THE WARD GROUP

GDPR- Fundamentals

Presented by:
Paula Carney-Hoffler E.I.I.C.M Credit Mgt.Cert,DipLaw
Client Credit Risk and Compliance Manager, The Ward Group

What is Data Protection

- Data Protection is about the fundamental right to privacy for Individuals. It covers the duty and obligations that companies who process, hold and use data on a daily basis must adhere to.
- Data Protection comes directly from privacy related laws which have existed in society as a whole for a very long time.
- It was first established and brought into law under the Irish constitution Article 40.1.3 which brought about the establishment of an implied right to privacy.
  - "The State guarantees in it laws to respect and as far as practicable by its laws, to defend and vindicate the personal rights of a citizen" .*Irish Constitution, Article 40.3.1 1st of July 1937.*
  - *The committee on Privacy chaired by David Calcutt, QC in 1990 created a working definition for the purpose of the report*
  - "*The right of the individual to be protected against intrusion into his personal life or affairs, or those of his family, by direct physical means or by publication of information*" *Sir David Calcutt,QC June 1990*

History of Data Protection

- Data Protection legislation can be tracked back to the General Assembly of the United Nations which adopted and proclaimed the Universal Declaration of Human Rights on the 10th of December 1948.
- In 1950 , the Council of Europe wanted to create greater unity between the member states and in realisation of Human Rights and Fundamental Freedoms.
- These documents were drafted in the aftermath of World War Two and the continuous drift towards the Cold War.
- In terms of privacy deep consideration is given to Article 8 and Article 10 of the European Convention on Human Rights

Data Protection Today

In 1981 the Council of Europe issues the "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" (Treaty108) 1981. This required member states in Europe to implement the Convention in their own jurisdiction the saw the birth of the Irish Data Protection Act 1988.

- **Data Protection Act 1988**

- An Act to give effect to the Convention for the Protection of the Individual with regard to Automatic Processing of Personal Data, done at Strasburg on the 28th day of January 1981, And for the purpose to regulate in accordance with its provisions the collection, processing ,keeping, use and disclosure of certain information related to individuals that is processed automatically"

- **The European Data Protection Directive 95/96/EC{Article32} Oct 1995**

- In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons and in particular their right to privacy with respect to the processing of personal data"

Ireland did not comply with the Act immediately and it was not till July 2003 that the Data Protection Amendment Act came into play

- **Communications (Retention of Data Act) January 2011**
  - Data in relation to telephone calls to be retained for two years, and data in relation to internet services to be retained for one year. At the end of the respective retention periods, the data must then be destroyed

- **The European Communities (Privacy and Electronic Communications) Regulations, July 2011**
  - With the ongoing development of electronic communications, organisations can now communicate with their customers by many means such as email, text ,push/pull marketing, tracking of IP's the list is continuing to grow.
  - This piece of Legislations covers topics like data security breaches(we have seen this recently in the news with regard to loyalty cards)retention, the conduct of e-mail and text based marketing campaigns, and the deployment of cookies on clients hardware

