MM ENG

A.Y. 2024/2025

BLAB

HANDOUTS

LEGAL ISSUES IN MARKETING

WRITTEN BY

CAMILLA BASTIA

TEACHING DIVISION

This handout is written by students with no intention of replacing university materials.

It is a useful tool for studying the subject, but does not guarantee preparation as exhaustive and complete as the material recommended by the University.

LEGAL ISSUES IN MARKETING

Introduction

We'll focus on different topics:

- *Data protection*
- *Trademarks offline and online*
- *Licensing*
- *Merchandising*
- *Unfair Commercial Practices*
- *Advertising*
- *Sponsorship /Ambush marketing*
- *Distribution via platforms*
- *Distribution contracts*

All those topics are linked since marketing is a set of activities (marketing mix) divided into four stages: product, placement, price and promotion. This course considers the legal aspects of 3 of those 4 phases (no price). When considering the product, we focus on data protection, trademarks offline and online, licensing and merchandising. Then, focusing on the promotion, we'll deal with unfair commercial practices, advertising and sponsorship/ambush marketing. In the end, talking about placement, we'll focus on distribution via platforms and distribution contracts.

In addition, this course aims at:

- Showing that marketing may have several painful legal implications -> we must recognise them and know how to manage them by using internal and external skills
- Showing how legal systems supply several business opportunities to marketing managers -> we must recognise them, and understand how to exploit them in the best way possible.

Jump on the moon - CASE STUDY

The case examines the phenomenon of user-generated content (UGC) in the food and tourism sectors. RouteAdvisor and Moonbucks Coffee Company launch "Jump on the Moon", an online campaign inviting RouteAdvisor users to submit photos of themselves jumping on a hotel bed with a Moonbucks drink in hand.

RouteAdvisor (RA) -> An online platform where users share reviews.

Moonbucks -> A U.S.-based coffee chain.

"Jump on the Moon" Campaign -> A promotional campaign where participants: visit a hotel, take a photo (or have someone take one) of themselves jumping on the bed while holding a Moonbucks drink and post the photo on RouteAdvisor.

1. Some of the images featured in the Jump on the Moon campaign display the Fritz Hotel logo. Fritz Hotel is a luxury 5-star hotel, based in London.

   - *The hotel might don't want to be connected to the campaign or the brand since it might have a different reputation -> there is a issue if something proper and specific of the hotel is recognisable via the picture -> the hotel should not be recognisable -> not showing logo, property of the hotels, distinction furniture's or something else -> trademark owners can only argue if the trademark appears in a promotional adv (commercial use) and not in a descriptive way (if you take a picture and there is the logo of a brand for accident, they can't say anything) -> the problem appears when there is the intention and it's not an accident. The hotel might sue the users because those are the people that actively damaged the image of the hotel, because they are those who materially infringe the trademark. On the other hand, the company could also sue the platform where the users post their pictures in order to get compensation.*

2. Lady Dada, a famous singer and songwriter, thinks Jump on the Moon is a really fun initiative and posts a photo of herself on AR jumping while holding her favourite Moonbucks drink. Moonbucks seizes the opportunity and uses Lady Dada's photo, published as part of Jump on the Moon, to personalise porcelain coffee mugs and launch a new health drink called 'Lady Dadaish'.

   - *They are not using the data collected just for the purpose of the campaign but they are also using the popularity (personality right -> right to exploit her image and name for promotional purpose) for their brand. They should ask her consent both for privacy reasons and commercials reasons.*

3. Moonbucks is using the 10 most popular Jump on the Moon photos to launch a new tasty and calorific drink: caramel white hot chocolate with whole milk and chopped cream.. The slogan for the new drink, along with the 10 photos of people jumping on the bed, is 'great for jumping higher'.

   - *The company can do this campaign only if it gets the consent to upload the picture on the website and the consent to choose the best ten pictures and use them for another campaign -> the consent must be specific (the consent for the first campaign might not be right for the second one). Moreover, this kind of adv might be misleading since the chocolate drink might give you more energy but it doesn't exactly make you jump higher, everything depends on the average consumer you take as a benchmark -> If you take a very naive consumer or if you take a consumer which is somehow skeptical and familiar with advertising, so that drink or jumping higher is not misleading for him or her. Also because there is a quantity of truth behind that*

4. In general, the RouteAdvisor platform collects and publishes user reviews. Many of these also relate to the photos from the *Jump on the Moon* campaign. Some of these comments are offensive, racist, or contain explicit sexual content.

