WILLIAM FRY

Legal News

Welcome to the January issue of Legal News. For further information on any of the topics covered in this edition, please call or email any of the key contacts or your usual William Fry contact person.

Investors and Firms Alerted to Initial Coin Offering Risks

The European Securities and Markets Authority (ESMA) recently published two separate statements addressed to firms and investors on Initial Coin Offerings (ICOs). The statements provide some insight into ESMA's current thinking on ICOs which have gained much attention in the fast moving and ever-expanding cryptocurrency arena.

An ICO is a relatively recently devised means of raising capital by offering virtual coins or tokens that are created in exchange for legal tender or other cryptocurrencies such as Bitcoin, with the capital raised usually going towards initiating or completing the creation of a new cryptocurrency. As well as speculating on the value of the prospective cryptocurrency, initial investors will usually also gain additional rights such as rights to participate in the project and to vote on how it is run.

The ESMA statement addressed to firms warns that coins issued in an ICO may constitute financial instruments resulting in firms involved in such ICOs being considered as carrying out regulated activities in the EU. While noting that it is up to each firm to consider the applicable regulatory framework, ESMA identified the Alternative Investment Fund Managers Directive, the Fourth Anti-Money Laundering Directive, MiFID and the Prospectus Directive as regulatory regimes that are likely to apply.

The ESMA statement addressed to investors recognises the possibility that ICOs may operate in a wholly unregulated space. ESMA highlights this as a major risk associated with ICOs along with a number of other concerns in respect of ICOs referring to them as *"extremely risky and highly speculative investments*". Among the concerns voiced by ESMA regarding ICOs are:

- the likelihood of fraud or money-laundering;
- the high risk of investors losing all of their invested capital, as many ICOs are very early stage ventures with a high risk of failure that issue tokens which have no intrinsic value if the platform is not subsequently developed;
- the volatility of the prices of tokens, and the fact that not all tokens are traded on virtual currency exchanges, meaning a lack of exit options;
- that the information provided in many ICO whitepapers has been "*unaudited, incomplete, unbalanced or even misleading"*; and
- potential technological flaws.

As the capitalisation of Bitcoin and other cryptocurrencies continues to soar, with investor interest as high as ever, regulators are sure to keep a close eye on developments in this space.

Employer Vicariously Liable for Data Breach in Class Action Case

The first UK class action case to arise from a data leak has found an employer vicariously liable for the act of one employee in leaking the personal data of nearly 100,000 other employees. The case is a harbinger of similar actions to come when the GDPR comes into force across the EU in May 2018.

The high profile case concerned the supermarket chain Morrisons. Andrew Skelton, a disgruntled employee, posted a file containing the personal data of 99,988 employees to a file-sharing website. Skelton was sentenced in 2015 to eight years imprisonment for a range of offences arising from this incident, including fraud, securing unauthorised access to computer materials and disclosing personal data. Subsequently 5,818 of the employees, whose data had been included in the file, sued Morrisons.

The High Court found that although Morrisons had fallen short of complying with the data protection principle of ensuring adequate technical and organisational measures to prevent the unauthorised or unlawful processing of personal data, this was not causative of the data breach, and so Morrisons was not directly liable. In determining whether Morrisons was vicariously liable for Skelton's actions, the Court had to consider whether Skelton's actions were "sufficiently closely connected" to his role at Morrisons. The Court found that they were, on the grounds that:

- there was "*an unbroken thread that linked his work to the disclosure*";
- Morrisons had entrusted Skelton with the data, rather than merely granting him access rights to it, such that even though he was not authorised to disclose the data in the manner he did, this action was sufficiently closely related to the acts he was entrusted to perform; and
- although his actions were injurious to his employer, this did not take his actions outside the scope of his employment.

However the Court was uneasy with the submission that because Skelton's acts were aimed at damaging Morrisons, the same party that the claimants sought to hold responsible, the Court's conclusion would have the effect of furthering Skelton's criminal aims. To this end the Court granted leave to Morrisons to appeal the decision regarding vicarious liability.

As data breaches become ever more frequent and larger in scale, affected data subjects across the EU will likely resort to class action claims, whereby resources can be pooled to achieve better outcomes. Such actions are likely to become more frequent after the GDPR comes into force on 25 May 2018, as it strengthens data subjects' rights and broadens the range of damages available.