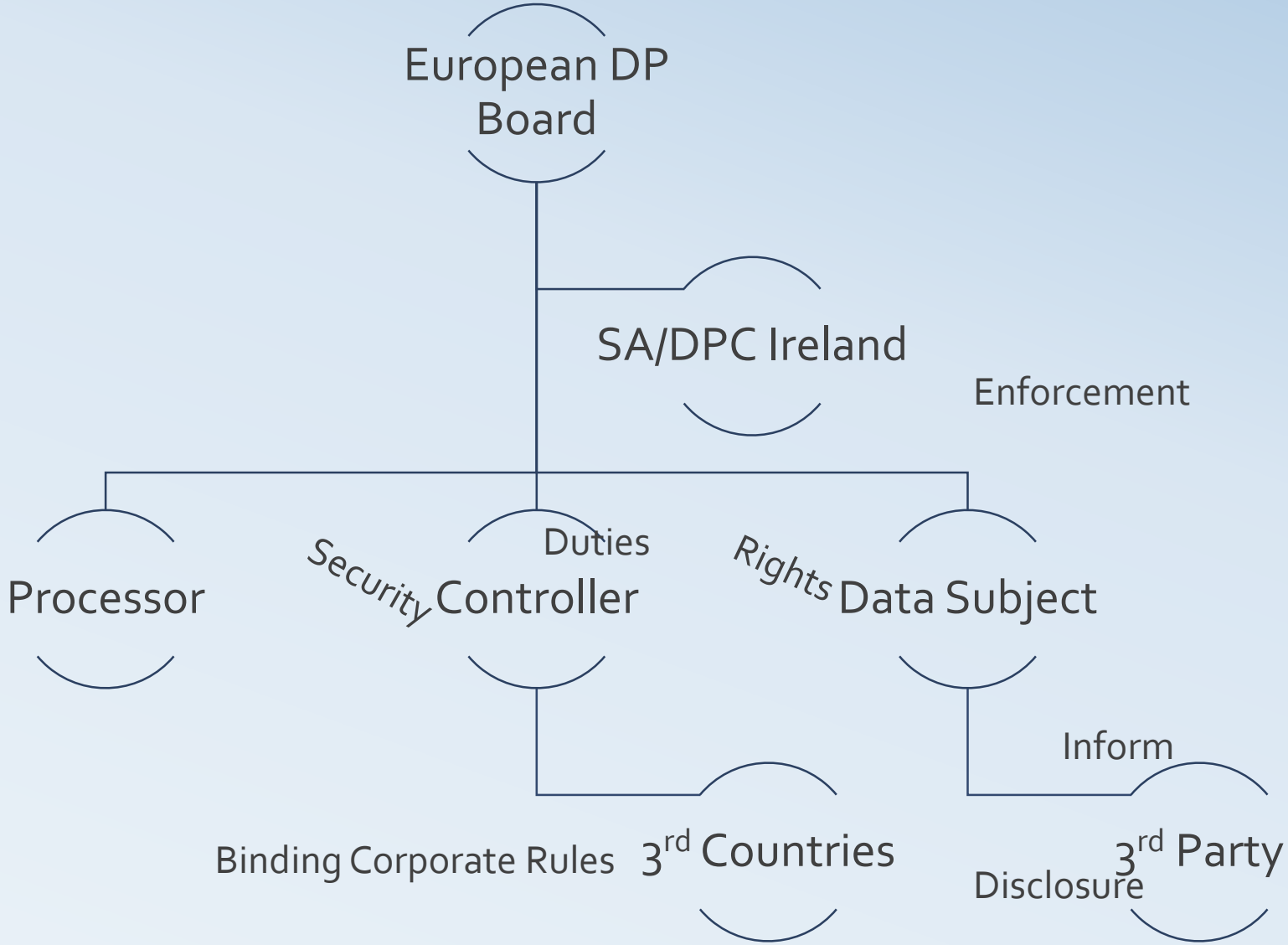
General Data Protection Regulation

- The GDPR (Regulation (EU) 2016/679 of the 27th of April 2016 comes into force on the 25th of May 2018
- This regulation repeals and replaces Directive 95/46/EU and the Irish data Protection Acts of 1988 and 2003
- The first significate item to note is that this is a **Regulation** and not a **Directive** and does not require any Local Law to facilitate it. It is to be adopted immediately by all member states and those that process EU natural persons data be they processing the data in the EU or not.
- There is no local interpretation it is a full harmonized regulation across all members states.

GDPR –Articles of Significant Importance

1. •General Provisions
   •Art 1-4
2. •Principles
   •Arts 5-11
3. •Rights of the Data Subject
   •Arts 12-23
4t. •Controller & Processor
   •Arts 24-43
5. •Transfer of Data to 3rd Countries
   •Arts 44-50
6. •Independent Supervisory Authority
   •Arts 51-59
7. •Cooperation & Consistency
   •Arts 60-76
8. •Remedies & Liability, Penalties
   •Arts 77-84
9. •Provisions relating to Specific Processing Situations
   •85-91

The GDPR Model



Step 1. Install a Data Privacy Officer (DPO)

- DPO is required for business with over 250 Employees or those that process large volumes of PII or personal data. Any organisation can employ a DPO if they wish regardless if obliged.
- DPO must have the relevant professional expertise to hold the position and a full understanding of data protection law.
- Reports to the highest level of management in the company (board level).
- Operates independently and can not be dismissed or penalised for preforming their tasks.
- First point of contact with the Supervisory Authority(SA) and individuals whose data is processed.
- DPO minimum tasks are laid out in Article 39.
- Provide training to all Employees where required.