   - *In this case we need to consider content moderation, that involves managing online interactions by regulating or removing comments. In Europe, the Digital Services Act (DSA) establishes legal frameworks for content moderation, providing publicly legislated rules enforced by the EU Parliament. However, in countries without such regulations, businesses seeking to prevent undesirable content can negotiate content moderation agreements with platforms. For instance, if a company like Walt Disney wishes to avoid explicit sexual content, references to weapons, drugs, or alcohol in connection with its characters, it can request the platform to enforce moderation policies aligned with its business interests. However, platforms may refuse such requests by citing principles of free speech. This highlights the ongoing debate surrounding the balance between content moderation and freedom of expression.*

Data protection -> protect personal data of the people. A company, in order to get personal data need authorisations -> the company needs to *get the consent* of the users in order to get them involve and engaged with the campaigns. The company must ask the consent and process the data in a specific way.

GDPR - General Data Protection Regulation

In out life as marketing managers, we'll have to collect data, to analyse data and make several other activities based on data. Now, as a consequence, we must be aware of the rules governing the processing of data, and in particular, the processing of personal data. In the digital age data are fundamental, we use data to make social networks work, to make e-commerce work, and many other activities, even IoT activities work. Data are the new oil, the currency in the digital age. And the point is that this data are collected and analysed and processed in the same way every day in order to realise many goals. Data are a valuable asset in the digital age. It is collected and processed daily, allowing business to:

- Personalise services and marketing campaigns
- Improve efficiency
- Improve products and services
- Gain a competitive edge

Once we have data, we can infer information from data and we can better understand how the world works, what people want, what your rivals are doing, how innovation will develop, and so

how the market will change. And so you work on data in order to acquire information, to acquire knowledge, and improve your businesses (both in the internal and external relationships). However, when it comes to data collection we need to take into consideration the distinction between general/ non-personal data and personal data (data connected to individuals, the data that are capable of identifying people) -> the second one might create some issues: we may have problems in relation to the identity of those individuals because the use we do of data can change and twist their identity, can reproduce a digital image of those individuals which is not true, which is not rooted in reality -> *identity theft* (pretending to be somebody else)*, discrimination and manipulative advertising* (sending an adv specific using data that might be sensitive -> selling specific products to people that might be more sensitive to them in a specific period just because we know that they are in a particular situation thanks to the data). The EU citizens were very worried about this use of data since many years ago and for that reason it was created a regulation called General Data Protection Regulation -> GDPR addresses these risks by establishing rules and safeguards to ensure *transparency, security, and fairness* -> the main idea behind it is we believe that human beings have the right to control their personal data. Has the right to be in control because otherwise their identity could be twisted and their will could be manipulated. The processing of personal data *can never be hidden*, can never be misguided. It has been created to guarantee that data breach are unlikely and if they happen, we immediately sort them. And it has been created to guarantee that the use of data is not meant to discriminate or to put somebody at a disadvantage.

The **General Data Protection Regulation (GDPR)** is a landmark law that came into force in May 2018, replacing the 1995 *Data Protection Directive* (A directive is a piece of EU law that gives member states leeway to adopt parts of it or not -> general piece of law from which member states can take distance, at least in some parts of it, in relation to some parts of it). GDPR establishes a comprehensive legal framework to protect personal data in the EU. It is directly applicable in all EU Member States without requiring national legislation -> is a *regulation*, meaning that the judges can immediately apply it without waiting for the national governments to adopt other rules and to better specify the general principles of a directive. GDPR applies to organisations processing EU citizens' personal data both inside and outside the EU.
It aims to:

- *Protect individuals' privacy*
- *Strengthen individual's control over their personal data*
- *Ensure responsible, lawful and transparent data use.*
- *Harmonise data protection laws across EU Member States.*

Material Scope Art.2(1) GDPR

- Automated processing of personal data
- Non-automated processing of personal data as part of a filing structured system

Personal data Art. 4(1) GDPR

Any information relating to an identified or identifiable natural person, i.e. any information that can be used to directly or indirectly identify an individual. It includes names, email addresses, IP addresses, and more. Users' names, birthdates, location data, photos, posts, online interactions.