Contributed by: John Magee

Court of Appeal Confirms Appointment of Examiner Despite Existence of Restructuring Agreement

The Court of Appeal recently ruled, in *Re KH Kitty Hall Holdings & Ors*, that an agreement to restructure and discharge the secured debts of a number of companies by selling certain secured assets was not a bar to the appointment of an examiner to those companies. This was the case despite the fact that the application for the appointment of an examiner was inconsistent with the obligations imposed on the companies under the restructuring agreement and was objected to by the secured creditor.

The Court confirmed the appointment of Mr Neil Hughes of Baker Tilly Hughes Blake as examiner to seven group companies (the "**Group**") in the Edward Capital Group. The Group, whose assets include the 5-star G Hotel, the 4-star Hotel Meyrick and the Eye Cinema in Galway, were controlled by Galway businessman Gerry Barrett.

The High Court initially appointed Mr Hughes as interim examiner to the Group in September 2017 following a petition by the Group after Deutsche Bank had appointed a receiver over the assets of five of the companies.

Deutsche Bank, to whom the Group owe more than €680 million, opposed the subsequent application to confirm the appointment of Mr Hughes as examiner. Deutsche Bank claimed that the petition was an abuse of process and an attempt to renege on an agreement entered into by the Group and Deutsche Bank in December 2016 to restructure and discharge the secured debt by selling down the secured assets of the Group (the "**Debt Settlement Agreement**").

Ultimately, Mr Justice O'Connor in the High Court refused to confirm the appointment of the examiner to four of the seven companies. These four companies owned and/or operated the G Hotel and the Eye Cinema. He said that the primary motivation behind the application was Mr Barrett's attempt to retain control of the firms in defiance of the Debt Settlement Agreement, which was not the purpose of the examinership process. He viewed the application as an abuse of process. Instead, Mr Justice O'Connor confirmed Mr Hughes's appointment as examiner to three of the companies, being the companies owning and/or operating the Meyrick Hotel. In doing so he cited his concern for the hotel's customers and employees and was satisfied that the three companies each had a prospect of survival as a going concern.

The Group appealed the decision to limit the extent of the examinership whilst Deutsche Bank cross-appealed that the examinership should not be confirmed in respect of any of the companies. The Court of Appeal, in overturning the High Court decision and confirming Mr Hughes's appointment as examiner to all seven companies, made the following observations:

1. The examinership system is premised on the assumption that pre-existing commercial contracts, of whatever kind, will be overridden, varied, negated and dishonoured in the wider public interest of rescuing an otherwise potentially viable company.
2. The Court, in exercising its statutory discretion to appoint an examiner, must take into account all relevant facts and circumstances from the evidence before it and balance any prejudice to creditors against the wider public interest in rescuing an otherwise potentially viable company.
3. The mere fact that the petition was inconsistent with the terms of the Debt Settlement Agreement could not in and of itself be a factor to justify the Court's refusal to appoint an examiner.
4. A company has a statutory entitlement, pursuant to section 510(1) of the Companies Act 2014 (the "**Act**"), to present a petition seeking the appointment of an examiner. The Group was exercising a statutory right for the intended purpose of procuring rescue from insolvency. The Court held that there were no prior proceedings which made the presentation of the petition an abuse of the due administration of justice. The ordinary commercial instincts of profit making and loss avoidance could not, in the circumstances of the case, be considered an improper motive in seeking to have an examiner appointed by the Court.
5. The Court noted that the Debt Settlement Agreement did not include an express provision seeking to exclude or prevent an examinership application by or on behalf of the Group although

it treated an application as a terminating event. The Court held that if the Debt Settlement Agreement purported to exclude or limit the statutory right to apply for examinership it would have to be shown that the Group had full knowledge that they were waiving such a right.

6. When considering whether or not to appoint an examiner the Court must determine whether the test in section 509 of the Act has been met and whether there is a reasonable prospect of the survival of the company. The Court confirmed that it was not necessary at the petition stage of the application to show that a company would probably survive.

The decision provides helpful clarity on the interaction of debt restructuring agreements with the examinership process, which as Mr Justice Hogan noted, had surprisingly been at best imperfectly explored in case-law since the introduction of examinership under the Companies (Amendment) Act 1990. The decision demonstrates the importance of fully and explicitly expressing any covenant or undertaking that would restrict a party's access to the Court and, in particular, a party's statutory right to apply to the Courts to commence an examinership process and the consequent protection offered by the Court.