Step 2. Understand the GDPR –SIGNIFICANT CHANGES

Privacy by Design	Right to be Forgotten	*Self Regulation & Certification*	Rights of Data Subject Strengthened
Access to Data	Big Fines & Rights to Compensation	Data Security	Extra Territoriality of the Regulation

Article 1-3 Who and Where are Data Subjects

- Article 1
  - This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.
  - This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.
  - The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.
- Article 2
  - This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.
- Article 3
  - This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
  - It also applies to controllers not in the EU but who process EU natural persons data

Article 5&6 Lawfulness

- Article 5-Principles relating to Processing personal Data
  - **processed lawfully**, fairly and in a transparent manner in relation to the data subject
  - **collected for specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes
  - **adequate, relevant and limited** to what is necessary in relation to the purposes for which they are processed ('data minimisation')
  - **accurate and, where necessary, kept up to date**; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
  - **kept in a form which permits identification** of data subjects for no longer than is necessary for the purposes for which the personal data are processed; processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

- Article 6-Lawfulness of Processing
  - processing is lawful when Consent is obtained from the data subject or one or more of the obligations of processing under Article 6
  - controllers and processers have clearly defined obligations
  - controllers must provide a contract to processors and are responsible for the processor meeting contractual requirements
  - controllers must also take into account the extra territoriality for meeting regulations

Article 7-9 Consent

- Article 7-Conditions for consent
  - Consent must be clear and affirmative (OPT IN **NOT** OPT OUT)
  - Controller must clearly demonstrate that consent was given
  - Silence or inactivity of the data subject is not consent
  - Written consent must be clear, legible and easy to access otherwise it is not binding.
  - Consent can be withdrawn at any stage in a process as simple as it was to provide consent (in other words you can't make it difficult)
  - **Where you already rely on consent that was sought under the previous acts (95/46/EC) you do not need to obtain fresh consent from individuals if the standard of that consent meets the new requirements under the GDPR(recital 171). You will be required to review the standards in place already to ensure that they meet GDPR requirements**
- Article 8-Conditions applicable to child's consent in relation to information society services
  - Special conditions will apply for Children (under 16) to give consent
- Article 9-Processing of special categories of personal data
  - Consent must be explicit when processing sensitive data
    - gender, race, ethic origin, sexual orientation
    - (New) genetic data and biometric data where processed to uniquely identify and individual
    - Personal data relating to criminal convictions and offences of Data Subjects are not included however similar safeguards will apply to this level of processing (Article 10)

Article 10 & 11

- Article 10- Processing of personal data relating to criminal convictions and offences
  - Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects.
  - Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

- Article 11 - Processing which does not require identification
  - If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation. .
  - Where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.

Article 12 -20 Transparency

- Communication with a Data Subject must be intelligible, concise and completely transparent- no big words and as to consider the level of a child's comprehension
- The Controller must provide details about itself and the use and purpose of data
- A controller must provide the Data Subject with information about their rights and the contact details for the DPO(Article 13)
- Article 14 provides specific provisions where data has not been obtained from the data subject
- Rights of data portability
- (Articles 16-18 cover access, rectification and the "right to be forgotten "erasure
  - Purpose, type of data, recipients of the data, period of time, automation, rectification, rights to restriction of processing, unlawful processing, withdrawal of consent and erasure where the data is no longer necessary to the purpose

Article 21 -22 Right to Object & Automated individual decision making

- Article 21-Profiling data (must adhere to Article 6.(1)), controller must seek consent or where it clearly demonstrates a compelling legitimate ground for processing the data. The Data Subject can object to the use of their data in direct marketing data (which includes profiling) and it shall no longer be used for such purposes.

- Article 22- The Data Subject has the right not to be subject to a decision based solely on automated processing (including profiling). The above shall not apply of the decision
  - Necessary for entering into, or performance of a contract between the Data Subject and Controller
  - Is authorised by the Union or State (safeguards in place for Data Subjects rights)
  - Contain explicit consent for the data subject
  - Data Controller has implemented suitable measures to safeguard the Data Subjects rights and at least provides the right to the Data Subject to Human intervention where the Data Subject can express their point of view and contest the decision

Article 24 - Controller and Processor Obligations & Privacy By Design

"….the Controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this regulation. Those measures shall be reviewed and updated where necessary."

