Information & Communication Technology Law

E-Commerce

Lecturer: Alexia Valenzia
Date: 21st May 2025

Diploma in Law (Malta)

CAMILLERI PREZIOSI

Electronic Contracts

- Electronic Contracts are governed by the Electronic Commerce Act (Cap. 426, Laws of Malta) (the **"E-commerce"** Act**).** Art. 9(2) allows contracts to be formed and concluded electronically.

- The above establishes that any offer, acceptance of an offer and any related communication (including any subsequent amendment), cancellation or revocation of the offer and acceptance of the contract may, unless otherwise agreed by the parties to the contract, be communicated electronically.

Electronic Contracts

- Art. 10 provides that E-contracts are legally valid in Malta and deemed to be formed when the recipient of the service has received an acknowledgement of receipt from the service provider (after an order is placed).

- Both the placement of an order and the acknowledgement of receipt are deemed to have been received when the addressee is able to access them and thus, the electronic contract is deemed to be concluded.

- Can take the form of any contract which is concluded wholly or in part through electronic communications or in an electronic form. When this is done through terms and conditions, these must be made available in a way which can be stored and reproduced.

Mandatory Requirements

- Art. 11 provides for information which is mandatory in electronic contracts and must be provided in a clear, comprehensive and unambiguous manner. This includes:
  - the name, address and email of the service provider;
  - the registration number of the service provider in any trade register or of any professional body (if applicable);
  - where the activity is subject to an authorisation, the activities covered by the authorisation and the particulars of the authority granting such authorisation;
  - the valued added tax (VAT) number of the service provider (if the service provider undertakes an activity subject to VAT);
  - the different steps that must be followed to conclude the contract;
  - the technical means for identifying and correcting input errors prior to the placing of the order;

Mandatory Requirements

- the language(s) in which the contract may be concluded;
- a statement of whether the concluded contract will be filed by the service provider and whether it will be accessible; and
- in relation to a regulated profession:
- any professional body or similar institution with which the service provider is registered;
- the professional title and the member state where it has been granted; and
- a reference to the applicable professional rules in the member state of establishment and the means to access them.

Restrictions

- The E-commerce Act excludes concluding transactions through e-contracts in relation to:
  - taxation;
  - information society services matters that are covered by data protection laws;
  - agreements or practices governed by competition law; and
  - the following activities of information society services:

  (a) the representation and defence of a client before the courts; and

  (b) gambling activities involving the wager of a stake with monetary value in games of chance, including lotteries and betting transactions.

E-Signatures

- Electronic signatures are legally valid in Malta and are regulated under the E-commerce Act and the EU eIDAS Regulation (910/2014).

- The latter defines an 'electronic signature' **("ES")** as "data in electronic form that is attached to, or logically associated with, other data in electronic form and which is used by the signatory to sign".

- 'advanced electronic signature' **("AES")** means an electronic signature which is uniquely linked to the signatory, is capable of identifying said signatory, is link created using electronic signature creation data that can be used under the signatory's sole control, and is ed to the data signed in a manner in which any subsequent change in the data is detectable.

- 'qualified electronic signature' **("QES")** means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures;

Legal Effects of Electronic Signatures

- Art. 9 provides that an electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures.

- A qualified electronic signature based on a qualified certificate issued in Malta shall be recognised as a qualified electronic signature in all other Member States.

Limitations

- Art. 23 of the E-Commerce Act provides rules against the misuse of e-signatures, particularly by forbidding:
  - Accessing, copying or obtaining in any other manner the electronic signature creation device pertaining to another person for the purposes of creating an unauthorised e-signature.
  - Any other fraudulent or unlawful alteration or creation of e-signatures.

Uses in Malta

- The use of e-signatures in Malta is largely dependent on the requirements of the particular businesses entering into the contract in question.

- There is no mandatory requirement for the use of e-signatures for any particular form of contract, and parties are free to adopt either of traditional paper signatures or e-signatures due to their equal legal value at law.

- It is worth noting that the Maltese Government has widely implemented the use of electronic identity verification (eID) as an authentication tool for its online services.

The EU Data Act

- The EU Data Act is the second main legislative proposal forming part of the EU's wider 'European Strategy for Data' adopted by the Commission in February 2022.