At the time of writing the examinership is ongoing.

Contributed by: Rebecca O'Connor

Irish Court Compels Data Access Request in Aid of Discovery

The High Court recently considered the novel issue of whether it should order a person to disclose documents which they do not hold but can obtain by exercising their access rights under the Data Protection Directive (EU Directive 95/46/EC). The Court concluded that a party may be directed to disclose all documents requested in discovery that are reasonably available to them by means of a data subject access request.

Background

In *Susquehanna International Group Limited v Needham*, the plaintiff (SIG) claimed that the defendant was in breach of the express terms of his contract of employment. SIG alleged that the defendant: (1) was in breach of a covenant not to induce employees of SIG to leave for employment elsewhere; and (2) breached his obligation to preserve confidential information, trading strategies, and commercial know-how belonging to SIG.

The defendant, a trader in financial instruments, was one of a number of employees who left their employment with SIG in 2016. He subsequently took up employment with Citadel, a firm in the same business as SIG. Prior to taking up employment with Citadel, the defendant interacted with a recruitment company, Execuzon.

SIG's Discovery Request

Discovery is a procedure for disclosing information, usually by furnishing documents, so that both parties to litigation may know the case that they have to answer. SIG sought discovery a category of documents relating to interactions between the defendant and Citadel or Execuzon. The category included any documents held by Citadel and/or Execuzon that could be obtained by the defendant *"on foot of data protection requests".*

SIG argued that personal data held by a third party were within the *"possession, power or procurement"* of the defendant as explained by the Supreme Court in *Thema International Fund plc v HSBC Institutional Trust Services (Ireland) Ltd*. In that case, Mr Justice Clarke described the test as follows:

"A party either has documents in its possession or has the legal entitlement to require possession. In those circumstances the document must be discovered. In all other circumstances, the document does not have to be discovered."

SIG argued that the defendant had a right as a matter of European law, under the Data Protection Directive, to obtain data relevant to him from the relevant data controller. Therefore, SIG submitted, it was within the defendant's power to produce that personal data in response to a discovery request.

Objections to Data Protection in Aid of Discovery

The defendant objected to being required to make data access requests, arguing that:

- it was wrong in principle to compel use of data protection processes to achieve a collateral purpose more properly realised by an order for third party discovery (an argument made by reference to the UK case of *Durant v Financial Services Authority* which refused to allow data subject access requests as a proxy for discovery);
- the objective of data protection law and of the Directive was to protect the right to privacy, to enable the correction of any inaccuracy in the personal data held, and to ensure that inaccurate records were not kept; and
- Mr Justice Barrett had previously found, in Glaxo Group v Rowex, that discovery should not be used to compel *"inappropriate disclosures of personal data*".

Decision

The Court restated that the test for discovery remains *"whether the documents are relevant and necessary and the request is proportionate and not unduly repressive."* In the circumstances, it found that compelling data access requests would not be disproportionate or oppressive for the defendant.

While finding that the information in question here was not of the personal or highly confidential nature contemplated in *Glaxo Group v Rowex,* the Court also noted that *Glaxo Group* did not prohibit the ordering of data access requests in aid of discovery. The Court was satisfied that the present request was not an attempt to use data protection law for a collateral purpose in the sense discussed in *Durant v Financial Services Authority.*

Ultimately, the Court directed the defendant to disclose all documents requested in discovery that were reasonably available to him by means of a data subject access request. The defendant was also directed to take reasonable steps to procure the documents.

Comment

While data subject access requests are often used to seek documents from the opposing party prior discovery, this case gives rise to novel questions and concerns.

For those embroiled in litigation, the decision has the potential to expand significantly the so-called "*universe"* of documents which must be identified, retrieved, and reviewed when making discovery. Litigators will wonder whether parties might also be compelled to submit access requests under the Freedom of Information Act, expanding that universe still further. There will be concern too that further delays in the discovery process may arise where data controllers refuse access and data subjects have to challenge that refusal, either voluntarily or at the direction of the Courts.

Ms Justice Baker did agree that this approach to discovery must not be used as a tool of oppression. Exactly what *"reasonable steps"* must be taken, and how far one must go in challenging a refusal of access by a data controller, remains an open question.

Contributed by: John Sugrue

Newly-merged Office of Financial Services and Pensions Ombudsman To Take Effect on 1 January 2018

The Finance Minister has appointed January 1, 2018 as the date on which the Financial Services and Pensions Ombudsman Act 2017 (the "FSPO Act") will come into operation.

