Oireachtas Library & Research Service
Seirbhís Leabharlainne & Taighde an Oireachtais
Houses of the Oireachtas
Tithe an Oireachtais

L&RS NOTE

European Union Data Protection Law & Policy

27 October 2016

This *L&RS Note* provides an overview of European Union ('EU') law and policy in the area of data protection. Technological advances not only generate trade and investment but are also impacting on the right to privacy of the individual and the right to data protection. As a result of a number of recent developments in the area, data protection has become a big policy issue within the EU.

Recent developments include disclosures of mass surveillance by United States' public authorities in the 'Snowden revelations' concerning disclosures of mass surveillance by US public authorities and data protection case law from the Court of Justice of the European Union ('CJEU'). These have resulted in data protection reform within the EU.

This paper will look at the following areas relating to data protection with the EU:

- The emergence of an explicit fundamental right to protection for personal data.
- The main piece of EU law governing data protection, namely the Data Protection Directive.
- Recent developments in the area of data protection, including the replacement of the Safe Harbour Decision by the EU-US Privacy Shield. Those decisions were adopted by the EU Commission under the Data Protection Directive and provide a framework under which United States ('US') based organisations that self-certify compliance with EU data protection rules can transfer personal data from the EU to the US.
- On-going data protection reform within the EU, including the recently adopted General Data Protection Regulation and the Police and Criminal Justice Authorities Data Protection Directive.

L&RS Central Enquiry Desk: Tel. 618 4701

Contents

Table of acronyms and commonly used technical terms	
Adequacy decision	A decision by the Commission of the European Union that a third country, e.g. country outside of the EU or EEA provides adequate safeguards for the protection of personal data transferred there
Anonymised data	Data which has been anonymised by removing all elements from the data which would identify the person whose data it is
Automated decision	A decision made using personal data which is processed entirely by automatic means, e.g. credit scoring
CJEU	Court of Justice of the European Union (formerly known as the European Court of Justice (ECJ))
Commission	The Commission of the European Union
Commissioner	Irish Data Protection Commissioner
Data Protection Directive	European Union Data Protection Directive (Directive 95/46/EC)
Data controller	A person who decides to process people's personal data
Data processor	A person who processes personal data on behalf of the data controller
Data protection officer	A person appointed by a data controller to ensure a data subjects' rights are respected during the processing of their data
Data subject	A person whose personal data is processed
ECHR	The Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms (also known as the 'European Convention on Human Rights')
EDPS	European Data Protection Supervisor – the EDPS monitors the processing of personal data by Community institutions or bodies.
NDAP	National Data Protection Authority – in Ireland the Data Protection Commissioner
EU Charter	Charter of Fundamental Rights of the European Union
Processing	Automated processing of data, e.g. the automatic collecting, recording, organising, storage, adaption or alteration, retrieval, use, transmission, disclosure or deletion of data
Pseudonymised data	Where the information in personal data which would identify a person has been replaced with a pseudonym, e.g. the name or date of birth is replaced with a different name or date of birth
SCC	Standard Contractual Clauses (SCC) are clauses for contracts concerning data protection, and have been approved either by the Commission or NDPAs.
Transatlantic data flows	The transfer of personal data from the European Union to the United States
WP29	Working Group established under Article 29 of the Data Protection Directive to advise on European data protection law and policy

1. Introduction

What is personal data? European Union ('EU') data protection law defines personal data as data that can identify a person, either directly or indirectly.[1] Examples include your name, phone number, email address, place of birth, etc. The protection of personal data is a fundamental right in the EU.

The advances in information and communications technology ('ICT') are resulting in the exchange of more and more personal data between people and organisations, between organisations and across State borders. Basic data about a person, such as where they were at a certain time, who they emailed, texted or called can be combined and analysed to create a personal profile of that person.[2] It can tell you a person's "wants, needs, prejudices and opinions".[3]

This data is increasingly valuable and as a result personal data has become a commodity. The EU Commissioner for Competition has described it as a new currency.[4] European Union citizens' data was estimated to be worth €315 billion a year in 2011 and could grow to €1 trillion a year by 2020.[5]

The Commission sees the transfer of personal data as necessary for the expansion of international trade.[6] The Commission also sees personal data as playing a vital role in the fight against crime, particularly in the cooperation between law enforcement agencies in different countries.[7] In recent years this has resulted in a tension between the right to privacy and the right to data protection on the one hand and on the other hand the expansion of international trade, national security concerns and the need to fight crime.

2. Data protection and international trade

Cooper and Wandall have described being able to transfer data across the world as "a critical function for many organisations".[8] For example, multi-national organisations may need to transfer employees data to an office located in a different country.

The quantity of personal data that is transferred between the EU and United States ('US') ('transatlantic data flows') is greater than anywhere else in the world.[9] The transfer of data between the two regions supports and generates trade and investment between the regions ('transatlantic trade').[10] Total transatlantic trade was valued at $1 trillion in 2014 – this is the world's largest investment relationship.[11]

In addition to generating transatlantic trade, transatlantic data flows create opportunities for the expansion of trade and investment with the developing world.[12] As access to the internet across the world continues to increase, more of the developing world will access the internet using 'smart' devices.[13]

Furthermore, it is projected that online shopping will continue to increase. For example, in 2013 40% of the world's population made at least one online purchase, this was up from 38% in 2012.[14] This figure is expected to increase to 45% by 2017.[15] The combination of increased connectivity and online shopping illustrates the opportunities for expanding international trade through online commerce.[16]

Impact of stopping transatlantic data flows and data protection concerns

Recent studies estimated that EU gross domestic product ('GDP') would fall by 1.3% if transatlantic data flows were stopped.[17] The Business Software Alliance estimate that a 1% drop in GDP due to the stopping of transatlantic data transfers would result in a loss of €143 billion per year.[18]

Furthermore, concerns about data protection and cyber security can negatively impact on trade. A 2014 survey of EU citizens' concerns about the misuse of personal and security of online payments resulted in:

- 13% of people responding they were less likely to make online purchases.
- 12% of people responding that were less likely to bank online [19]

Ireland

All of the world's top ten 'born on the internet' companies, such as Facebook and Google have operational bases in Ireland[20] and are Ireland's top exporters.[21] These companies regularly transfer data from Ireland to the US.[22] The digital economy contributes 6% of Ireland's GDP.[23] The tech sector in Ireland employs 105,000 people.[24] The indigenous tech sector employs 12,000 people and has an annual sales revenue of over €2 billion.[25]

Given the importance of the ICT sector to the Irish economy, Dara Murphy T.D., Minister of State for European Affairs, Data Protection and the EU Single Digital Market, has stated that any negative effects on the ability of technology companies to trade in this sector would negatively impact on Ireland the most.[26]

3. Data protection law in the European Union

There are a number of EU legislative instruments regulating data protection. The right to privacy and data protection are fundamental rights under EU law. Table 1 summarises the main pieces of data protection law applicable in the EU. It also includes Council of Europe data protection law.[1]

[1] The Council of Europe is distinct to the EU. It is an international organisation focused on promoting human rights, democracy and the rule of law in Europe. There are 48 Member States of the Council of Europe, including the 28 EU Member States. The European Union is preparing to sign the European Convention on Human Rights.