- Seeks to make data sharing and the use/reuse of data easier for all by setting standards at an EU-wide level. The EU Data Act covers aspects of the use of various business-to-business and government-to-business data across all sectors in relation to the use of various data.

- Entered into force on 11 January 2024 and will become applicable in September 2025

- Applicable to:
  - manufacturers and providers of products and related services placed on the EU market and the users of such products and services;
  - data holders that make data available to data recipients in the EU;
  - businesses that are data recipients in the EU to whom data holders make data available;
  - businesses providing data processing services (e.g., cloud services) to customers in the EU; and
  - public sector bodies in the EU.

The EU Data Act – Key Principles

- **Design** – connected products and related services should be designed and made to allow, by default, easy and secure access by users (who could be either consumers or business users) to data generated through their use.

- **Transparency** – before a contract is concluded for the purchase, rent or lease of a connected product or a related service, certain information must be provided to the user in a clear and comprehensible format, particularly regarding the nature and volume of data likely to be generated by the use of the product or services, how the user may access said data, and how the manufacturer/service provider intends to use the data itself or allow third parties to do so.

- **Right of users to access and use data generated by connected products or related services** – where data cannot be directly accessed by the user from the product or related service, the data holder must make available to the user the data generated by the product or related service without undue delay, free of charge and, where applicable, continuously and in real time. Various related provisions govern:
  - how access must be provided;
  - protection of trade secrets and competition; and
  - protection of personal data where the user is not the data subject

The EU Data Act – Key Principles

- **Protection of users' commercial interests** – data holders may only use non-personal data generated by the use of a connected product or related service if a written contract is in place with users. The data holder may not use the data to derive insights about the economic situation, assets and production methods of, or the use of the data by, the user that could undermine the commercial position of the user in the market in which it operates.

- **Sharing data with third parties in accordance with user instructions** – obligation on holders of data from connected products or related services to make the data available to third parties of the user's choice. Users can authorise data to be given to other third parties and it should be easy for the user to refuse or discontinue access by the third party to the data.

The EU Data Act – Key Principles

- **Compensation for data** – data holders can require "reasonable" compensation from the data recipient for making the data available. Compensation must be fair, non-discriminatory and reasonable. For SMEs, it must not exceed the actual cost of making the data available.

- **Dispute resolution** – the EU Data Act includes provisions for member states to establish dispute settlement bodies to resolve disputes between data holders and data recipients in relation to the determination of fair, reasonable and non-discriminatory terms for and the transparent manner of making data available.

- **Sharing data with public bodies** – obligation to provide certain data to public bodies in exceptional circumstances, such as in response to a public emergency or to fulfil legal obligations.

Requirements for Smart Contracts for Data Sharing Under the Data Act

The essential requirements for smart contracts for data sharing are set out in Article 36(1) of the Data Act:

(a) robustness and access control, to ensure that the smart contract has been designed to offer access control mechanisms and a very high degree of robustness to avoid functional errors and to withstand manipulation by third parties;

