the proposed UPC which, if ratified, will establish a specialised patent court with exclusive jurisdiction for litigation in relation to both European patents and European patents with unitary effect in all participating Member States.

Trade marks: Trade marks may be secured by applying for: (i) a national registration; (ii) an EU trade mark (which offers protection across all 28 EU Member States); or (iii) a registration under the Madrid System which provides for a single application through the national office resulting in a bundle of national trade mark registrations for the countries designated in the application. Irish and EU trade marks may be enforced in the Irish courts.

6.4 How do you exploit/monetise IP in your jurisdiction and are there any particular rules or restrictions regarding such exploitation/monetisation?

Licensing: In Ireland, licensing IP rights creates revenue streams whilst retaining ownership. An important consideration is that of an exclusive *versus* non-exclusive licence which has the potential to limit the use of the IP to one third party. If, for commercial reasons, an exclusive licence is granted, there are other options available that can be employed to maximise value, for example, by limiting exclusivity to a particular location or limiting the scope of use of the licence, thus retaining the ability to commercialise the same IP in other territories and/or other fields of use with other licensees. In any event, a licensor should retain sufficient control over its IP by ensuring sufficient obligations are imposed on the third party,

including provisions allowing the licensor to monitor the licensee's use of the IP and appropriate termination rights. The granting of a licence for a patent, trade mark or design should be notified to the Controller of Patents, Designs and Trade Marks (the **Controller**).

Assignment: In general, the assignment of IP must be in writing. Assignment of patents, trade marks and designs must be registered with the Controller. Copyright may be freely assigned and is not subject to any specific registration requirement.

Granting a security interest: Security may be granted over IP (most commonly patents, trade marks and copyright) under Irish law. Particulars of a security interest which is granted by an Irish company must be registered with the Irish Companies Registration Office within 21 days of the granting of the interest. Security interests granted over patents, trade marks and designs must be notified to the Controller and an original or certified copy of the security interest evidencing the agreement between the parties must be submitted to support the application.

Claire Morrissey
A&L Goodbody
IFSC, North Wall Quay
Dublin 1
Ireland

Tel: *+353 1 649 2246*
Email: *cmorrissey@algoodbody.com*
URL: *www.algoodbody.com*

Claire Morrissey is a Partner in the Firm's Commercial & Technology Group. She advises on a broad range of commercial contracts with a particular focus on technology, IP and sourcing agreements. Claire also advises on the technology, IP and data aspects of joint ventures, mergers & acquisitions.

Peter Walker
A&L Goodbody
IFSC, North Wall Quay
Dublin 1
Ireland

Tel: *+353 1 649 2000*
Email: *pwalker@algoodbody.com*
URL: *www.algoodbody.com*

Peter Walker is a Partner in the Banking and Financial Services Department. His principal practice areas are asset-backed finance (including portfolio sales and acquisitions), debt capital markets, private equity finance, general banking and restructurings.

A&L Goodbody

With an established banking sector in Ireland and a rapidly evolving technology landscape, A&L Goodbody's FinTech Group's legal expertise facilitates a cutting edge approach to advising companies in this sector. Our clients include domestic and international financial services and technology companies and our team provides a complete legal service for related legal needs.

We advise on a wide range of fintech matters including: the development, acquisition and use of technologies and services; strategic software development agreements; IT managed and shared services arrangements; complex transitional services agreements; transactional advice; and business process outsourcing. We also advise clients in relation to technology, financial regulation, compliance, risk management, data privacy, financing, cyber risk and the implications of Brexit.

In addition, A&L Goodbody is a member of the Fintech and Payments Association of Ireland.