Table 1: Summary of data protection law within the EU

European Data Protection Law	Summary
1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms ('ECHR')	Article 8 provides for the right for respect for private and family life, home and correspondence ('right to privacy').
1981 Council of Europe Convention for the protection of individuals with regard to the automatic processing of personal data ('Convention 108')	Convention 108 regulates the processing, by both private and public entities, of personal data and personal data flows (transfers). It is the only legally binding international instrument in the data protection field. It entered into force in Ireland on 1 August 1990.
Charter of Fundamental Rights of the European Union 2000 ('the EU Charter')	Article 7 provides for the right to respect for private and family life (privacy). Article 8 formally recognised the right to protection of personal data.
Treaty on the Functioning of the European Union (TFEU) ('the Lisbon Treaty')	Article 16 obliges EU legislatures to set down data protection rules. In addition, it provides that EU legislators must set down rules for the free movement of personal data.
Data Protection Directive (Directive 95/46/EC)	The Data Protection Directive gave substance to, and expanded, the data protection rules set down in Convention 108. The Directive applies to all EU Member States and non-EU Member States that are part of the European Economic Area (EEA). Directive is limited to matters relating to the internal market. It does not extend to police and criminal justice cooperation.
Regulation (EC) No 45/2001	Regulation (EC) No 45/2001 applies to the processing of personal data by the EU institutions, bodies, offices and agencies.
Directive on privacy and electronic communications (Directive 2002/58/EC)	The Directive on privacy and electronic communications (ePrivacy Directive) aims to ensure the protection of fundamental rights, particularly the right to privacy in respect of the processing of personal data in the electronic communications sector.
Data Retention Directive (Directive 2006/24/EC amending Directive 2002/58/EC)	The Data Retention Directive required public electronic communication and network providers to retain certain data. It was struck down by the CJEU in 2014 (see *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others* at page 9 for more information).
Data Protection Framework Decision 2008 (Decision 2008/977/JHA)	The Data Protection Framework Decision aims to protect the processing of personal data for the purposes of preventing, detecting, investigating or prosecuting a criminal offence or executing a criminal penalty.
General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR')	The GDPR provides a single set of data protection rules thereby streamlining EU data protection law. It will apply from 25 May 2018 and will replace the Data Protection Directive (see section 5.1).
Police and Criminal Justice Authorities Directive (Directive (EU) 2016/680)	The Police and Criminal Justice Authorities Directive establishes rules for the processing of personal data in cases relating to criminal offences and related judicial activities (see section 5.2).

Source: Compiled by L&RS

3.1. The Right to Protection for Personal Data

The 1950 *Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms* ('ECHR') recognises the right to respect for one's private and family life, his or her home and his or her correspondence ('right to privacy'). The right to privacy includes respect for private life with regard to the processing of personal data.[27]

The 2000 *Charter of Fundamental Right and Freedoms of the European Union* ('the EU Charter') formally recognised the right to protection of personal data ('right to data protection'). The EU Charter became legally binding in the EU after the adoption of the *Treaty on the Functioning of the European Union* ('the Lisbon Treaty') in 2009, and in doing so the right to data protection contained therein became a specific fundamental right in EU law.[28] Furthermore, Article 16 of the Lisbon Treaty requires EU legislatures to set down data protection rules.

In Ireland, the right to privacy has been recognised by the Irish courts as an unenumerated right under Article 40.3 of the Constitution of Ireland.[29] The courts have also recognised that the right to privacy includes the right to privacy of private communications free from interference by the State, e.g. interception or surveillance.[30]

Furthermore, in *Schrems v Data Protection Commissioner*[31] the High Court stated that the accessing of private communications originating within a person's home by State Authorities directly engages the Constitutional right to privacy and the right to inviolability of the dwelling under Article 40.5.

Limitations to the right to privacy and right to data protection

Neither the right to privacy nor the right to data protection are absolute rights. The Lisbon Treaty recognises that the right to data protection must be balanced against other rights and freedoms.[32] In addition to the obligation to set down data protection rules, Article 16 of the Lisbon Treaty provides that EU legislators must also set down rules for the free movement of personal data.

The EU Charter also provides that the rights contained in it may be limited, where the limitation is set down in law and it respects the essence of the right being limited. Under Article 52 any limitations must be limited to what is proportionate and necessary, and genuinely meet objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others.

Similarly, the ECHR recognises that the right to respect for private and family life under Article 8 may be limited in accordance with the law, where it is necessary:

- in the interests of national security, public safety or the economic wellbeing of the country;
- for the prevention of disorder or crime;
- for the protection of health or morals; or
- for the protection of the rights and freedoms of others.

In Ireland, the High Court in *Schrems v Data Protection Commissioner* recognised that the interception of private communications by the State is not in itself necessarily unlawful. The Court stated that where appropriate safeguards are in place, the interception or electronic surveillance of communications may be lawful where it is indispensable for the preservation of State security.[33]

Recent developments in EU data protection law (discussed in section 4) highlight the challenges of balancing the right to privacy and right to data protection against other rights and freedoms. This balancing exercise is one of the reasons why reform of EU data protection rules (discussed in section 5) is taking so long.[34]

3.2. Data Protection Directive

The 1995 Data Protection Directive[35] is the primary piece of EU law regulating the processing of data protection. The objective of the Data Protection Directive is the protection of fundamental rights and freedoms, in particular the right to privacy with respect to the processing of personal data.

The Directive is transposed in Ireland through the *Data Protection Act 1988* (as amended) and accompanying secondary regulations. The Data Protection Directive will be replaced by the recently adopted General Data Protection Regulation when it comes into effect in May 2018 (the GDPR is discussed in section 5.1).

The Data Protection Directive does not explicitly recognise the right to protection of personal data; rather it established rules for the processing of personal data by private and national public bodies and data protection rights for individuals. It does not apply to the EU institutions and bodies or to police and criminal justice cooperation.

The Data Protection Directive provides a number of principles for the processing of personal data (Article 6). The data processing principles are provided for in section 2 of the *Data Protection Acts 1988 to 2003*. Table 2 sets out the key data processing principles provided for in the Data Protection Directive.

Table 2 sets out the key data processing principles of the Data Protection Directive

Principle	Summary
Lawful processing	The principle of lawful processing - personal data must only be processed in accordance with the law, it must be for a legitimate purpose, and it must be necessary to achieve that legitimate purpose.
Legitimate / specific purpose	The principle of purpose specification and limitation - before personal data is processed, the 'data controller' must specify the reason for processing the data. The processed data may not be used for any other purpose.
Data quality principles	The data quality principles require: • relevancy of data - only relevant data should be processed, e.g. only personal data that is necessary to fulfil the specified purpose; • accuracy of data - personal data should be accurate and up-to-date; and • limited retention of data - personal data should only be retained for the minimum period necessary for the fulfilment of the specified purpose.
Fair processing	The principle of fair processing - data controllers must inform people of the identify and address of the controller, and the purpose for processing their personal data before processing their personal data.
Accountability	The principle of accountability - data controllers must process personal data in accordance with the law and have safeguards in place for processing personal data and they must be able to demonstrate compliance with data protection law.[36]

Source: EU Agency for Fundamental Rights and Council of Europe (2014), "*Handbook on European data protection law*", Chapter 3 (available here)

The Data Protection Directive also provides individuals with a number of rights related to the protection of their personal data (Articles 12, 14, 15 and 23). These include the right to access to your personal data, the right to rectify errors in your personal data and in certain circumstances to right to object to the processing of your personal data. Table 3 highlights the main data protection rights in the Data Protection Directive.