GDPR applies *only to personal data*, which refers to any information that can directly or indirectly identify a natural person (e.g., names, emails, IP addresses, location data). Non-personal data, such as corporate financial records or stock prices, falls outside its scope. However, data related to company operations may still be classified as personal if they involve tracking individuals (e.g., monitoring office entries and exits).

Territorial Scope Art. 2(1) GDPR

GDPR applies to organisations inside and outside the EU if they:

- Are located within the EU
- Offer goods or services to individuals in the EU
- Monitor behaviour of individuals in the EU

This ensures data protection even for international businesses. It is a standard legal principle that laws apply within the jurisdiction of the legislating authority. Therefore, if a company operates within the EU, it must comply with EU regulations. This is a common practice worldwide -> businesses must adhere to local laws when operating in a specific territory. Furthermore, the GDPR extends its reach beyond EU borders. Companies outside the EU that offer goods or services to individuals in the EU or track their behaviour are also subject to GDPR compliance. This ensures that personal data protection remains robust, regardless of where a company is headquartered. The GDPR's extraterritorial scope is a groundbreaking legal principle, as it applies to organisations regardless of their geographic location, as long as they process data related to EU citizens. Whether a company offers products or services to individuals in the EU or monitors their behaviour, it must comply with GDPR regulations. This approach aligns with the idea that personal data protection is a fundamental right, which justifies the EU's decision to impose its rules globally. This phenomenon, also called "*Brussel effect*", extends EU data protection laws beyond traditional jurisdictional boundaries, ensuring that companies worldwide must adhere to GDPR when dealing with EU citizens' data. While this model strengthens privacy rights, it also raises concerns about *overregulation and its impact on innovation and competition*. Compliance with GDPR can be costly, potentially placing businesses, especially smaller firms, at a disadvantage compared to those in less regulated regions. The debate, therefore, lies in balancing *strong data protection with the need to foster innovation and economic competitiveness*.
The EU's approach to data protection prioritises fundamental rights over business concerns. When the GDPR was introduced, its primary goal was to safeguard individuals' personal data, even at the expense of profitability, innovation, or market competition. The EU's stance has been criticised, particularly by US companies, which argue that while they focus on innovation and technological advancements, the EU primarily produces regulations. In response, the EU

maintains that its rules are designed to protect individuals and apply equally to all companies, regardless of origin.
One issue of the GDPR is that many kinds of data are personal and for that reason there might be problems when talking about that and assuming that those are not personal while they actually are personal. Personal data includes any information capable of identifying an individual, such as internet behaviour, sensor-tracked movements, or IoT data from personal vehicles. While anonymisation can remove personal identifiers, data is initially considered personal if it can be linked to an individual. This broad definition means organisations must carefully evaluate whether data falls under GDPR rules. GDPR applies to both automated and non-automated personal data processing if it is part of a structured filing system.

Personal data -> any information relating to an identified or identifiable natural person

There are several key actors in data processing:
Data subject -> the individual whose data is being processed
Data controller -> the entity that determines the purposes and means of processing personal data
Data processor -> the entity that processes personal data on behalf of the data controller

Sometimes data controllers and data processors are the same just because one big company may have those capabilities, those skills within itself.
For a social media company collecting user data:

- *Personal data*: users' names, birthdates, location data, photos, posts, online interactions.
- *Data subjects*: the individual users of the platform.
- *Data controller*: the social media company
- *Data processor*: the third-party analytics provider that analyses data and provides insights for targeted advertising.

The GDPR is founded on **seven key principles** that guide data processing activities and are fundamental for ensuring that personal data is managed responsibly, ethically, and in compliance with legal standards. Those principles were formulated for the first time by the United States for managing how public administration works with the personal data of U.S. citizens. In the seventies the U.S. government decided that in order to guarantee its citizens and the fairness of the relationship between U.S. citizens and U.S. public administration, the public administration entities should be subject to those principles. Those principles were very popular and were even embraced by some international organisations.
The *GDPR expands data protection beyond government oversight* to regulate the relationship between individuals and private organisations. While the U.S. initially developed privacy principles to limit government power over citizens, the EU applies similar principles to private companies, recognising their growing influence over individuals' lives.