Headline changes under the FSPO Act:

1. Dissolves the offices of the Pensions Ombudsman and the Financial Services Ombudsman Bureau
2. Establishes the office of Financial Services and Pensions Ombudsman ("FSPO")
3. Appoints a single office holder, the 'Financial Services and Pensions Ombudsman' (the "Ombudsman")
4. Regulates procedures for complaints to the Ombudsman.

Time Limits for complaints against financial service providers:

Since July 2017, legislation has been in place (the Central Bank and Financial Services Authority of Ireland (Amendment) Act 2017 (the "CB Act")) which extends the previous time periods for complaints in relation to long-term financial services. The FSPO Act will repeal the CB Act, whilst retaining the extended time limit for such complaints. Under the FSPO Act, a "long-term financial service" is defined as a financial service with a duration of 5 years and 1 month, or more, and also life assurance policies. Section 51 of the FSPO Act provides that such complaints against a financial services provider can be made on the later of:

1. 6 years from the date of the act or conduct giving rise to the complaint; or
2. 3 years from the earlier of the date on which the person became aware of the act or conduct given rise to the complaint or ought reasonably to have become aware of that act or conduct; or
3. within such longer period as the Ombudsman may allow where it appears to him just and equitable to so extend.

To avail of the extended time period, the long-term financial service must not have expired or been terminated more than 6 years before the complaint, and the conduct complained of must have occurred during or after 2002. This in effect means that the FSPO Act has retrospective effect.

For other short-term financial services, the current 6 year time limit is retained.

Other Notable Aspects of the FSPO Act:

- Allows a complainant whose complaint was refused on the basis of time under the old regime to re-submit their claim to the Ombudsman, where it falls within the time limits under the FSPO Act.
- Enables the Ombudsman to require "any person" to provide information, documents or give evidence that the Ombudsman believes is relevant to the investigation of a complaint. Previously, the Ombudsman's powers only extended to compel documents or information from a financial services provider or an associated entity thereof and to officers, members, agents or employees of the financial services provider to give evidence.
- A decision of the Ombudsman is final, subject to right of appeal to the High Court within 35 days (previously 21 days).
- The Ombudsman may consider a complaint before the internal dispute resolution process is complete where a financial services provider has failed to complete the review within the time limit or the Ombudsman determines a complaint is of such importance as to warrant waiving the internal dispute resolution procedure.
- Allows an appropriate person to refer a claim on behalf of a deceased complainant, a minor or a complainant that is unable to act for himself or herself.

- The Ombudsman is obliged to inform the Central Bank of Ireland where there is a persistent pattern of complaints or facts or evidence against a financial services provider.
- Retains the 'name and shame' provisions of the previous regime, such that where a financial service provider has 3 or more complaints against it upheld, substantially upheld or partially upheld in the preceding financial year, the Ombudsman can name the financial service provider in its annual report.

Whilst the FSPO Act is a welcome modernisation of the legislation governing complaints against financial services providers, the extended limitation period will result in a significant increase in complaints. All financial service providers, including insurers, should consider the resulting impact on their complaints processes and procedures.

Contributed by: Catherine Carrigy and Gail Nohilly

Challenge to Privacy Shield by Digital Rights Ireland Dismissed by EU General Court

The General Court of the European Union has dismissed as inadmissible an action by Digital Rights Ireland (DRI) to annul the EU-U.S. Privacy Shield (Privacy Shield), meaning that Privacy Shield remains valid and in force. As we previously reported, Privacy Shield is the successor to the Safe Harbor framework following the latter's invalidation by the Court of Justice of the European Union (CJEU) in October 2015. Since July 2016, Privacy Shield has facilitated the free-flow of cross-border transfers of personal data between Europe and the US and has already been subscribed to by over 2400 companies. Privacy Shield has also just passed its first annual review, something which has provided much-needed certainty to participating organisations.