Table 3: Summary of the main data protection rights in the Data Protection Directive

Right	Summary
Right to access	Article 12 provides the right to access to your personal data. This includes: • the right to be informed that your personal data is being processed; • the right to know the specified purpose for the processing of the data; • the right to know what type of data is being processed; and • the right to know to whom the data is disclosed.
Right to rectify or erase data	Article 6 provides that a data subject has the right to have inaccurate or incomplete data or data which is unlawfully processed rectified or erased. In addition, Articles 10 and 11 provide, among other things, that a data subject has a right to rectify data concerning him or her.[37]
Right to object to processing	Article 14 provides a person with the right, in some instances, to object to the processing of their personal data. The objection must be based on legitimate grounds that relate to his or her particular situation.
Direct Marketing	Article 14 provides the right to object to personal data being used for direct marketing.
Automated decisions	Article 15 provides the right to object to automated individual decisions. Such automated decisions must not produce legal effects that significantly affect the person and must not involve the processing of data intended to evaluate certain personal aspects relating to a person, such as his or her creditworthiness.

Source: Compiled by L&RS

3.3. Data Protection Authorities

The Data Protection Directive is monitored and enforced by national Data Protection Authorities (NDPAs) - in Ireland this is the Data Protection Commissioner ('Commissioner'). At the EU level, the European Data Protection Supervisor (EDPS) monitors the processing of personal data by Community institutions or bodies.[38]

The EU Charter (Article 8), the Lisbon Treaty (Article 16) and the Data Protection Directive (Article 28) provide that Member States must establish an independent data protection authority. The Court of Justice of the European Union ('CJEU') has re-affirmed the importance of the independence of NDPAs.

The CJEU stated that:

> [t]he guarantee of the independence of national supervisory authorities is intended to ensure the effectiveness and reliability of the monitoring of compliance with the provisions concerning protection of individuals with regard to the processing of personal data and must be interpreted in the light of that aim. It was established in order to strengthen the protection of individuals and bodies affected by the decisions of those authorities.[39]

The CJEU has described the independence of NDPAs as being "an essential component of the protection of individuals with regard to the processing of personal data". The CJEU has also confirmed that NDPAs must be free to perform their duties free of external influence, including political influence. The CJEU stated that the removal from office of a data protection commissioner by a Member State before their full term has been served could breach the independence obligation.[40]

In January 2016, Digital Rights Ireland (DRI), a privacy advocacy group, commenced legal proceedings against the Irish State challenging the independence of the Commissioner.[41] In the legal papers served on the State, DRI alleged that the Commissioner did not effectively monitor databases containing personal data that had been created by public bodies and, as a result, failed to act independently.[42] Furthermore, the legal papers noted that the Commissioner is integrated with the Department of Justice and that her staff are civil servants.[43]

While acknowledging that the Commissioner is government funded, Dara Murphy T.D., Minister of State for European Affairs, Data Protection and the EU Single Digital Market, has stated the Commissioner and its functions are independent of government.[44] There were no further updates relating to these proceedings at the time of publication.

3.4. Cross-border transfer of personal data

The Data Protection Directive provides that personal data can only be transferred to a third country, e.g. non-EU or non-EEA country, if that country *ensures an adequate level of protection*, through its *domestic laws or international commitments*, for personal data.

Under the Data Protection Directive the Commission may adopt a decision finding that a third country ensures an adequate level of protection for personal data. In 2000, the Commission adopted such a decision for the US, known as the Safe Harbour Decision.

The Commission through the Safe Harbour Decision found that the US, through a series of privacy principles, ensured an adequate level of data protection for EU citizens' personal data transferred to the US. The Safe Harbour Decision provided a legal basis for organisations to partake in transatlantic data flows. The Safe Harbour Decision was subsequently declared invalid by the CJEU (see discussion of *Schrems v Data Protection Commissioner* at pages 12-13 for more information).

4. Recent developments

A number of developments have resulted in data protection becoming a major policy issue in the EU. Most notably, the CJEU has delivered a series of judgments emphasising the importance of the right to privacy and right to data protection.[45]

4.1. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others

In *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others*, the CJEU declared invalid the Data Retention Directive ('DR Directive') on the grounds that it represented a wide-ranging and serious interference with the right to privacy and right to data protection, which went beyond what is strictly necessary. The DR Directive was transposed in Ireland by the *Communications (Retention of Data) Act 2011*.

The DR Directive required public electronic communication and network providers to retain certain location and traffic data, such as who sent an email and to whom and when it was sent. It also required related data that identified the subscriber or user of the service be retained. The data was to be retained for different periods ranging from six months to two years. The purpose for retaining the data was for the prevention, investigation, detection and prosecution of serious crime, e.g. organised crime or terrorism. The DR Directive provided the retained data was to be made available to national law enforcement agencies where requested.

The Court found that the obligation on providers to retain data, the periods for the retention of the data, and access to the data by competent national authorities interfered with the right to privacy. In addition, the Court found the retention of data amounted to the processing of data and as a result interfered with the right to data protection. The Court went onto consider whether the interference with these rights was justified in accordance with the EU Charter, i.e. whether it was in pursuit of a genuine interest and was necessary, appropriate and proportionate.

Noteworthy findings by the Court in its examination as to whether the interference was necessary, appropriate and proportionate include that the DR Directive did not:

- provide any rules to limit access to data to what was strictly necessary, or safeguards to limit the risk of abuse or unlawful access or use of the personal data;
- require that a court or other independent body to review access to the personal data by competent authorities before the data was accessed;
- require the retained data to remain within the EU, thereby removing the protection of the personal data and data subjects rights beyond the scope of the NDPAs.

Accordingly, the Court ruled that the interference with the right to privacy and right to data protection went beyond what was strictly necessary and was disproportionate.

4.2. Google Spain v AEPD and González

In *Google Spain v AEPD and González*,[46] the CJEU held that search engine operators are, in certain circumstances, obliged to de-list links to third-party webpages (URLs) from the list of search results when searching for the individual's name.[47] This is commonly referred to as 'the right to be forgotten'.

The Court found that the use by search engine operators of information published by third parties amounts to the processing of personal data for the purposes of the Data Protection Directive. It also found that searching for a person by name is likely to return information about their private life in a structured format, which allows the searcher to build a profile of the person searched for. As a result, the processing is likely to significantly affect a person's right to privacy and right to data protection. In such circumstances the search engine operator is a data controller and must ensure that its activities comply with the requirements of the Data Protection Directive.

The Court ruled that personal data in search results is incompatible with the Data Protection Directive where, in light of all the circumstances of the case and the amount of time that has passed, the data is inaccurate, inadequate, irrelevant, or excessive to the specified purpose for which it was originally processed.