" …shall included the implementation of appropriate data protection policies by the controller"

- Privacy must be *designed into data processing* by default
- Controllers and Processors outside of the EU must have a DESIGNATED REPRESENTATIVE in the EU
- When processing is carried out on behalf of a controller. The controller shall use only a processor that sufficiently guarantees to implement the appropriate technical and organisational measures in such a manner that meets the requirements of the regulation
- Data Audits
  - GDPR requires that all existing and future data meets regulation
  - Privacy can be deigned retrospectively
  - Security of Data must meet the regulation

Article 32-34 - Security and Breaches

Security of Personal Data

- Controllers and processors must implement the appropriate technical and organisational measures to ensure a level of security appropriate to the risk.....
  - pseudonymisation and encryption of personal data
  - Ensure ongoing integrity ,confidentiality ,availability and resilience of processing systems and services
  - Process for testing, evaluating the security measures of system
  - Security measure taken to meet Privacy by Design (to meet the measure of the data not the other way around)

Data Breach

- Data Breach notification to the SA must happen within 72 hours, if there is any delay it must have a valid reason. Data Breach notification to a Data Subject must happen without undue delay
  - If you can provide proof that the Data Breach is secured (encryption or other measures of security)and that no data has been breached (cyber attacks) you do not need to notify the Data Subject
- Data Privacy Impact assessment are mandatory(Article 35) where the data processing is considered high risk to the rights of the Data Subject
- Significant measures must be taken to prevent a Breach and mitigate the potential consequences
- Data breach reporting process should be set in place as best practice

Article 40-43 - Code of Conduct & Certifications

- Requirements for an Organisation to apply appropriate measures. These can be demonstrated through the following:
  - Creation of Codes of Conduct
  - Meeting International Standards such as ISO /IEC 27001 or equivalent
    - https://www.iso.org/isoiec-27001-information-security.html
  - Recognised Technical Standards
  - New standards emergence such as Privacy Seals
- Monitoring of approved codes
  - A body with the appropriate level of expertise in relation to the subject matter of the codes and is accredited by the SA can without prejudice to the powers of the competent SA (Article 57 and 58) can monitor or approve a code of conduct
- Certification
  - Certification Bodies are as above
  - Approved by the SA
  - Have established procedures for issuing, periodic review and withdrawal of data protection certs , seals and marks.

Article 44 - 50 -Transfer of personal data to 3rd countries or international organisations

- Transfer of Personal Data to 3rd Countries/International Organisations must meet the following compliance.
  - Based on adequacy
  - Binding corporate rules- **contract** with company and where you can enforce legislation against them for not meeting obligations
  - Safeguards must be in place
  - All protection in place must ensure that the protection of the data subject (natural person) is not undermined
    - Rule of law, human rights, fundamental freedoms and relevant legislation are just some of the considerations before transfer of data is allowed- this is part of adequacy
  - It is noted that Cloud Service Providers are the highest of risk (adequate level of protection must be taken into account)
  - Data of EU Subject **can not** be transferred unless the protection of the natural person is met

- In October 2015 EU Court of Justice declared Safe Harbour (US) ***Invalid***
- April 2016 – Serious Flaws in Privacy Shield (US)
  - Does not meet EU Standards
  - Indiscriminate collection of personal data for national security purposes
  - Insufficient legal remedies
  - Lack of data retention principles
  - Privacy Shield discussions are ongoing

Article 51 -59 Supervisory Authority

" Each member state shall provide for one or more independent public authorities to be responsible for monitoring the application of this regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union".

Each State Must:

- *Recourse the SA appropriately*
- *Independent in their own right - can not be circumvented*
- *Monitor & enforce*
- *Communicate*
- *Promote Public Awareness*
- *Lead SA for Multi –State Operators*
- *The SA is given powers to*
  - *Enforce*
  - *Advise*
  - *Correct*
  - *Investigate*

Article 60 + Supervisory Authority Cooperation & EDPB

" In order to contribute to the consistence application of this Regulation through the union Supervisory Authorities shall cooperate with each other and, where relevant , with the Commission, through consistency mechanism as set out in the articles……"

European Data Protection Board ensures the:

- Cooperation
- Communication
- Consistency
- Mutual Assistance between the National Supervisory Authorities
- Monitors and ensure the correct application of the Regulation
- Examination of any questions in the Regulation application
- It provides for a level and harmonised playing field