DRI based its action against Privacy Shield on Article 263 of the Treaty on the Functioning of the European Union (TFEU) which provides that: “[a]ny natural or legal person may […] institute proceedings against an [EU] act addressed to that person or which is of direct and individual concern to them” or “against [an EU] regulatory act which is of direct concern to them and does not entail implementing measures.” However, the Court found that DRI did not have standing under Article 263 TFEU to challenge Privacy Shield either in its own name (including because legal persons do not possess personal data rights) or in the name of its members or the general public. While Article 80 of the General Data Protection Regulation (GDPR) will introduce the possibility for consumers to permit a "not-for-profit body, organisation or association" to assert their privacy rights before EU courts, the GDPR only applies from 25 May 2018 and so DRI could not claim its protection.

DRI may decide to appeal the General Court's ruling to the CJEU and we will be closely monitoring any future developments. There is also a challenge to Privacy Shield by a French digital rights group and it will be interesting to see if the same rational will be applied by the General Court as in the DRI decision. The DRI judgment, combined with the fact that Privacy Shield has passed its first annual review, is positive news for organisations using the transfer mechanism, especially in light of the ongoing judicial challenges that the standard contractual clauses are currently facing.

Contributed by: John Magee

Heating Up? New Energy Efficiency Regulations for Buildings

The Building Regulations (Part L Amendment) Regulations 2017, SI No 538/2017 (the "Regulations") have been published, aiming to improve energy and carbon performance of new buildings, extensions to new buildings and major renovations.

Purpose of the Regulations?

The Regulations transpose EU requirements for nearly zero-energy buildings and major renovations set out in Directive 2010/31/EU on the energy performance of buildings (recast) (the "Directive"), seeking to increase energy efficiency across the EU and reduce greenhouse gas emissions.

Article 9(1) of the Directive requires EU Member States to ensure that:

- By 31 December 2020, all new buildings are nearly zero-energy buildings ("NZEB"); and
- After 31 December 2018, new buildings occupied and owned by public authorities are nearly zero-energy buildings.

Nearly Zero-Energy Buildings

The Directive defines a NZEB as a building with a very high energy performance, as determined in accordance with a methodology of calculation set out in the Directive. This definition was already incorporated to Irish law under the Building Regulations (Amendment) Regulations 2017, SI No 4/2017.

The nearly zero or very low amount of energy needed should be covered to a significant extent by energy from a renewable source, ideally produced on-site or nearby.

In Ireland, both energy consumption and carbon dioxide emissions for new buildings other than dwellings can be calculated using the Non-Domestic Energy Assessment Procedure ("NEAP") published by the Sustainable Energy Authority of Ireland.

Under the Regulations, buildings will need to be designed and constructed so as to ensure that the energy performance of the building is such as to limit the amount of energy required to operate it and reduce associated carbon dioxide emissions, in so far as practicable.

Types of buildings and works affected?

The Regulations apply to works to buildings other than dwellings, including new buildings and existing buildings in which a material change of use takes place or which undergoes major renovation. The Regulations describe major renovation as a renovation where more than 25% of the surface envelope of the building undergoes renovation.

The Regulations amend Part L (Conservation of Fuel and Energy) of the Building Regulations 1997-2017, Second Schedule, setting out statutory minimum standards of energy efficiency and carbon dioxide emissions to be delivered by such buildings upon construction.

When do the Regulations commence?

Subject to transitional arrangements, the Regulations will apply from 1 January 2019. Transitional arrangements will apply where:

- A planning application for planning permission or approval is made on or before 31 December 2018 and substantial work is completed by 1 January 2020; or

- A notice under Part 8 of the Planning and Development Regulations 2001 SI 600/2001 has been published on or before 31 December 2018 and where substantial work has been completed by 1 January 2020.

In turn, substantial work has been completed means that the structure of the external walls of the building have been erected.

Overview

Owners, public sector bodies, contractors, designers, asset and facilities managers need to carefully consider and map out how to meet the challenges of designing, constructing and managing works, projects and buildings to meet the Regulation's new energy efficiency requirements prior to 1 January 2019 - before things heat up.

Contributed by: Cassandra Byrne

Class Actions Make Political Agenda on the Back of the Tracker Mortgage Scandal

Discussions about the introduction of a class action procedure in Ireland have been very much on the agenda in recent weeks amidst the tracker mortgage scandal. A private member's bill on multi-party actions, the Multi-Party Actions Bill 2017, was introduced and debated in the Dáil in November 2017 and although opposed by the Government, the matter of class action lawsuits was referred to Mr Justice Kelly for consideration as part of the Review of Civil Justice Administration.