However, the obligation to de-list the information must be balanced against other fundamental rights and freedoms and the interest of the public in having access to the information, such as the role the individual plays in public life. The assessment and the decision to de-list is made by the relevant search engine operator on a case-by-case basis.

How many requests have been made since the judgment?

All search engine operators must also comply with the Data Protection Directive and judgment. However, Google processes the most right to be forgotten requests.[48] Since May 2014, Google has received 565,794 requests and evaluated 1,718,688 URLs for de-listing and 43.2% of those URLs have been de-listed.[49]

The New York Times has reported that Google considers approximately 572 right to be forgotten requests per day.[50] It further reported that:

> Google's total number of privacy-related judgments is double those of most of Europe's biggest individual national authorities over the same period, even though these public agencies address a wider range of data protection complaints.[51]

According to The New York Times, the NDPAs do not appear to have queried the fact that Google is deciding so many data protection requests.[52] Luciano Floridi, a professor at the University of Oxford, has commented that:

> [i]f Europe really wanted to regain control over personal data, giving Google this type of power is an odd outcome.

Some privacy experts have expressed concern over the lack of transparency on the procedure used by search engines operators in handling right to be forgotten requests.[53]

Ireland

In relation to Ireland, since May 2014 4,072 people with a relationship to Ireland have made 4,420 removal requests to Google to have a combined total of 13,495 URLs de-listed and 36.8% of those URLs were de-listed.[54]

The Commissioner's office has received 55 appeals from decisions by search engine operators not to de-list URLs.[55] Fifty-one of those appeals concerned decisions by Google. In 30 of the appeals the Commissioner upheld Google's decision and in 17 of the appeals the Commissioner ordered the URLs to be de-listed.[56]

Who are the requests to be forgotten from?

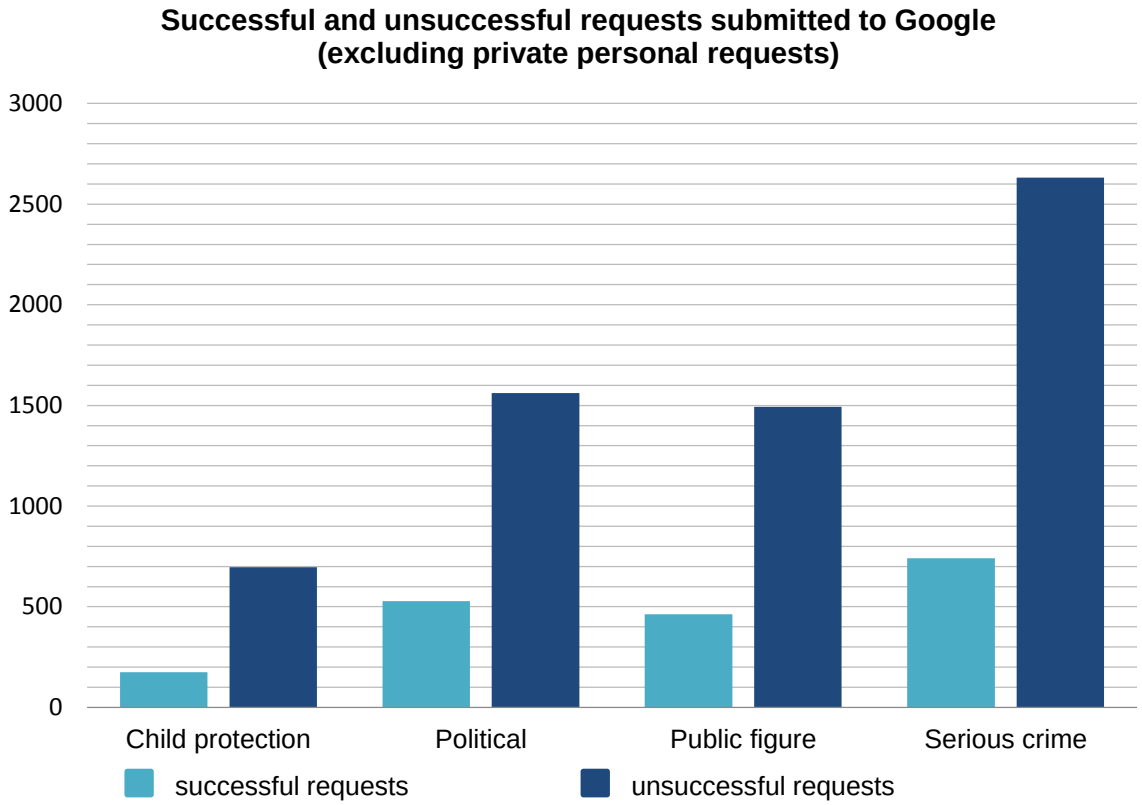
Google does not give a breakdown of who or what the requests it receives concern. However, The Guardian reported in July 2015 that from May 2014 to March 2015 Google received 218,320 requests to have URLs de-listed.

It reported that more than 95% of the right to be forgotten requests it received concerned private individuals. Forty-six percent of requests from private individuals were successful, the majority of which related to 'personal or private information'. Less than 5% of the requests involved criminals, politicians and high-profile public figures.

Graph 1 provides a breakdown of the number of successful and unsuccessful requests made to Google from May 2014 to March 2015 in the following four categories:

- child protection – accounted for 0.47% of the requests;
- political – accounted for 1.05% of the requests;
- public figure – accounted for 0.96% of the requests;
- serious crime – accounted for 1.88% of the requests;

These four categories made up less than 1% of the number of successful requests received from May 2014 to March 2015.



4.3. Schrems v Data Protection Commissioner

In *Schrems v Data Protection Commissioner*,[57] the CJEU declared invalid the Safe Harbour Decision adopted by the Commission under the Data Protection Directive. The case arose from a complaint by Mr Schrems to the Irish Data Protection Commissioner ('the Commissioner') alleging that by transferring his data to its US parent company Facebook Ireland Ltd was breaching his data protection rights. The basis of Mr Schrems' complaint was that due to mass surveillance by US intelligence agencies, the US failed to ensure adequate protection for personal data.

The Commissioner found that he could not investigate the complaint as the Commission, via the Safe Harbour Decision, had decided that the US adequately protected personal data transferred there from the EU. The Irish High Court asked the CJEU to rule whether, as a matter of law, the Safe Harbour Decision prevented the Commissioner investigating Mr Schrems' complaint.

Judgment of the Court of Justice of the European Union

The CJEU held the Safe Harbour Decision invalid as it did not state that the US, through its laws and international obligations, ensured an adequate level of data protection when compared to the protection afforded under EU law. The level of protection must be essentially equivalent to the protection afforded to personal data under EU law.

The Court found that the safe harbour scheme, by allowing US public authorities generalised access to EU citizens' personal data in the interest of national security, public interest and law enforcement e.g. mass surveillance, enabled the interference with EU citizens' fundamental rights, in particular the right to privacy under Article 7 of the EU Charter.

The Court also found that under Article 8 of the EU Charter, NDPAs must be able to investigate a complaint that a third country does not ensure an adequate level of protection for personal data transferred there. However, only the CJEU has jurisdiction to declare an EU act invalid.