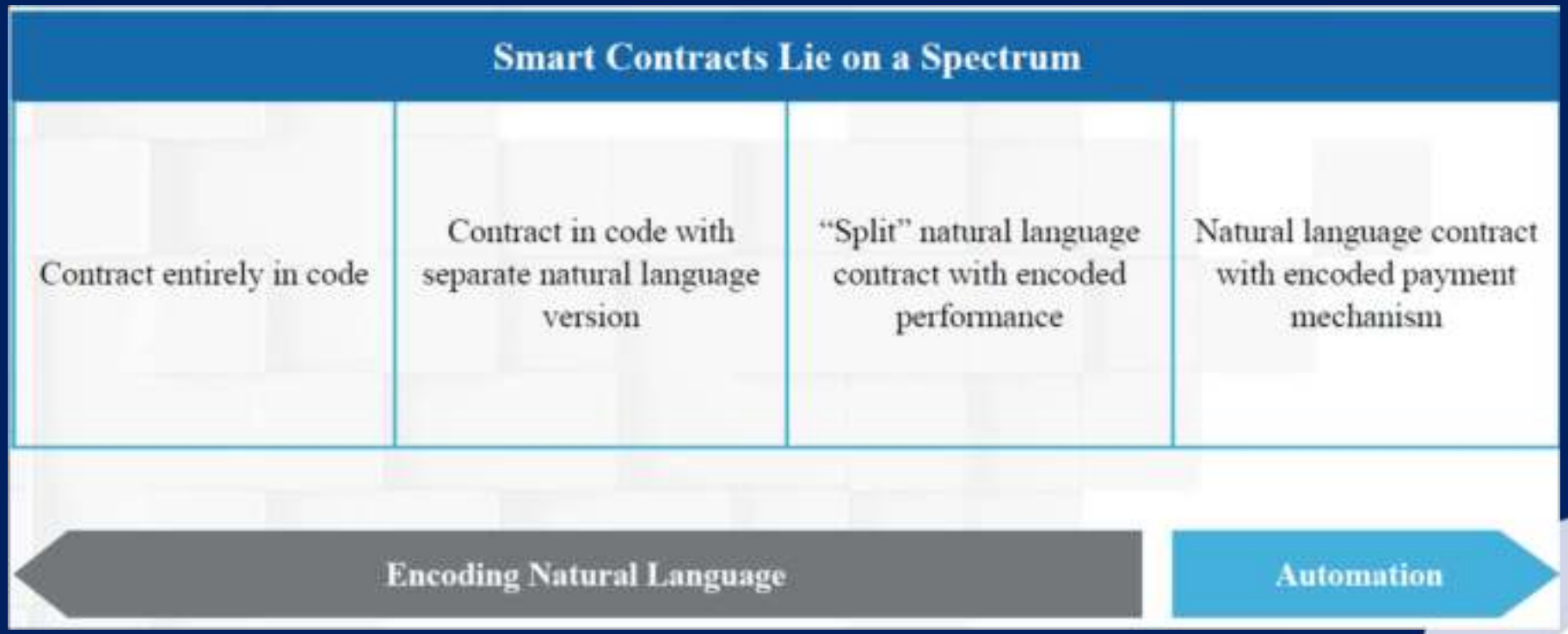
(b) safe termination and interruption, to ensure that a mechanism exists to terminate the continued execution of transactions and that the smart contract includes internal functions which can reset or instruct the contract to stop or interrupt the operation, in particular to avoid future accidental executions;

(c) data archiving and continuity, to ensure, in circumstances in which a smart contract must be terminated or deactivated, there is a possibility to archive the transactional data, smart contract logic and code in order to keep the record of operations performed on the data in the past (auditability);

(d) access control, to ensure that a smart contract is protected through rigorous access control mechanisms at the governance and smart contract layers; and

(e) consistency, to ensure consistency with the terms of the data sharing agreement that the smart contract executes.

Types of Smart Contracts



Types of Smart Contracts

- **A natural language contract with automatic performance by code:**

code does not define contractual obligations but is used to perform obligations. The code itself falls outside the scope of the legally binding part of the agreement.

- **A hybrid contract:**

some contractual obligations are defined in natural language and others are defined in code. Some or all the obligations are performed automatically by the code. The same contractual terms can be written in both natural language and code, and the natural language terms can be incorporated in an accompanying natural language agreement or in natural language comments included in the code.

- **Contract recorded solely in code:**

all the contractual terms are defined in and performed automatically by the code and there is no natural language version of the agreement or any part of it. This type of smart contract is likely to be rare in practice.

Smart Contracts – Limitations

- Feasibility of applying smart contracts may significantly vary by business case.

- **Inflexibility:**
- interest in smart contracts among enterprises can be largely attributed to the automation capabilities that this technology implies. However, the majority of commercial relationships are complex in nature.
- Accounting for all possible contingencies and nuances in a contract is impossible both in written and digital agreements.

Smart Contracts – Limitations

- **Link to the real world:**
- Many contractual agreements require some sort of a link to the real world, which hinders the promise of smart contracts to be fully autonomous.
- While certain aspects can be verified from trusted sources (such as stock prices, or weather conditions), a number of cases require one's physical presence to be verified.
- Many contractual obligations that fall into the off-chain category can't be objectively measured and computationally verified. For example, the notion of reasonableness may not be captured by binary logic.

Smart Contracts – Limitations

- Enforceability is not guaranteed but dependent on whether national legislation caters for the validity (and therefore, enforcement) of the smart contract.