Current Procedures

Under Irish law as it stands, multi-plaintiff litigation can occur via two procedures; "representative actions" and "test cases". The Rules of Court provide for a representative action procedure whereby a named individual(s) can bring an action representing a class of persons interested in the same matter. It is generally confined to situations where the class is relatively small since the Court must be satisfied that each individual member of the class has authorised the named party. The procedure is further limited by the strict application of the rule that parties must have a similar claim, so that in essence claims must be almost identical. Considering the limitations of the representative action procedure, the preferred approach to multi-party litigation is the "test case". A test case can arise where numerous separate claims arise out of the same circumstances. A single case is run which then sets a precedent by which the remaining cases are resolved.

Past Recommendations

There has been discussions around the introduction of class actions for some time and in 2005 the Law Reform Commission published a report recommending that a formal procedural structure be set out in the Court Rules to deal with multi-party litigation. Those recommendations remain unimplemented.

At EU level, the European Commission published a Recommendation in 2013 on collective redress which invites member states to adopt a collective redress mechanism for both injunctive and compensatory relief for breach of EU law rights. Although the Recommendation states that member states should implement the principles within two years (i.e. by mid-2015), the recommendations do not have binding legal force and there has been no changes in this jurisdiction since the Recommendation. Click here to view a 2013 William Fry article on the Recommendation.

Multi-Party Actions Bill 2017

The Bill is largely based on the Law Reform Commission's paper on multi-party litigation from 2005. Under the Bill, proceedings which involve multiple parties (whether plaintiffs or defendants) and which involve common or related issues of fact or law, can be certified as a multi-party action by the Court. Once a party has contacted the Courts Service and confirmed that no previously certified multi-party action is relevant, a party can bring a motion seeking certification. The President of the High Court is to nominate a judge to deal with the application. If the certification application is granted, the judge will grant a multi-party action order and a register will be established pursuant to criteria set out by the judge. To join the register, a party will have to apply to the nominated judge to be entered. The appointment of a lead solicitor should be agreed by the parties and in the event that the parties fail to agree the Court will so appoint. The costs of the action will be divided equally amongst the members of the register who are liable, jointly and severally, for costs.

Next Steps

The Government opposed the Bill on grounds that it was technically flawed for seeking to enact as primary legislation a scheme that was intended by the Law Reform Commission to be in the form of the rules of court. While the Government was not dismissive of the Bill or its intent, it was submitted that a Bill of this nature, and the associated policy considerations, would benefit from pre-legislative scrutiny and examination as is the procedure for all government Bills. The Government informed the house that

it has agreed to put the possible introduction of class action lawsuits to Mr Justice Peter Kelly for consideration as part of the Review of Civil Justice Administration which he has recently commenced.

As the current Bill lacks government support is likely to fall off the statute book however now the matter is clearly on the agenda, we may see a procedure for class actions introduced through Court managed procedures (following President Kelly's review) or alternatively class-actions may be marked for the Government's legislation programme in Spring or Autumn next year.

Contributed by: Louise Mitchell

In Short: Data Protection Commissioner Warns Retailers on Use of E-Receipts

Following a recent series of audits and inspections, the DPC became aware that many retailers who were issuing e-receipts were doing so in order to obtain e-mail addresses for marketing purposes. Unsolicited marketing emails can bring about fines for retailers ranging from €5,000 to €250,000.

Retailers that obtain customer email addresses for providing e-receipts must have a clear retention period in place for storing this information. After this period, the customer's email address should be deleted.

Any customer who provides their email address to a retailer must be informed as to the purpose or purposes of obtaining this information. If the retailer intends to send future marketing materials to the customer, the customer will have to provide consent for this additional purpose.

For customers that only want to receive an e-receipt, retailers should clearly provide an "opt-out" box for the customer to tick if they do not want to receive future marketing materials. This should be placed beside where the email address is given. The DPC has advised that retailers should have a means to electronically record whether a customer has agreed to receive marketing materials or not.

Further marketing emails can be sent to the customer in certain circumstances under what is known as the "customer exception" which sets out additional rules.

This guidance is a timely reminder for retailers as to the rules around usage of data generated by e-receipts. This is particularly important in the lead up to the implementation of the GDPR in May 2018. Retailers should be reviewing and rewriting their current practices and policies in relation to the issuing of e-receipts as part of their GDPR readiness plans.