In addition, the Court found that a failure by a third country to provide an administrative or judicial review for EU data subjects to access, rectify or erase their personal data breaches the right to an effective judicial remedy under Article 47 of the EU Charter.

Current status of Mr Schrems' complaint

On the basis of the CJEU's ruling, the High Court referred Mr Schrems' complaint back to the Commissioner to investigate. In May 2016, the Commissioner commended legal proceedings challenging the validity of a Commission decision that permits the transfer of personal data to third countries using Standard Contractual Clauses (SCCs) – an alternative method used for transferring data to a third country.[58]

The basis of the Commissioner's legal proceedings is that the SCCs being used by Facebook Ireland Ltd to transfer data to its US parent company do not ensure that EU citizens' will be able to obtain an effective legal remedy for data breaches, if any, in the US.[59]

A number of groups applied to the Court to be joined to the proceedings as 'amicus curiae' – a friend of the court who can offer relevant expertise or assistance to the court.[60] Parties who were successful in being added to the proceedings include the US government, the Business Software Alliance who represent the interests of companies such as Apple, Microsoft and Intel, Digital Europe and Electronic Privacy Information Centre (EPIC).[61,62]

The High Court has listed the matter for a three week hearing in February 2017.[63] If the High Court also concludes that the SCCs do not ensure EU citizens' can obtain an effective legal remedy for data breaches, the Court must make a preliminary reference to the CJEU to make a determination on the matter.

Review of Safe Harbour Decision

A 2013 Commission review of the Safe Harbour Decision identified a number of weaknesses in the Safe Harbour framework. This was in part due to the 'Snowden revelations' concerning disclosures of mass surveillance by US public authorities.[64]

The Commission decided that revoking the Safe Harbour decision would negatively impact companies in the EU and the US.[65] Instead of revoking the decision the Commission set about renegotiating the Safe Harbour Decision with the US. The decision in *Schrems* added urgency to those negotiations.

4.4. EU-US Privacy Shield

On 12 July 2016, the Commission adopted a new adequacy decision under the Data Protection Directive, known as the '*EU-US Privacy Shield'* ('Privacy Shield'). The Privacy Shield is made up of a series of privacy principles ('the Principles'), and of official representations and commitments by US authorities.[66] Text box 2 highlights the main points of the Privacy Shield.

Text box 2: Main points of the Privacy Shield

- Voluntarily self-certification by US organisations with the Principles when processing EU citizens' personal data.
- A "Privacy Shield List" is to be maintained by the US Department of Commerce listing US self-certified companies. The US Department of Commerce will amongst other things *ex officio* monitor for false claims by US organisations that they participate in the Privacy Shield.
- Written assurances from the US that there will be clear limitations, safeguards and oversight mechanisms concerning access to EU citizens' personal data by US public authorities for law enforcement and national security purposes.
- Various redress mechanisms to deal with data protection disputes by EU citizens', including:
  - access to an independent dispute resolution or self-regulatory body free-of-charge through the US self-certified companies;
  - complaining directly to EU NDPAs and national courts if the NDPA fails to address or inadequately addresses such a complaint;
  - review and enforcement of the Privacy Shield by the US Department of Commerce and the Federal Trade Commission (FTC);
  - binding arbitration which is available as a last resort.
- Establishment of a US Privacy Shield Ombudsperson to ensure that complaints by EU citizens' relating to US intelligence activities are adequately dealt with.
- An annual joint review on the implementation of the Privacy Shield will be carried out by the Commission and US public authorities.

European Union citizens' personal data can be transferred from the EU to US organisations that have voluntarily self-certified compliance with the Principles in the Privacy Shield ('US self-certified companies').[67] Organisations can self-certify with the US Department of Commerce from 1 August 2016.[68] Compliance with the Principles is compulsory and organisations must re-certify on an annual basis.[69]

The Principles in the Privacy Shield are "limited to the extent necessary to meet national security, public interest or law enforcement requirements".[70] United States self-certified

companies will remain obligated to disclose personal information when requested to do so by US public authorities, including for national security or law enforcement purposes.[71]

Investigative tools used by US public authorities, e.g. court orders or warrants to obtain data (including personal data) apply to all US organisations regardless of the nationality of the data subject.[72]

With the exception of the "Accountability for Onward Transfer Principle", the Principles will apply immediately upon self-certification by a US organisation. The Accountability for Onward Transfer Principle relates to "onward transfers" to third parties, e.g. where EU citizens' personal data is transferred from a US self-certified company to a third party in the US or another country outside of the EU. Under the Accountability for Onward Transfer Principle, the US self-certified company has nine months from self-certification to ensure that the third party complies provide the same level of protection as required by the Principles.[73]

5. Data protection reform

As noted above, the primary piece of legislation governing data protection is the Data Protection Directive. The Data Protection Directive was adopted 21 years ago - before the rise of the internet and smart devices.

In January 2012, due to the impact of technological advances and globalisation on the amount of personal data being collected, stored and transferred, the Commission proposed a reform package to overhaul EU data protection law.[74] The main aims of the EU data protection reform package include:

- strengthening of EU citizens' rights, including giving them more control of their data and to empower them to effectively exercise their rights;
- boosting the development and competitiveness of EU industries within the digital economy by enhancing people's trust in online services;
- providing uniform rules in the interest of legal certainty and reducing administrative burdens for the purpose of ensuring the EU single market and encouraging economic growth, job creation and innovation.

The Commission states that the proposed data protection reforms will streamline the regulation of data protection, thereby making it easier for small and medium enterprises to comply with the EU's data protection regime and reduce administrative costs.[75] The reform package includes:

- General Data Protection Regulation to replace the Data Protection Directive (see section 5.1);
- Police and Criminal Justice Authorities Data Protection Directive to provide for data protection in the areas of police and judicial cooperation in criminal matters (see section 5.2).

The Government's Legislation Autumn Session 2016 contains a Data Protection Bill to give effect to the GDPR and Police and Criminal Justice Authorities Data Protective Directive in Irish law.

5.1. General Data Protection Regulation

The General Data Protection Regulation ('GDPR') (Regulation (EU) 2016/679) provides a single set of data protection rules thereby streamlining EU data protection law. The GDPR was adopted on 24 May 2016 and will apply from 25 May 2018. The existing Data Protection Directive will stay in force in the interim period. Table 4 outlines notable features of the GDPR.