Article 77-84Remedies, Penalties and Liability

- Article 79: *Right to an effective judicial remedy against a controller or processor*
  - *Where rights have been infringed due to the processing of personal data*
    - *Courts of the Member State in where the controller or processor is established*
    - *Courts of the Member State where the data subject resides*

- Article 82: *Right to compensation and Liability*
  - *Any person who has suffered material or non material damage shall have the right to compensation from the controller or processor*
  - *Controller involved in processing shall be liable for the damage caused in the processing*
  - *No limit set in compensation (subject to the court decisions)*

- Article 83: General Conditions for imposing administrative fines
  - Imposition of administrative fines will be in each case effective, proportionate and dissuasive
  - **€ 10 000 000** , or in the case of an undertaking, up **to 2 % of the total worldwide annual turnover** of the preceding financial year, whichever is higher.
  - **€ 20 000 000** , or in the case of an undertaking, up **to 4 % of the total worldwide annual turnover** of the preceding financial year, whichever is higher.
  - Article 83 ,section 7 –" without prejudice to the corrective posers of the SA pursuant to Article 58(2) each Member state may lay down rules on whether and to what extent administrative fines mat be imposed on public authorities and bodies established in that Member State

RECAP

- *This is a significant enhancement of Data Protection since its inception*
- *Applies to all Member States*
- *Applies to all organisations processing EU Citizens data not matter where they are geographically*
- *Specific updates on Consent, Erasure, Right of Data Subject, Fines, Obligations of Controllers and Processors*
- *Data Privacy Officers*
- *Powers of the SA*
- *Certification and Seal*
- *Significant Penalties and Fines – which take into account technical and organisational measures*
- *Data Subject can seek Judicial Remedy*

Step 3.If you have not started your Data Privacy Program and Updates now, you are reaching the red-line of too late!

Resource Spot

- Regulation (EU) 2016/679
  - http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN
- Data Protection Commissioner (Supervisory Authority)
  - https://www.dataprotection.ie/docs/Home/4.htm
- ADPO –Association of Data Protection Officers
  - https://www.dpo.ie/
- Reading Material (Historical Context on the Why Privacy is Important)
  - https://en.wikipedia.org/wiki/IBM_and_the_Holocaust

THE WARD GROUP

AML& CFT
Best Practice Approach
Local Authority's

Current Legislation

3RD EU money Laundering Directive (2005/60/EC) for which was trans positioned into the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (CJA 2010) and which was amended under the Criminal Justice Act 2013 and in such transposes the Third Money Laundering Directive (2005/60/EC) and its implementing directive 92006/70/EC) into Irish Law.

New Legislation

4AMLD (Directive 2015/8/49)

- The 4th Anti-Money Laundering Directive 2015/8/49 (4AMLD) and the associated Funds Transfer Regulation (FTR) was agreed on the **25th of June 2015** at EU level.
- The negotiations were led by the Department of Finance in consultation with other relevant departments, agencies and stakeholders. A series of terrorist attacks in Europe during 2016 and revelations in the Panama papers prompted the EU Commission to propose a number of amendments to 4AMLD in July 2016 and these proposed changes are now under consideration by the European Parliament.
- (4AMLD,) together with amendments will come into force in Ireland on the **26th of June 2017,** it will update and replace the existing 3AMLD / FTR framework and will better align EU law with the FATF's revised international standards on AML/CFT.

Obliged Entities within the Legislation

The legislation imposes obligations in terms of money laundering and terrorist financing on a wide range of legal persons (referred as 'designated persons 'within the legislation) including:

- Credit and Financial Institutions
- *Property Service Provider*
- Independent Legal Professionals
- Auditors, external Accountants or Tax Advisers
- Trust or Company Service Providers
- Dealers in High Value Goods (Cash Transactions)
- Private Members' Clubs

Notable Areas of Legislation

- **Notable Areas of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010**
  - Requirement for CDD by Designated Person(s) - sections 33 to 40
  - Requirement of Designated Person(s) for awareness of complex or unusual activity- section 33(2)
  - Special measures to be applied by the Designated Person(s) to monitor the ongoing business relationship - section 35
  - Requirement of Designated Person(s) to investigate PEP and Beneficial ownership outside the state- section 37
  - Legal requirement of Designated Persons to report suspicious transactions to the Garda Siochana and the Revenue Commissions and the obligation to "Tipping Off" sections - 41 to 53