We'll analyse the seven principles:

- **Lawfulness, Fairness, and Transparency** -> Personal data must be processed lawfully, fairly and transparently -> you have to explicitly state the purpose of the data collection -> Data processing must comply with laws, be fair, and clearly communicated.
- **Purpose Limitation** -> Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes -> you can't use the data collected for one reason for other purposes
- **Data Minimisation** -> Only personal data that is adequate, relevant, and limited to what is necessary for the intended purposes should be collected -> you need to collect the data that are strictly necessary and no more than that.
- **Accuracy** -> Personal data must be accurate and kept up to date, with reasonable steps taken to rectify or erase inaccurate information without delay -> you have to leave the possibility to the users to modify the data at any point (i.e. they must be able to change their marital status if they divorce)
- **Storage Limitation** -> Personal data should not be retained longer than necessary for the purposes for which it was collected and processed, ensuring appropriate time limits for storage and periodic review or deletion
- **Integrity and Confidentiality** -> Organisations must implement appropriate technical and organizational measures to ensure the security of personal data against unauthorised or unlawful access, processing, accidental loss, destruction, or damage.
- **Accountability** -> Data controllers (those that want to realise a purpose) are responsible for ensuring compliance with GDPR principles and must be able to demonstrate their adherence through appropriate policies, procedures, and documentation.

The Article 6, GDPR mandates that personal data processing must have a *valid legal basis*. Organisations must ensure compliance by relying on one of the **six lawful bases**:

- **Consent** -> The data subject must give freely given, specific, informed and unambiguous consent for the processing of their personal data for a specific purpose -> no coerced consent, the person must be free to say no. Moreover, unambiguous means that you must do something proactive to say yes (I.e. check a box)

- **Contract** -> Processing is necessary for the performance of a contract with the data subject or to take steps prior to entering into a contract at their request.
- **Legal Obligation** -> Processing is necessary for compliance with a legal obligation to which the controller is subject (i.e. a judge must publish the rulings since those are public acts and everybody must be able to read it -> only option for the children)
- **Vital Interests** -> Processing is necessary to protect the life or safety of the data subject or another natural person.
- **Public Task** -> Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.
- **Legitimate Interests** -> Processing is lawful if necessary for the legitimate interests of the controller or a third party, unless overridden by the fundamental rights and freedoms of the data subject.

Organisations must document and justify the chosen lawful basis before processing personal data.

Consent is crucial for marketing activities, enabling businesses to engage in activities like:
- Sending marketing emails
- Displaying personalised ads
- Conduct other direct marketing activities

GDPR sets requirements for valid consent. Consent must be:
- *Freely given* -> No coercion, pressure or preconditions.
- *Specific* -> Clearly linked to a well-defined purpose
- *Informed* -> Individuals must understand what they are consenting to, receiving clear, concise, and accessible information about the processing
- *Unambiguous* -> Requires an active opt-in (e.g., no pre-ticked boxes).
- **Right to Withdraw** -> Data subjects must be informed that they can withdraw consent at any time, and the process to do so must be *easy and accessible*.

The concept of a contract is straightforward. When a customer purchases a product or service, they enter into a contractual agreement with the company. As part of this transaction, the company must collect and process personal data, a necessity inherent to fulfilling the contract. Consequently, explicit consent for data collection is *not required* in such cases, as the processing is implicitly justified by the contractual obligation.

On the one hand, **Legitimate Interests** can be a lawful basis for processing personal data, including for marketing purposes (Art. 6(1)(f) GDPR). Organisations must carefully document and justify their actions to ensure compliance with data protection regulations, such as the General Data Protection Regulation (GDPR).

Examples could be:

- *Fraud prevention* –> Organisations may process data to detect and prevent fraudulent activity -> Businesses may analyse customer data to detect and prevent fraudulent activities, thereby safeguarding both the company and its customers from financial harm.
- *Direct marketing* –> Businesses may send marketing communications to existing customers about similar products or services -> Companies may use customer data to promote products similar to those previously purchased. For instance, a makeup retailer may send promotional emails about blushes to customers who have previously bought lipstick.

On the other hand, the organisation must ensure that its legitimate interest does not override the rights and freedoms of the data subject. A careful assessment is required before proceeding with data processing. Therefore, organisations must engage in the **Legitimate Interest Assessment (LIA).** The LIA is a structured and documented process that helps organisations determine whether their use of personal data under the legitimate interest base is *lawful* and *proportionate*. LIA is necessary since it ensures compliance with GDPR Article 6(1)(f), it demonstrates a responsible and ethical approach to data processing, it helps prevent legal, financial, and reputational risks and ensures transparency

Transparency Obligation -> Indeed, when using legitimate interest as a legal basis, organisations must inform individuals about the processing and provide them with the right to object (Articles 13(1)(d) & 14(1)(d) GDPR).