The Commission states that it will enhance EU citizens' data protection rights and reduce administrative requirements for organisations.[76] The Commission estimates that the reduction in administrative requirements will save businesses around €2.3 billion a year.[77]

Table 4: Notable features of the GDPR

Provision	Summary
Territorial scope of the Regulation	Article 3 provides the GDPR will apply to the processing of EU citizens' data by a data controller or processor even if not established in the EU e.g. it will apply to a company offering a service to citizens in the EU, regardless of whether the processing takes place in the EU.
Data processing principles	Article 5 sets out principles for the processing of personal data. These are: • **lawfulness, fairness, transparency principle -** personal data must be processed lawfully, fairly and in a transparent manner; • **purpose limitation principle -** personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; • **data minimisation principle -** personal data must be adequate, relevant and limited to what is necessary; • **accuracy principle -** personal data must be accurate and, where necessary, kept up to date; • **storage limitation principle -** personal data must be kept in a form which permits identification of data subjects for no longer than is necessary; • **integrity and confidentiality principle -** personal data must be processed in a way that ensures appropriate security of the data; • **accountability principle** - the data controller must be responsible for and be able to demonstrate compliance with all the data protection principles.
Consent to data processing	Article 7 provides that a data controller must be able to demonstrate that the data subject gave unambiguous consent to the processing of their data. A person's consent can be withdrawn at any time. Where consent is being given as part of a larger written declaration concerning other matters, the request for consent must be clear, use plain language and be distinguishable as a separate matter.
Consent for children using information society services	Article 8 provides that consent for children below 16 years of age to use information society services must be given or authorised by the holder of parental responsibility, e.g. the child's parent or legal guardian. Member States may lower the age to 13 years, but no lower. The data controller must take reasonable efforts to verify that the consent is actually given by the holder of parental responsibility. Under Article 83 a breach of this provision could result in a fine of up to

	€10,000,000 or up to 2% of the total worldwide annual turnover for the previous year (whichever is higher).
Right of access for the data subject	Article 15 provides that a person has a right to obtain from the controller certain information relating to the processing of the data, including confirmation as to whether or not their personal data is being processed, the purpose of its processing, and to whom their personal data has been disclosed, in particular recipients in third countries or international organisations. Furthermore, where their personal data is being transferred to a third country or international company a person has a right to be informed of the appropriate safeguards relating to the transfer.

Right to erasure ('right to be forgotten')	Article 17 provides that a person has a right to the erasure of their personal data without undue delay where:
	• the data are **no longer necessary** for the purposes for which they were collected or otherwise processed;
	• the data subject **withdraws** their **consent** on which the processing is based and where there is no other legal ground for processing the data;
	• the data subject has **objected** to the processing of their personal data under:
	  ○ Article 21(1), e.g. the processing is for a task being carried out in the public interest or in the exercise of official authority vested in the data controller, or in pursuit of a legitimate interest and there are no overriding legitimate grounds for the processing, or
	  ○ Article 21(2), e.g. direct marketing, including profiling.
	• the data was **unlawfully processed**;
	• the data must be erased to comply with a **legal obligation** under EU or Member State law; or
	• the data was collected in relation to the offering of information society services to a **child**.

Right to restriction of processing	Article 18 provides a right to restriction of processing of personal data. A person has a right to restriction of processing where:
	• they challenge the **accuracy** of the data, the processing will be restricted to enable the controller to verify the accuracy of the data;
	• the processing is **unlawful** and the data subject opposes to its erasure and requests that processing is restricted instead;
	• the controller **no longer needs** the personal data for the purposes of the processing, but the data subject requires the data to establish, exercise or defend legal claims; or
	• the data subject has **objected** to the processing of their personal data under Article 21(1):
	  ○ the processing is for a task being carried out in the public interest or in the exercise of official authority vested in the data controller, or
	  ○ in pursuit of a legitimate interest, the processing is to be restricted pending a determination of whether the legitimate grounds of the controller override those of the data subject.

Right to data portability	Article 20 provides a right to data portability. A person has the right to receive their personal data from a data controller and to transmit (transfer) the data to another controller. Where technically feasible, a person can have the data transferred directly from one controller to another.
Right to object	Article 21 provides a right to object to the processing of personal data where the data is processed: • under Article 6(1)(e) – for a task being carried out in the public interest

	or in the exercise of official authority vested in the data controller e.g. by a public authority who is statutorily mandated to process the data or in pursuit of a legitimate interest, including profiling based on the processing; or • Article 6(1)(f) – for direct marketing purposes, including profiling; unless the controller can show legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. A data subject also has the right to object to the processing of personal data on grounds relating to his/her particular situation where it is being processed for scientific or historical research purposes or statistical purposes, unless the processing is necessary for the performance of a task carried out for reasons of public interest.
Notification of personal data breach	Article 33 provides that where there is a data protection breach that is unlikely to result in a risk to the rights and freedoms of individuals, the controller must notify the supervisory authority without undue delay and, where feasible, not later than 72 hours after becoming aware of the breach.
Communication of a personal data breach	Article 34 provides that, subject to certain specified objections, where a personal data breach is likely to result in a high risk to the rights and freedoms of individuals, the controller must inform the data subject of the breach without undue delay. The communication must be comprehensive and use clear and plain language.
Data protection impact assessment	Article 35 provides that a data controller must carry out a privacy impact assessment where the processing is likely to result in a high risk to the rights and freedoms of individuals before the processing begins.
Designation of the data protection officer (DPO)	Article 37 provides that the data controller and processor must in certain circumstances designate an independent data protection officer (DPO). The DPO must be designated based on, amongst other things, their professional qualities, in particular their expert knowledge of data protection law and practices.
Supervisory Authority	Article 51 provides that each Member State must appoint at least one independent supervisory authority to monitor the application of the GDPR in order to protect people's fundamental right to data protection and facilitate the flow of personal data within the EU. Article 56 provides that the supervisory authority in the Member State where a company has it main establishment is competent to act as the lead supervisory authority for cross-border processing of data. Where a complaint has been received by a non-lead supervisory authority, the lead supervisory authority must decide whether it will handle the complaint within three weeks. Where the lead supervisory authority decides not to handle the complaint the referring supervisory authority will handle it.
Powers of Supervisory Authority	Article 58 grants supervisory authorities a number of investigative and enforcement powers, including the power to ban processing or suspend data transfers. Article 83 provides general conditions for the imposition of administrative fines by supervisor authorities for breaches of certain data protection laws. At the maximum end these can be up to €20,000,000 or 4% of total worldwide annual turnover for the previous year (whichever is higher).
Right to compensation	Article 82 provides that a person who suffers material or non-material damage due to a breach of their data protection rights has a right to receive compensation from the data controller or processor.

Source: Compiled by L&RS

5.2. Police and Criminal Justice Authorities Data Protection Directive

As part of the Commission's reform package, the EU institutions adopted the Police and Criminal Justice Authorities Data Protection Directive (Directive (EU) 2016/680) concerning data protection in the police and judicial sectors. The Police and Criminal Justice Authorities Data Protection Directive entered into force on 5 May 2016. Members States must transpose the Directive into national law by 6 May 2018.

The purpose of the Police and Criminal Justice Authorities Data Protection Directive is to establish rules for the processing of personal data in cases relating to criminal offences and related judicial activities. The Directive provides a harmonised framework under which personal data can be exchanged between Member States police and judicial authorities. Table 5 highlights notable features of the Police and Criminal Justice Authorities Data Protection Directive.

Table 5: Notable features of the Police and Criminal Justice Authorities Data Protection Directive

Provision	Summary
Subject-matter and objectives	Article 1 provides that the Directive applies to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.
Processing Principles	Article 4 sets out the principles relating to processing of personal data. These mirror those provided for in the GDPR as set out in Table 4.

Distinction between different categories of data subjects	Article 6 requires Member States to make distinctions between personal data of different categories of people. Examples of categories provided include:
	• persons for whom there are serious grounds for believing they have committed or are about to commit a crime;
	• persons convicted of a crime;
	• victims of a crime or persons where facts give rise to a belief that they could be the victim of a crime; and
	• other parties to a criminal offence, such as:
	  ○ possible witnesses in criminal proceedings,
	  ○ people who can provide information on a crime, or contacts or associates of people suspected of committing a crime or being about to commit a crime.