- Parties will need to rely on a trusted, technical expert to either capture the parties' agreement in code or confirm that code written by a third party is accurate.

- No simple path to amend a smart contract, creating certain challenges for contracting parties

Questions

- What are the key principles within the EU Data Act?
- Name the four essential requirements for smart contracts under the EU Data Act.
- What are the three main forms that smart contracts may take?
- Mention certain limitations of employing smart contracts for daily business activities.

Payment Services

- Directive 2015/2366 **("PSD II")** aims to regulate the payments industry and to enhance consumer protection, improving upon PSD I which did not accurately reflect how some payment methods operate.

- Previously, certain payment service providers **("PSPs")** escaped regulation under PSD 1. PSD 1 also required a revision due to the rapid technological changes in this sector.

- PSD II covers both public law aspects regarding the supervision of PSPs, and private law aspects relating to the rights and obligations related to the offering and use of payment services.

Positive Scope

- Extension of the application of the transparency requirements concerning the conditions and information requirements regarding:
  - Payment transactions in a currency that is not that of a Member State where the payment service provider of both the payer and payee are located in the EU, where it concerns transactions in the EU; and
  - Payment transactions in all currencies where only one of the payment service providers is located in the EU (“one leg principle”), however, limited to transaction carried out in the EU.

Introduction of New Payment Services

- **Payment initiation services**, which help consumers make online payments and inform the merchant immediately of the payment initiation, allowing for the immediate dispatch of goods or immediate access to services purchased online;

- **Account information services**, which give consumers and businesses an overview of their financial situation by consolidating information across the different payment accounts they may have with one or more payment service providers;

- **Issuance of card-based payment instruments** by third-party payment service providers that request confirmation of the availability of funds from the payment service provider servicing the account.

Liability

- The PSD2 clarifies liability issues between the bank holding the account and the payment initiation service provider.

- In case of an unauthorised payment transaction initiated through a payment initiation service provider, the account-servicing payment service provider must refund the payment service user.

- If the payment initiation service provider is liable for the unauthorised payment transaction, it must immediately compensate the account-servicing payment service provider.

Consumer Protection

- The PSD2 enhances consumer protection. In case of an unauthorised transaction, the payment service user must be refunded immediately.
- The payment service user is not liable if it was not possible for him/her to be aware of a loss that resulted from theft or misappropriation of the payment instrument (e.g. copied payment cards).
- In other cases of lost or stolen payment instruments (e.g. a lost wallet), the payment service user can be held liable for a maximum of €50, provided he/she fulfilled the obligation to notify the payment service provider and did not act in a grossly negligent or fraudulent manner.
- Payment users have an eight-week unconditional refund right for direct debits in euro

No Surcharge on Payments

- The PSD2 prohibits merchants from charging consumers additional fees for specified payment methods.

- The surcharge ban applies where the consumer's bank or card issuer and the payment service provider of the merchant are both located in the European Economic Area (EEA) and the consumer makes a payment either using a debit or credit card, or by direct debit or credit transfer.

- Even when the surcharge ban does not apply, the amount of any surcharge imposed cannot exceed the cost incurred by the merchant in accepting the particular payment method.

Increased Security

- A PSP must apply strong customer authentication where the payer:

(a) accesses its payment account online;

(b) initiates an electronic payment transaction;

(c) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.

- For remote transactions (e.g. online payments), the security requirements require a dynamic link to the amount of the transaction and the account of the payee, to further protect the user by minimising the risks in case of mistakes or fraudulent attacks.

- Exemptions from the requirement to have strong customer authentication, for example for low-value payments at the point of sale or for remote transactions.

Increased Security

- The PSD2 sets out strict security requirements for electronic payments and the protection of consumers' financial data. Payment service providers are required to ensure strong customer authentication for the initiation and processing of electronic payments.

- Customer authentication is a process whereby the identity of the user of a payment service is validated. Customer authentication is considered to be strong if it is based on the use of two or more of the following elements:
  - Knowledge – something only the user knows (PIN);
  - Possession – something only the user possesses (Card);
  - Inherence – something the user is (Fingerprint);

Questions

- What were the main issues within the previous Payment Services Directive? ("PSD I")?
- How is PSD II beneficial for consumers?
- What additional security requirements were introduced?