LIA involves conducting the Three-Part Test for Legitimate Interest:

- **Purpose Test** –> Is there a valid legitimate interest? -> Clearly define the reason for processing personal data. If the purpose is fraud detection, explicitly state the type of fraud being prevented. If the purpose is direct marketing, specify that the marketing will be related to similar products or services.
- **Necessity Test** –> Is processing essential for achieving that interest? -> Ensure that the data collected is essential for achieving the stated purpose. Organisations must follow the data minimisation principle, meaning they should use existing data before requesting additional information. If more data is required, they must justify why it is necessary.
- **Balancing Test** –> Do the rights of the individual override the business interest? -> Demonstrate that the data processing is proportionate and does not unduly infringe upon the rights of the data subject. This involves: assessing the sensitivity of the data being processed, ensuring that individuals do not suffer distress, discrimination, or a significant loss of privacy and implementing safeguards such as *opt-out mechanisms*, allowing users to withdraw from marketing communications.

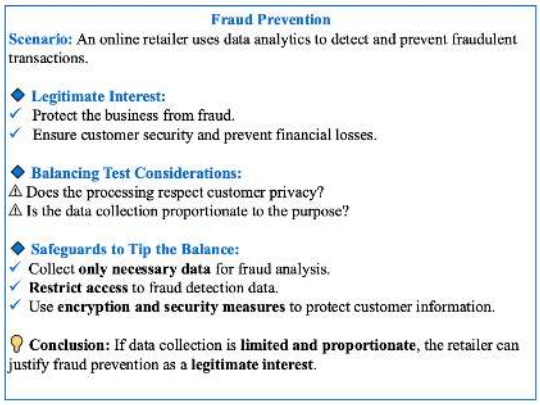
For example, a company sending promotional emails should ensure that messages are relevant and not excessive -> daily promotional emails may be considered intrusive. Providing a clear

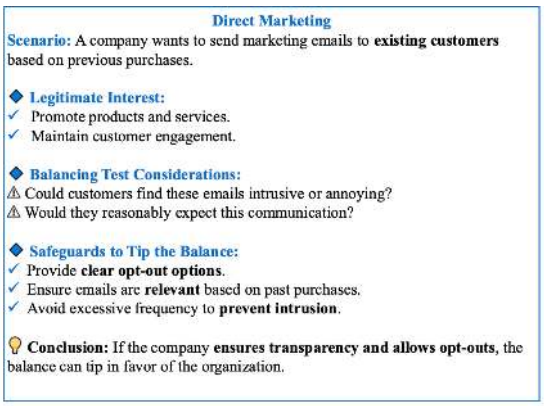
unsubscribe option helps demonstrate that the marketing activity is balanced and respects user rights.

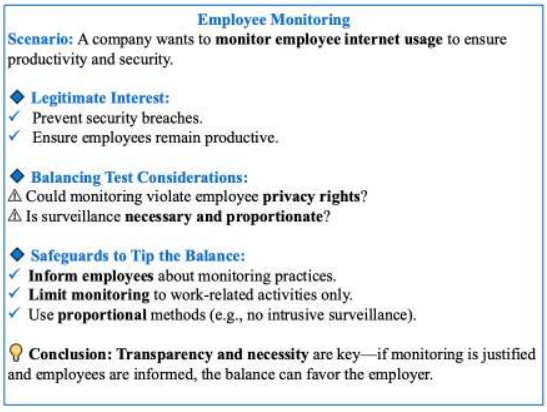
Three part test for legitimate interest:

- The nature of the data being processed (e.g., standard vs. sensitive data). If the data is sensitive (e.g., health, biometric, or financial data), stronger safeguards are required.
- The potential impact on the individual (e.g., distress, discrimination, or loss of privacy).
- Whether the data subject would reasonably expect their data to be used in this way. Consider prior interactions and user consent.
- The safeguards in place to mitigate risks (e.g., opt-out options, encryption, right to object).

If the interests of the individual outweigh the legitimate interest of the organisation, processing is not permitted under GDPR. The balancing test ensures that organisations act ethically and lawfully while protecting data subjects' rights. As a best practise, organisations must *document their assessment* and ensure that necessary safeguards are in place before proceeding with data processing under legitimate interest.