- **Notable Changes to Current Legislation under (4AMLD)**
  - Enhanced risk – based approach (a lot more prescriptive than previously) requirement of the obligated entities to assess the risk of each of its personal business relationships and transactions with regard to ML & TF
  - Beneficial Ownership and Trustee Beneficial Ownership - A central registry is to be created and updated and the information shared to a competent authority
  - PEP's (Politically Exposed Person(s)) both domestic and foreign - enhanced risk based approach
  - Amendments to SDD (Simplified Due Diligence) has been removed and the continuation of the use of SDD must be proven where the risk in the business relationship is considered low
  - Property Service providers are now included as obligated entities
  - HVGD's cash transaction value has been reduced from €15k to €10k

Local Authority-Best Practice Consideration

Although Local Authorities are not directly obligated within the requirements of the legislation, certain factors such as the acceptance of cash should be considered.

Compliance with the Legislation and it requirements is a "Best Practice Approach" and shows the commitment of the Local Authority to meeting highest possible standards that are proportionate to the risk associated through the implementation of AML & CFT safeguards and reporting processes.

AML & CFT Measures -Why?

According to (NRA) *National Risk Assessment Ireland*

" the use of cash for Money Laundering and Terrorist Financing is seen as one of the key vulnerabilities by National and International (AML)Anti-Money Laundering & (CFT) Combating the Financing of Terrorism regimes"

" with an estimated 46% to 82% of all transactions in all countries being conducted in cash"

"the inherent risk in the use of cash reinforces the need for AML & CFT measures in sectors such as HVGD's, cash-based businesses, gambling and MVTS's,(Money or Value Transfer Service) amongst others"

AML & CFT measures protect not just your business, your name but also your community and country

ML & TF- What does it support

- Drugs
- Human Trafficking
- Child Pornography Rings
- Black Market Economy
  - Fuel
  - Tobacco
  - Alcohol
- Terrorism (Berlin, Paris, London, Brussels, New York , Istanbul)
- Prostitution

Local Authority Steps to Best Practice

- Utilise a risk based approach for (CDD) Customer Due Diligence
  - Acquire the identifying information
  - Risk Banding by risk assessment
- Establish the Business Relationship
  - Contractual relationship between the parties
  - Transparency of funds
  - Signatories and Beneficial Ownership
  - Transaction Types - Occasional or Linked Transactions
- Transaction Reporting & Monitoring Controls and Review
  - Cash Transaction Reporting
  - Suspicious Transaction Reporting- Statutory Obligation
  - Ongoing monitoring of BO and customer transactions and risk category
- Staff Training & MLRO/Designated Person
  - Appointment of MLRO
  - Ongoing recorded training of all staff members where awareness is required
- Breaches, Fines and Sanctions
  - Brand Impact
  - Impact of Tipping off (indirectly or purposefully)
  - Imprisonment of DP or MLRO on Breach

Local Authority Considerations

- The LA is committed to the prevention, detection and reporting of money laundering and has a zero tolerance approach to fraud of all kinds.
- All employees must be vigilant for the signs of money laundering and be trained should their position require so.
- Any employee who suspects money laundering activity must report this promptly to the Money Laundering Reporting Officer or Designated Person (Manager).
- No payment to the LA should be accepted in cash if exceeding €10,000 as a single or linked transaction.
- Where the LA is carrying out certain regulated activities by way of business, then the customer due diligence procedure should be followed using the risk based approach.

Resource Spot

- AMLCU
  - http://www.amlcu.gov.ie/website/aml/amlcuweb.nsf/page/legislation-en
- Department of Finance
  - http://www.finance.gov.ie/what-we-do/banking-financial-services/financial-services-division-2-eu/anti-money-laundering-counter
- 4th EU Anti-Money Laundering Directive and Funds Transfer Regulation
  - http://www.finance.gov.ie/sites/default/files/AMLD%20National%20Discretions%20Consultation%20Paper.pdf
- FATF-Guidance Documentation and Risk Assessments
  - http://www.fatf-gafi.org/home/

Contact Details

Paula Carney-Hoffler E.I.I.C.M Credit Mgt.Cert,DipLaw

Client Credit Risk & Compliance Manager

Hugh J Ward & Co Solicitors

9 Seville Place

Dublin 1

Email: PCarney-Hoffler@hughjwardsolicitors.ie