Electronic Money

- Electronic money (e-money) is broadly defined as an electronic store of monetary value on a technical device that may be widely used for making payments to entities other than the e-money issuer.

- The device acts as a prepaid bearer instrument which does not necessarily involve bank accounts in transactions.

- The second Electronic Money Directive 2009/110/EC ("EMD2") defines 'electronic money' as "electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions […] and which is accepted by a natural or legal person other than the electronic money issuer".

Electronic Money

- E-money products can be hardware-based or software-based, depending on the technology used to store the monetary value.

- In the case of hardware-based products, the purchasing power resides in a personal physical device, such as a chip card, with hardware-based security features. Monetary values are typically transferred by means of device readers that do not need real-time network connectivity to a remote server.

- Software-based products employ specialised software that functions on common personal devices such as personal computers or tablets. To enable the transfer of monetary values, the personal device typically needs to establish an online connection with a remote server that controls the use of the purchasing power. Schemes mixing both hardware and software-based features also exist.

Summary of Changes from EMD 1

- The Electronic Money Directive (EMD1) was revised in 2011 (EMD2).
- Electronic money issuers are not allowed to grant interest or other benefits related to the length of time the electronic money is held.
- The initial and minimum on-going capital requirement for authorised electronic money institutions is reduced from €1 million to €350,000, to reduce the potential that this might be a barrier to entry.
- EMD2 requires authorised electronic money institutions to safeguard funds received from customers for electronic money so that, if there is an insolvency event, the electronic money issued would be protected from other creditors' claims and can be repaid to customers.

Summary of Changes from EMD 1

- Restriction on business activities of electronic money institutions was removed. This allows them to provide unrelated payment services without additional authorisation and to engage in other business activities.

- Electronic money issuers are no longer allowed to set a minimum threshold of redemption nor will they be able to set a time limit on the holder's right to redeem.

Distance and Online Selling

- Regulated by the Consumer Rights Regulations (S.L 378.17), which defines a ‘distance contract’ as “any contract concluded between the trader and the consumer without the simultaneous physical presence of the trader and the consumer, with the exclusive use of one or more means of distance communication up to and including the time at which the contract is concluded”.

- Entails certain information requirements on the trader, as well as provides various rights to the consumer for the good or services received.

Consumer Rights – Legal Guarantee

- The law provides that goods purchased by consumers must be as described by the trader, fit for the purpose and have the qualities and performance which are normally found in goods of the same type.

- If this is not the case, consumers can ask for a free of charge remedy from the trader. The time-limit for the free remedy is two years from the date the product purchased came into the consumer's possession.

- The remedies provided in the legal guarantee are:
  - Repair
  - Replacement
  - Part or full refund

- Consumers would not be entitled for these remedies, however, if the defect in the product is the result of some kind of misuse. During the first year, if the product is defective, it will be considered as a latent defect, unless the trader does not prove otherwise.

Repair

- When a good develops a fault, the trader has the right to first choose to repair the product free of charge. The repair, however, should be carried out within a reasonable period of time and without causing any significant inconvenience to the consumer.

- The period of the guarantee will be suspended until the product is repaired and given back to the consumer. The suspended time shall then be added with the guarantee

Replacement

- Replacement of defective or non-conforming goods can be chosen if the product cannot be repaired or if the repair would cause significant inconvenience to the consumer.

- When a product is replaced, the two year legal guarantee does not start over again with the replaced product, but will continue from the original date of purchase.

Part or Full Refund

- A part or full refund of the money paid for the product may be claimed when repair or replacement of the product are either not possible or if opted for may cause a significant inconvenience to consumers

- One is not entitled to request a full refund when the lack of conformity is only minor or insignificant or when the product has been used for quite some time.

Information Requirement

- Art. 5 imposes certain information which the consumer should be provided with **prior** to entering into the distance/off-premises contract. This includes:
  - A clear description of the main characteristics of the goods or services offered for sale;
  - The identity of the trader (such as trading name, address and contact number);
  - The total price of the goods and services, including taxes and additional charges (e.g. delivery charges);
  - The cost of using the means of distance communication if the charge is more than the basic rate;
  - The method of payment and by when the goods will be delivered or in case of services when these will be performed;

Information Requirement

- The duration of the contract or, if the contract is of indefinite duration, the conditions for terminating the contract;
- The right of withdrawal if it is applicable to the sale being concluded;
- A reminder of the existence of a legal guarantee of conformity for goods;
- Where applicable, the existence and the conditions of after sales customer assistance, after sales service and commercial guarantees.