KEY CASES IN LEGITIMATE INTEREST ASSESSMENT (LIA)

Case 1: Royal Dutch Tennis Association (KNLTB)

Key Issue: Use of members' data for commercial purposes without consent.

CJEU Ruling:
- Promoting tennis is a **legitimate interest**, but using members' data for **unrelated commercial purposes** was not justified.
- The processing was **not directly necessary** or **proportionate** to the stated interest.
- Legitimate interest **cannot be used to bypass consent** for direct marketing activities.

Takeaway: There must be a **clear and proportional link** between the legitimate interest and data processing.

Case 2: Prosecution of AA Ireland Limited

Key Issue: Inadequate security measures leading to a **data breach**.

Findings:
- AA Ireland **failed to implement sufficient data security measures**.
- Demonstrated that **accountability and security** are critical parts of the balancing test.
- Legitimate interest cannot be justified if risks to individuals are not properly mitigated.

Takeaway: Data controllers must **not only identify legitimate interests** but also ensure appropriate **technical and organizational measures** to **protect personal data**.

These cases illustrate key aspects of applying the balancing test in practice.

Key Lessons from These Cases:
- ✓ Legitimate interest must be **directly necessary** and **proportionate** to the processing activity.
- ✓ Data controllers must ensure **transparency, accountability, and security** when conducting an LIA.
- ✓ Legitimate interest **cannot override the need for consent** in direct marketing.
- ✓ Implementing **strong security measures** is essential to meet GDPR compliance.

Conclusion: A well-documented **LIA is critical** to demonstrating compliance with GDPR and ensuring that data processing is justified and safe.

The GDPR grants data subjects key rights over their personal data, ensuring transparency and control. Data controllers must comply with these rights to maintain lawful processing.

Data Subject Rights (Articles 12-13 GDPR)

- *Right to access* -> right to get access to the datasets of the company and to get in touch with all the data that companies stored about us -> we can request a copy of our personal data and the clusters we the company has put our personal data (the company has one month to answer our question) -> The right to get access to the data sets of the company. And so to get in touch with all the data the company stored about us. In particular, we can request a copy of our personal data and also about the way in which the company has analysed them -> the company has a month to answer to our question
- *Right to rectification*
- *Right to erasure* (Right to be forgotten)
- *Right to restriction of processing*
- *Right to data portability*
- *Right to object*

Obligations of Data Controllers to uphold these rights

Right to access -> data subjects can request a copy of their personal data and information on processing purposes, categories of data, recipients and retention period. We want individuals to be in control of their personal data and to trust the company

- a customer request a retailer to provide all personal data held about them, including purchase history and marketing preferences
- A social media user requests a copy of all posts, messages, and interactions stored on the platform.
- A patient asks for access to their medical records, diagnoses, and test results.

- An employee requests their personnel file, performance reviews, and salary details.

Obligation of data controllers -> must respond within one month and provide requested information in a clear, structured format.
The right to access is fundamental for transparency, that is instrumental to exercise control -> We want individuals to be in control of their personal data, because their personal data identifies themself, and they don't want anybody to twist their identity.

Right to rectification -> Individuals can request correction of inaccurate or incomplete personal data. This ensures that data remains accurate and up to date. If the company is doing something wrong, we have the right to rectify what the company is doing.

- A customer notices their address is incorrect and asks a company to update it.
- A social media user requests correction of their birthdate on a platform.
- An individual requests a credit reporting agency to correct errors in their credit report.
- A customer updates their marketing preferences in a company's database.

Obligation of Data Controllers -> must promptly verify and correct inaccurate data upon request.

Right to Erasure (Right to be forgotten) -> individuals can request deletion of their personal data when data is no longer necessary for its original purpose, they withdraw consent for processing and when data has been unlawfully processed.

- A user deletes their social media account and requests removal of all stored data or asks for an uploaded photo to be removed.
- A former customer asks an online store to delete their purchase history and saved payment details.
- An individual withdraws consent for marketing emails and requests data removal.
- A job applicant requests deletion of their application data after losing interest in a position.

Obligation of Data Controllers -> must assess and, where applicable, delete the requested data unless there is a legal basis for retention (e.g., regulatory compliance).