Processing of special categories of personal data	Article 10 provides that Member States can only permit the processing of personal data revealing "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation" where it is:
	• strictly necessary and is subject to appropriate safeguards for the rights and freedoms of the data subject, and only where:
	  ○ it is authorised by EU or Member State law; or
	  ○ it is to protect the vital interests of the data subject or of another natural person; or

	○ such processing relates to data which are manifestly made public by the data subject.
Measures based on profiling and automated processing	Article 11 provides the Member State shall prohibit the automated processing of personal data, including profiling, which produces an adverse legal effect for or significantly affects the data subject, unless it is authorised by law and the law provides appropriate safeguards. It also provides that national law shall not permit the automated processing of personal data using any of the prohibited categories listed in Article 10, e.g. race, ethnic origin, etc. unless suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.
Limitations to the right of access	Article 15 provides that in certain circumstances Member States may restrict a data subject's right of access to their personal data where it is necessary and proportionate in a democratic society in order to: • avoid obstructing official or legal inquiries, investigations or procedures; • avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or for the execution of criminal penalties; • protect public security; • protect national security; or • protect the rights and freedoms of others. Due regard must be had to the fundamental rights and legitimate interests of the data subject concerned.
Impact assessment	Article 27 provides that Member States must provide a data controller carry out a privacy impact assessment where the processing is likely to result in a high risk to the rights and freedoms of natural person before the processing begins.
General transfer principles	Article 35 sets out the general principles for data transfers to third countries or international organisations in the area of police co-operation and judicial co-operation in criminal matters, including onward transfers.
Derogations for specific situations	Article 38 provides that where there the Commission has not adopted an adequacy decision for the transfer of data to a third country or international organisation, or the third country does not provide appropriate safeguards, Member States must provide that personal data may be transferred ***only*** where the transfer is necessary: • in order to protect the vital interests of the data subject or another person; or • to safeguard legitimate interests of the data subject where provided for in law; or • for the prevention of an immediate and serious threat to public security of a Member State or a third country; or • in individual cases for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties; or • in individual cases for the establishment, exercise or defence of legal claims relating to the prevention, investigation, detection or prosecution of a specific criminal offence or the execution of a specific criminal penalty.
Supervisory authority	Article 41 provides that Member States must provide for one or more independent supervisory authorities to monitor application of the Directive. The supervisory authority may be the one which has been designated under the GDPR. Article 52 provides that every data subject must have a right to lodge a complaint with the supervisory authority. Article 53 provides a right to an effective judicial remedy against a decision of a supervisory authority.

Source: Compiled by L&RS

5.3. EU-US Protection Umbrella Agreement

In September 2015, the Commission and the US finalised the 'EU-US Protection Umbrella Agreement' - a transatlantic data protection agreement in the in the area of law enforcement.[78] The Umbrella Agreement is concerned with protecting personal data which has been transferred and processed for the purposes of preventing, investigating, detecting or prosecuting criminal offences, including terrorism.[79]

Unlike the Privacy Shield, the Umbrella Agreement is not an adequacy decision, nor can data be transferred under it.[80] Text box 3 highlights the main protections afforded to transferred personal data under the Umbrella Agreement.

Text box 3: Main protections for transferred personal data under the Umbrella Agreement[81]

- Clear limitations on what personal data may be used for.
- Consent from the authority which originally transferred the personal data must be gotten before the data can be transferred to a non-US or non-EU country or international organisation.
- Personal data may not be retained for longer than necessary or appropriate.
- People have a right to access and rectify their personal data, subject to certain conditions.
- A mechanism will be put to notify competent authorities and, where appropriate the data subject, of data security breaches.
- EU citizens a right to seek judicial redress the before US courts under *Judicial Redress Act* where US authorities deny access or rectification, or unlawfully disclose their personal data.

6. Conclusion

Data protection is a major policy issue in the EU. European Union data protection law was adopted before the rise of internet technology and the events of 9/11. Advances in technology are constantly testing the boundaries of the EU data protection regime and the risks those advances pose to the right to privacy and right to data protection. What ensures adequate protection for personal data is a dynamic concept that changes as technology and EU and national laws and policies evolve. In response, the EU has undertaken an extensive programme of reform of EU data protection law. This *L&RS Note* highlights the focus of the main reforms. However, it does not address all the work being done in this area. For example, there are proposed changes to the ePrivacy Directive (Directive 2002/58/EC) and the adoption of an Airline Passenger Directive (Directive 2016/681/EU). The evolving nature of the data protection landscape will result in legislative and regulatory changes to the data protection regime in Ireland.

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive) (available here)
[2] Karen Murray (2016), '*EU Data Protection Reform*', (2016) 34 Irish Law Times 26-28
[3] Karen Murray (2016)
[4] Denis Kelleher (2016), "*Reform of EU data protection; progress & future*", presentation at CMG Events Conference, "*Implementing The New EU Data Protection Regulations*", on 24 February 2016
[5] European Commission (2013) at p.3
[6] European Commission (2013), '*Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems)*', COM(2015) 566 final at p. 2 (available here)
[7] European Commission, '*Reform of EU data protection rules*' (available here)
[8] Daniel Cooper and Hilary Wandall (2016), '*Dual certification: a tale of two frameworks*', Data Protection Ireland Vol. 9, Issue 3 at p.12
[9] Dr. Joshua P. Meltzer (2015), '*Testimony to the Subcommittee om Commerce, Manufacturing, and Trade and Subcommittee on Communications, Technology, United States House of Representatives Hearing on "Examining the EU Safe Harbour Decision and Impacts for Transatlantic Data Flows*"' (03 November 2015) (available here)
[10] Dr. Joshua P. Meltzer (2015)
[11] Dr. Joshua P. Meltzer (2015)
[12] Dr. Joshua P. Meltzer (2015)
[13] Dr. Joshua P. Meltzer (2015)
[14] Dr. Joshua P. Meltzer (2015)
[15] Dr. Joshua P. Meltzer (2015)
[16] Dr. Joshua P. Meltzer (2015)
[17] Murphy (2015), '*Statement of the U.S. Chamber of Commerce On: the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows*' Testimony to the Subcommittee om Commerce, Manufacturing, and Trade and Subcommittee on Communications, Technology, United States House of Representatives Hearing on "Examining the EU Safe Harbour Decision and Impacts for Transatlantic Data Flows", (03 November 2015) (available here)
[18] Mary Carolan, '*Ruling against data transfer regime may cost Europe €143bn a year, says Facebook*' The Irish Times 07/07/2016 (available here) (accessed 19/07/2016)
[19] European Commission Special Eurobarometer 423, '*Cyber Security*', at pp. 23 & 30 February 2015 (available here)
[20] IDA Ireland (2016), webpage '*Information Communications Technology*' (available here) and Department of Communications, Energy and Natural Resources (2015), '*National Cyber Security Strategy 2015-2017*' (available here)
[21] Irish Exporters Association & Investec (2015), '*Top 250 Exporters 2015*' (available here)
[22] Will Goodbody, '*The EU-US Privacy Shield – what is it?*', RTÉNews.ie 02 February 2016 (available here)
[23] John Kennedy (2016), *Hey big spenders: Ireland's digital economy now worth 6pc of GDP*, Silconrepublic 21 September 2016 (available here)
[24] IBEC (2016), *Making Ireland a Global Technology Powerhouse* (available here)
[25] IBEC (2016), *Making Ireland a Global Technology Powerhouse*
[26] Suzanne Lynch, '*Transatlantic data deal keeps Ireland in hot seat*', The Irish Times 04/02/2016 (available here)
[27] C-362/14 *Maximillian Schrems v Data Protection Commissioner*, at 39 (available here)
[28] EU Agency for Fundamental Rights and Council of Europe (2014), "*Handbook on European data protection law*", at p.20 (available here)
[29] *Kennedy and Arnold v Attorney General* [1987] IR 587; *Re a Ward of Court* (No 2) [1996] 2 IR 79
[30] *Kennedy and Arnold v Attorney General* [1987] IR 587 at p. 592 and *Schrems v Data Protection Commissioner* [2014] IEHC 310 at para.47
[31] *Schrems v Data Protection Commissioner* [2014] IEHC 310 at para.48
[32] Karen Murray (2016)
[33] *Schrems v Data Protection Commissioner* [2014] IEHC 310 at para.49
[34] Karen Murray (2016)
[35] Data Protection Directive