Right of Withdrawal

- Before concluding such contracts, consumers should also be informed about their right of withdrawal, which amounts to **14 days**.

- When exercising their cancellation rights, consumers do not have to give any reason and must not incur any costs, except the cost of returning the unwanted goods back to the seller. This cost will however be incurred by the seller if the consumer was not informed of such cost beforehand.

Right of Withdrawal

- In both distance and off-premises contracts, the cancellation period starts from the day consumers acquire physical possession of the goods.

- In the case of services, the withdrawal period expires after 14 days from the conclusion of the contract.

- If consumers are not informed about the withdrawal period, the right to cancel the sale will be extended to 12 months or will start when consumers are informed about it.

Right of Withdrawal

- When the right of withdrawal does not apply, consumers must be informed accordingly.

- When deciding to cancel a sale during the 14 days cooling off period consumers will need to either fill in the withdrawal form provided by the seller at the time of purchase or write to the seller about their intentions to cancel the sale.

- It is the consumers' responsibility to have proof of having cancelled the sale within the stipulated time-limit.

Exceptions

- When the service has begun with the consumers' consent and with the knowledge that they are forfeiting the right of withdrawal;
- Supply of goods and services, which price depends on fluctuations in the financial market;
- The supply of goods which are liable to deteriorate or expire rapidly;
- The supply of sealed goods which are not suitable for return due to health protection or hygiene reasons and were unsealed after delivery;

Exceptions

- The supply of newspapers, periodicals and magazines except for subscription contracts for the supply of such periodicals;
- Sales contract concluded at a public auction;
- The supply of digital content which is not supplied on a tangible medium if the performance has begun with the consumers' prior express consent and their acknowledgement that they thereby lose their right of withdrawal.

Right to Redress

- If the product purchased through a distance means of communication or off-premises turns out to be faulty, or not as described before the sale was concluded, consumers have the same legal rights as when they buy goods personally from a shop.

- Hence, consumers would be entitled to claim a legal remedy, which may be either repair or replacement, or else part or full refund. The time limit to claim these remedies is two years from purchase.

The Commercial Warranty

- This type of guarantee is not obligatory. In fact, it is given to the consumer voluntarily by the seller when buying certain goods, for example cars or electronic goods.

- This, however, does not replace the legal warranty but should provide the consumer with additional benefits.

- If the product is returned to the trader to be repaired or replaced as per the commercial guarantee's terms and conditions, the guarantee is automatically extended by the period during which the guarantor had the goods in his possession while executing the repairs.

The Commercial Warranty

- A commercial guarantee should be written clearly, in plain language, in either Maltese or English, and should include the following details:
  - The name and address of the guarantor
  - The length of the commercial guarantee and when it starts
  - Description of the goods and services that are covered by the warranty
  - Contents, including territorial scope if limited
  - Instructions on how the consumer should claim remedy under this guarantee and an address where claims can be sent
  - The remedies offered to the consumer under the guarantee if there is a defect
  - Declaration of whether the consumer can transfer the guarantee to others – if not specified, subsequent owners will have the right to avail themselves of the guarantee.

Questions

- Differentiate between the Legal and Commercial Warranties.
- What remedies are provided to the consumer under the Consumer Rights Regulation?
- What rights does the consumer have when purchasing goods or services at a distance?
- Are there any exceptions to the above rights/remedies?

Digital Content Directive

- The Digital Content and Digital Services Contracts Regulations (S.L 378.20) were published by means of Legal Notice 406 of 2021 on the 29 October 2021, and came into force on 1 January 2022.

- The purpose of these Regulations is to transpose Directive (EU) 2019/770 of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content and digital services.

- Applicable to any contract where the consumer pays or undertakes to pay a price; or when the consumer provides personal data in exchange for a service that is provided without payment.