Contributed by: John Magee

In Short: New Equality Bill Targets Gender Pay Gap

On 25 October 2017 the Irish Human Rights and Equality Commission (Gender Pay Gap Information) Bill (the "Bill") passed the Committee Stage of the Seanad, following a floor debate. The Bill seeks to improve upon the Anti-Discrimination (Pay) Act, 1974 and to close the existing pay gap of 13.9% between men and women in Ireland.

The Bill, put forward by Labour Senator Ivana Bacik, contains provisions for the increased monitoring and publication of gender pay gap data, provisionally enforced by the Irish Human Rights and Equality Commission (IHREC).

If passed, IHREC, which already has the power to require an employer to carry out an equality review, will be given the further ability to oblige companies with 50 employees or more to publish the results of such a review.

The United Kingdom introduced gender pay gap reporting on 6 April 2017 under the Equality Act 2010 (Gender Pay Gap Information) Regulations 2017, with a qualifying threshold of 250 employees or more.

Several amendments to the Bill had been tabled prior to the Seanad debate, with a view to limiting IHREC's discretion to request and publish surveys and to compelling employers to participate. A system of fines for offending employers and a database of companies not in compliance were also proposed.

Minister of State for Justice, David Stanton, delivering the Government's submissions, successfully argued for the withdrawal of these proposed amendments, although they may be proposed again during the upcoming Report Stage.

Deputy Stanton submitted to the Seanad that smaller employers, in particular, require a greater degree of flexibility. Regular mandatory reporting for a company of a smaller size, it was suggested, may make it possible for employees to deduce an individual's salary, thereby breaching their data protection rights. It was also proposed that the Department of Justice and Equality would be a more appropriate enforcement body, with IHREC limited to an oversight and monitoring role.

The Deputy's comments suggest that further Government amendments, to be compiled during the upcoming Report Stage, will see the Bill focus on larger employers initially. Commentary surrounding the Bill suggests that the Government may seek to raise the qualifying threshold to 100 employees.

It is likely that, following the Report Stage, an amended Bill will be put back to the Seanad in the New Year. While aspects of the Bill are yet to be finalised, its central aim of eradicating the gender pay gap currently has cross-party support. It would, therefore, seem likely that Government-led measures will be enacted in 2018.

Contributed by: Catherine O'Flynn

In Short: European Court Rules that Exam Scripts and Comments Constitute Personal Data

In a landmark decision the European Court of Justice (ECJ) has ruled that exam scripts constitute personal data. As we previously reported, the Irish Supreme Court had asked the ECJ to determine whether an exam paper was personal data, a question which arose out of a trainee accountant's attempt to access his exam paper under the Irish Data Protection Acts (DPA).

The EU Data Protection Directive, implemented in Ireland by the DPA, defines personal data as *"**any information** relating to an identified or identifiable natural person".* Under the DPA, individuals have various rights in relation to their personal data, including rights to access it and rectify it in certain circumstances, and organisations which control that data must enable individuals to exercise these rights.

In its ruling, the ECJ said that a candidate sitting a professional examination is a natural person capable of identification either directly by name or indirectly by identification number from the exam script. The question of whether or not an examiner can identify the candidate at the time when the exam script is being marked is irrelevant.

The ECJ further stated that the phrase *"any information*" in the definition of personal data reflects the EU's intention that the concept should be interpreted broadly. Such an interpretation would not only include information which is sensitive and private but would also extend to objective and subjective opinions and assessments, provided that these were linked to an individual by reason of their content, purpose or effect. The ECJ found that written examinations submitted by a candidate at a professional examination would fall within this expansive interpretation.

As a result, the ECJ found that candidates could potentially exercise their personal data rights in relation to their written answers in a professional examination and also to the examiner's comments regarding those answers. However, the ECJ pointed out that these rights would not extend to the examination questions themselves as they would not constitute personal data. Further, there would be practical limitations to the exercise of such rights, for instance the right of rectification might apply to situations where examinations scripts had been mixed-up, but would not enable a candidate to retroactively correct incorrect answers.

The decision is a reminder of the sweeping nature of data protection legislation. It is particularly relevant in light of the GDPR which will apply across the EU from 25 May 2018 and which provides for top-level fines of up to €20m or 4% of total worldwide annual turnover in circumstances where organisations breach individuals' personal data rights.

For a more detailed analysis and expert insights on the incoming GDPR, we invite you to register here for PrivacySource, William Fry's dedicated GDPR website.

Contributed by: Barry Connolly and David Cullen