[36] EU Agency for Fundamental Rights and Council of Europe (2014), Chapter 3
[37] The European Court of Human Rights (ECtHR) has upheld that data subjects have the right to rectify, erase or block the processing of personal data that does not comply with the requirements in the Data Protection Directive, e.g. it is inaccurate or was unlawfully processed. See *Cemalettin Canli v Turkey* (Application No. 22427/04), 18 November 2008 (available here) and *Dalea v France* (Application No. 965/07), 02 February 2010 (available here) as cited in the EU Agency for Fundamental Rights and Council of Europe (2014), at p.109
[38] European Commission Justice (2010), "*Protection of personal data in the European Union*", (available here)
[39] C-362/14 *Maximillian Schrems v Data Protection Commissioner*, at p.41 (available here)
[40] Case C‑288/12 *European Commission v Hungary* 08 April 2014 at paras. 51-55 & 62 (available here)
[41] Digital Rights Ireland (2016), "*DRI challenges independence of Ireland's Data Protection Authority*", 28 January 2016 (available here)
[42] Elaine Edwards, "*Independence of Data Protection Commissioner questioned*", The Irish Times 28/01/2016 (available here)
[43] Elaine Edwards (2016), The Irish Times 28/01/2016
[44] RTE.ie (2016), *Minister says Data Protection Commissioner is independent*, 28 January 2016 (available here)
[45] Not all the cases are discussed in this L&RS Note. Other prominent cases which are not discussed include: Case C-230/14 *Weltimmo v Nemzeti Adatvédelmi és Információszabadság Hatóság* (available here)*;* Case C-201/14 *Bara v Președintele Casei Naționale de Asigurări de Sănătate and others* (available here)*;* C-212/13 *František Ryneš v Úřad pro ochranu osobních údajů* (available here).
[46] Case C-131/12 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González* 13 May 2014 (available here)
[47] The webpage itself is not deleted from the original publisher's source nor from the search engines indexes. A search using search terms other than an individual's name may still list the webpage at the centre of the request – see Article 29 Date Protection Working Party (2014), '*Guidelines on the implementation of the Court of Justice of the European Union on the judgment on "Google Spain and Inc v. Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalex" C-131/12*' adopted on 26 November 2014 (available here)
[48] Ellen P. Goodman (2015), '*Open Letter to Google From 80 Internet Scholars: Release RTBF Compliance Data*' (available here)
[49] Google Transparency Report, '*European privacy requests for search removals*' (available here)
[50] Mark Scott, '*Europe Tried to Rein In Google. It Backfired*', The New York Times 18/04/2016 (available here)
[51] Mark Scott (2016), The New York Times 18/04/2016
[52] Mark Scott (2016), The New York Times 18/04/2016
[53] Ellen P. Goodman (2015)
[54] Google, '*European privacy requests for search removals*' (available here)
[55] Colm Keena (2016), '*Key tribunal witness in failed bid to be 'forgotten' online*' The Irish Times 03/03/2016 (available here)
[56] Colm Keena (2016), The Irish Times 03/03/2016
[57] C-362/14 *Maximillian Schrems v Data Protection Commissioner* (available here)
[58] Data Protection Commissioner (2016a), '*Statement by the Office of the Data Protection Commissioner in respect of application for Declaratory Relief in the Irish High Court and Referral to CJEU*', 25/05/2016 (available here)
[59] Data Protection Commissioner (2016b), '*Update on litigation involving Facebook and Maximillian Schrems Explanatory Memo*', 28/09/2016 (available here)
[60] Data Protection Commissioner (2016b)
[61]Data Protection Commissioner (2016b)
[62] Data Protection Commissioner (2016b)
[63] Mary Carolan, '*Schrems and Facebook privacy case: next round set for February'*, The Irish Times 25/07/2016 (available here)
[64] European Commission, '*Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU*', at p.3 COM(2013) 847 final (available here)

[65] European Commission, '*Communication from the Commission to the European Parliament and the Council Rebuilding Trust in EU-US Data Flows*', at p.7 COM(2013) 846 final (available here)
[66] European Commission, '*Commission Implementing Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield*', at p.4, C(2016) 4176 final, 12.7.2016, ('EU-US Privacy Shield') (available here)
[67] EU-US Privacy Shield, at pp. 4-5
[68] European Commission - Press release, '*European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows*', 12 July 2016 (available here)
[69] EU-US Privacy Shield, at p.8
[70] EU-US Privacy Shield, at p.16
[71] US Department of Commerce, *Letter to EU Commissioner for Justice, Consumers and Gender Equality*, 23 February 2016, Annex 1 (available here)
[72] U.S. Department of Justice Criminal Division, Letter to U.S. Department of Commerce and Deputy Assistant Secretary International Trade Administration, 19 February 2016 (available here)
[73], For a full list of the privacy principles in the see pages 7 – 9 of the EU-US Privacy Shield. See also pp. 4-5 and 9 of the EU-US Privacy Shield.
[74] EU Agency for Fundamental Rights and Council of Europe (2014), at p. 21
[75] European Commission - Press release, '*Agreement on Commission's EU data protection reform will boost Digital Single Market*' 15 December 2015 (available here)
[76] European Commission, webpage '*Protection of Personal Data*' (available here)
[77] European Commission - Press release IP/12/46, '*Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses*' (available here)
[78] European Commission (2016), '*Communication from the Commission to the European Parliament and the Council Transatlantic Data Flows: Restoring Trust through Strong Safeguards*' COM(2016) 117 final 29 February 2016, at p.12 (available here)
[79] European Commission (2016), at p.12 footnote 25
[80] European Commission (2016), at p.13
[81] European Commission - Fact Sheet, '*Questions and Answers on the EU-US data protection "Umbrella agreement"*', 8 September 2015 (available here)