Digital Content Directive

- Lay down common rules on certain requirements concerning contracts between traders and consumers for the supply of digital content or digital service, in particular, rules on:
  - the conformity of digital content or a digital service with the contract;
  - remedies in the event of a lack of such conformity or a failure to supply, and the modalities for the exercise of those remedies, and
  - the modification of digital content or a digital service.

- Consumers are now protected when digital content and digital services are faulty; a protection which previously only existed for tangible goods.

Digital Content Directive

- Does not apply to the following:
  - Provision of services other than digital services;
  - Electronic communications services;
  - Healthcare;
  - Gambling services;
  - Financial services;
  - Open-source software where the consumer does not pay a price and the personal data provided by the consumer are exclusively processed by the trader for the purpose of improving the security, compatibility or interoperability of that specific software;
  - Supply of digital content where the digital content is made available to the general public other than by signal transmission as a part of a performance or event, such as digital cinematographic projections;

Digital Content Directive

- Includes provisions on:
  - The supply of digital content;
  - Subjective requirements;
  - Objective requirements;
  - Liability of the trader;
  - Burden of proof;
  - Remedies;
  - Personal Data;
  - Modification;
  - Redress

Digital Content Directive

- ‘digital content’ is defined as “data which is produced and supplied in digital form” – extremely broad description to cover various instances.

- ‘digital service’ means:
  - “a service that allows the consumer to create, process, store or access data in digital form” or
  - “a service that allows the sharing of or any other interaction with data in digital form uploaded or created by the consumer or other users of that service”.

Supply of Digital Content

- Art. 5 obliges the trader to supply the digital content or services without **undue delay** upon conclusion of the contract.

- The above is satisfied when the content or any means suitable for accessing or downloading the content is made available to the consumer.

- The digital content supplied must meet certain requirements within the Directive.

Subjective Requirements

- The digital content or service shall be:
  - of the description, quantity and quality, and possess the functionality, compatibility, interoperability and other features, as required by the contract;
  - be fit for any particular purpose for which the consumer requires it and which the consumer made known to the trader at the latest at the time of the conclusion of the contract, and in respect of which the trader has given his acceptance;
  - be supplied with all accessories, instructions, including on installation, and customer assistance as required by the contract; and
  - be updated as stipulated in the contract.

Objective Requirements

- Fit for the purposes for which the content or service would normally be used
- Be of the quantity and possess the qualities and performance features which the consumer may reasonably expect given the nature of the content or service.
- Supplies along with any accessories and instructions which the consumer may expect to receive.
- Comply with any trial version or preview of such content or service which is made available by the trader before the conclusion of the contract.

Objective Requirements

- The trader shall ensure that the consumer is informed of and supplied with updates, including security updates, that are necessary to keep the digital content or digital service in conformity.
- Where the consumer fails to install, within a reasonable time, updates supplied by the trader, the trader shall not be liable for any lack of conformity resulting solely from the lack of the relevant update, provided that:
  - the trader informed the consumer about the availability of the update and the consequences of the failure of the consumer to install it; and
  - the failure of the consumer to install or the incorrect installation by the consumer of the update was not due to shortcomings in the installation instructions provided by the trader.

Right of Termination

- Consumer to exercise right to terminate the contract by means of a statement to the trader expressing their decision.

- Trader shall reimburse the consumer for all sums paid in terms of the contract.

- Where the contract supplies contact or services in exchange for payment over a period of time, the trader shall reimburse the consumer only for the proportionate part of the price paid.

Questions

- What does the Digital Content Directive seek to regulate?
- Mention some of the subjective and objective requirements?
- What rights do consumers have vis-à-vis digital content or services?

Digital Services Act

- Confirmed on 23rd April 2022, the European Commission stated "The DSA sets out an unprecedented new standard for the **accountability** of online platforms regarding illegal and harmful content".

- Provide better protection for internet users and their fundamental rights, as well as define a single set of rules in the internal market, helping smaller platforms to scale up.

- The DSA applies to:
  - online intermediary services such as internet providers;
  - hosted service providers; and
  - online platform providers such as online marketplaces, app stores, and social media platforms.

Digital Services Act

- The obligations of the DSA increase depending on the size of the organization, but the fundamental principles of transparency and accountability apply to all organizations under the scope of the DSA.