In the past, legal systems in Spain, Italy, and other countries mandated *public disclosure of bankruptcies to prevent failed entrepreneurs from obtaining further credit.* When an individual declared bankruptcy, their name and company details were published in a publicly accessible register. One such entrepreneur experienced financial failure and was listed in the register. Fifteen years later, despite successfully rebuilding his business, he discovered that his bankruptcy record was still prominently displayed in Google search results. Arguing that this outdated information was damaging his reputation, he sought legal action -> not to erase the register itself, but to have Google remove the link associating his name with the record. The case escalated to the *Court of Justice of the European Union* (CJEU), which ultimately ruled in his favour. The court determined that the continued public visibility of his bankruptcy was *disproportionate to the original intent of*

protecting investors. This landmark decision established the "right to be forgotten," allowing individuals to *request the removal of personal data that no longer serves its original purpose*, has been unlawfully processed, or is no longer representative of their current status. However, enforcing this right remains complex, as data controllers must *evaluate requests while balancing privacy rights against the public's right to access information*. In some cases, courts must intervene to determine whether removal is justified.

Right of restriction of processing -> individuals can request that the processing of their data be limited in certain cases such as if they contest the accuracy of the data, if the processing is unlawful, but they prefer restriction over deletion and they need the data for legal claims -> you can ask that your data will be only stored on the server of the company, but they will not further process or analyse to provide you to find what your preferences are.

- A customer disputes the accuracy of their product preferences and requests restricted processing.
- An individual asks a company to limit data use while they challenge a legal issue.
- A user objects to profiling for marketing purposes.

Obligation of Data Controllers -> must limit processing to storage only until the issue is resolved

Right of data portability -> individuals have the right to receive their personal data in a structured, commonly used, and machine-readable format and transmit that data to another controller without hindrance. There are some key considerations to make: this right applies only to automated data processing based on consent or contract and does not apply to data processed for legal obligations or public interests -> the idea is if you individuals are interested in transferring their data, personal data, to another company different from the controller, they have the right to do that. And the controller must accomplish this request.

- A customer requests their purchase history to transfer it to a competing service.
- A social media user downloads all their posts and photos to migrate to another platform.
- A banking customer exports their transaction history for financial planning software or switches banking providers with transaction history.
- A patient shares health records with a new healthcare provider.

Obligation of Data Controllers -> provide data in a portable format and facilitate transfer where technically feasible

Companies create data clusters and use them for analysis and decision-making. To safeguard individual rights, legislation allows individuals to request the portability of their raw data but not of inferred data. The economic rationale behind this distinction is that raw data consists of

unprocessed information that companies merely collect, without significant investment. In contrast, inferred data is derived through analysis by data scientists and engineers, requiring financial and intellectual investment. Allowing competitors to access such processed data would undermine the company's proprietary efforts. Therefore, while data controllers *must provide raw data in a portable format that can be accessed by individuals and competitors, they are not obligated to transfer inferred or more sophisticated data resulting from their analytical processes*.

Right to object -> Individuals can objects to data processing if it is based on legitimate interest, it is used for direct marketing or if is for scientific or historical research (with exceptions). There are some key considerations to make: direct marketing objections must always be honoured and objections lo legitimate interests must be evaluated against the organisation's compelling reasons -> the right to object is crucial because there may be biases in automated processes and the only way to understand if these biases are going on is to have a human being with his own discretion to analyse those data.

- A customer objects to receiving marketing emails. The company must stop unless they can justify a compelling need

Obligations of Data Controllers -> evaluate objections and cease processing unless overriding legal grounds exist. Individuals must state specific reasons.

Direct marketing -> direct marketing includes emails, telemarketing and postal marketing. A key concept in GDPR for marketing is consent and how companies obtain and manage it. We need to focus on consent requirements for electronic marketing, on when legitimate interest can be used and on online advertising and cookie compliance.
GDPR requires individuals to **actively** agree to receive marketing messages. Users must take a clear and affirmative action, like checking a box or clicking a button. **Opt-out mechanisms** (where users must uncheck a box) are **not permitted**. The only valid opt-in methods are:

- **Unchecked checkboxes** -> Users must actively select them.
- **Clear subscription forms** -> Explain what data is collected and how it's used
- **Double opt-in systems** -> Send a confirmation email to verify interest.

Individuals have the right to object to direct marketing activities, such as receiving unsolicited emails. When this right is exercised, the company *must cease communication unless it can demonstrate a legitimate interest in processing the individual's data*. To justify its actions, the company must provide evidence of a *balancing test*, which assesses whether its legitimate interest outweighs the individual's right to privacy. This assessment involves three key tests: the *purpose test* (determining the objective of the data processing), the *necessity test* (ensuring the processing is essential for that objective), and the *balancing test* (weighing the company's interests against the individual's rights).