- The European Union has adopted this approach to ensure that small to medium-size businesses are not adversely affected by costs of compliance.

- Hosting services, such as cloud services, have to be provided in accordance with a greater number of obligations than the services provided by simple intermediaries, such as domain name registrars.

- Online platforms, such as online marketplaces or social media platforms, have to go further still and finally the most onerous set of obligations are reserved for very large online platforms and search engines.

Digital Services Act

- **Targeted advertising:**
- More obligations aimed at ensuring a transparent and informed choice for recipients of digital services, including information on how their data will be monetised.
- Refusing consent to be tracked should be no more difficult for the users than giving consent. Users should also be given options to access the online platform based on tracking-free advertising.

- **Minors and vulnerable groups**:
- The DSA provides for a ban on the use of targeting or amplification techniques involving the data of minors for the purpose of displaying ads.
- It is also prohibited to target individuals based on special categories of data that allow for the targeting of vulnerable groups.

Digital Services Act

- **Recommender systems**:
- users should have more choice regarding recommender systems based on algorithms and used to promote or rank certain content or products.

- **Anonymity**:
- a new provision was introduced on the right to use and pay for digital services anonymously, in accordance with the principle of data minimisation and to prevent unauthorised disclosure, identity threat and other forms of abuse of personal data.

Digital Services Act

- **Compensation**:
- recipients of digital services and organisations representing them must be able to seek redress for any damages resulting from platforms not respecting their due diligence obligations.

- **Dark patterns**:
- online platforms are prohibited from using deceptive or nudging techniques to influence users' behaviour.

- **Waiver for SMEs**:
- the DSA also includes an exemption for micro, small and medium-sized enterprises (SMEs) from certain DSA obligations. SMEs are deemed to be enterprises that employ fewer than 250 persons with an annual turnover not exceeding €50 million and/or an annual balance sheet total not exceeding €43 million.

Digital Markets Act - Gatekeepers

- The DMA includes prohibitions on discriminating against other businesses in favour of the gatekeeper’s services, obligations to ensure interoperability with the gatekeeper’s platform, and obligations to share, in compliance with privacy rules, data that is provided or generated through business users' and their customers' interactions on the gatekeeper’s platform.

- A platform may be deemed to be a gatekeeper if it:
  - has a strong economic position and a significant impact on the internal market, and is active in multiple EU countries;
  - has a strong intermediation position, meaning that it links a large user base to a large number of businesses; and
  - has (or is about to have) an entrenched and durable position in the market, meaning that it is stable over time if the company met the two above criteria in each of the last three financial years.

Digital Markets Act

- Came into force in May 2023
- Aims to ensure that gatekeepers behave in a fair way online, thereby allowing innovators and technology startups to compete and innovate in the online platform environment
- Consumers will have more and better services to choose from, direct access to services, and fairer prices.
- Gatekeepers will still retain all opportunities to innovate and offer new services, without, however, using unfair practices against business users and customers that are dependent on them to gain undue advantage.

Gatekeeper Obligations

- Gatekeepers will have to:

(a) Allow third parties to inter-operate with the gatekeeper's own services in certain specific situations;

(b) Allow their business users to access the data they generate in their use of the gatekeepers' platform;

(c) Provide companies advertising on their platform with the tools and information necessary for advertisers and publishers to carry out their own independent verification of their advertisements hosted by the gatekeeper; and

(d) Allow their business users to promote their offer and conclude contracts with their customers outside the gatekeeper's platform.

Gatekeeper Obligations

- Gatekeepers will not be able to:

(a) Treat services/products offered by the gatekeeper more favourably in ranking than similar services/products offered by third parties on the gatekeeper's platform;

(b) Prevent consumers from linking up to businesses outside their platforms;

(c) Prevent users from uninstalling any preinstalled software or app if they wish; or

(d) Track end-users outside of the gatekeepers' core platform service for the purpose of targeted advertising, without effective consent having been granted.

Questions

- What is the scope of the Digital Services Act?
- Briefly explain some enhanced regulations found within the Act.
- Are there any exceptions or waivers to the above?
- What are ‘Gatekeepers’ and how are they regulated?

21 ACADEMY

Diploma in Law (Malta)

21 LAW

CAMILLERI PREZIOSI