A legitimate justification for data processing might include automated verification of a user's identity to prevent fraud, such as confirming the connection between a bank account and a PayPal account. However, if the processing extends beyond fraud prevention, such as assessing an individual's creditworthiness, the *justification becomes more complex*, as it shifts from identity verification to evaluating financial reliability. In such cases, the right to object may be more strongly enforced but in general, the right to object is not the right to get the result.

If you want to process data in an accountable, lawful way, you must have consent from your data subjects, or you may have a legitimate interest. The consent must be freely given, and the consent must be explicit -> you must always need your data subjects to do something practically in order to express your concerns. It means that when you create a page online, or when you create also a form, a written form, opt-out mechanisms are never permitted. Pre-ticked boxes, silence or inactivity and implied consent are invalid methods.
In some cases, companies can rely on legitimate interest as a lawful basis for direct marketing. This applies when businesses communicate with existing customers to provide relevant updates or promote similar products or services they have previously purchased. Companies must ensure:

- **Proportionality and privacy** -> the marketing activity must be reasonable, ensuring that it does not excessively impact customer privacy.
- **Reasonable expectations** -> Customers should reasonably expect to receive such communications based on their prior relationship with the company.
- **Transparency & Rights** -> Businesses must clearly inform individuals about their right to object to such communications.

The best practise is always to provide a simple and accessible opt-out option, allowing recipients to easily unsubscribe if they no longer wish to receive marketing messages. This helps maintain trust and ensures compliance with GDPR regulations.
The GDPR imposes strict regulations on the use of cookies and tracking technologies, especially for advertising and user behaviour analysis. Websites must obtain *clear and informed consent* before placing cookies that track user activity.
For consent to be valid under GDPR, users must:

- **Understand what cookies do** -> Websites must clearly explain if cookies are used for analytics, advertising, or functionality (websites use the option “give me more information” but not many people look at it because it creates fatigue)
- **Have control over their choices** -> Users must be able to accept, reject, or customise which cookies they allow
- **Be able to withdraw consent at any time** -> A simple and accessible option should be provided to change cookie preferences later.

The best practise in this case is to use *transparent cookie banners* (ensure that banners provide clear information without misleading language) and *implement Consent Management Platforms*

(CMPs): CMPs help automate consent collection, manage preferences, and ensure ongoing GDPR compliance.

Cookie banners are essential tools for ensuring legal compliance and protecting user privacy. A well-designed banner should be *transparent, user-friendly, and GDPR-compliant*, allowing users to manage their preferences effectively. There are some key principles for an effective cookie banner:

- **Clarity and Simplicity** -> a minimalist design with clear messaging reduces information overload and enhance user experience
- **Layered approach** -> provide essential information upfront, with an option to access detailed cookie settings
- **Well-defined choices** -> users should have easily accessile options such as “Accept All”, “Reject All” and “Manage Preferences”
- **No Pre-Selected cookies** -> GDPR requires freely given and active consent, meaning users must explicitly choose which cookies to accept.
- **Smooth and Engaging Experience** -> Light animations can guide users through the selection process without causing distractions or frustration.

In Marketing law designing effective and GDPR compliant cookie banners matter due to:

- **Legal compliance** -> A well-structured banner prevents GDPR violations and potential fines.
- **Trust and transparency** -> clear and honest communication enhances user trust and strengthens brand reputation
- **User Experience and Informed consent** -> An effective banner reduces consent fatigue and increases the likelihood of users making an informed choice

Designing an effective cookie banner is not just a legal requirement but it is also a strategic marketing tool that fosters trust, ensures compliance and enhance the overall user experience. Supporters of the General Data Protection Regulation (GDPR) acknowledge that, despite its intent to safeguard fundamental individual rights, its implementation has led to unintended consequences. One of the primary concerns is "*consent fatigue*," where individuals, overwhelmed by frequent consent requests and complex privacy notices, tend to grant permission without fully understanding the implications. Although consent under the GDPR is intended to be explicit, specific, and freely given, in practice, individuals often do not engage with privacy policies, mirroring behaviour seen in offline settings, such as signing forms in stores without reading them. This raises a fundamental critique of the GDPR -> not merely its cost or regulatory burden, which are debatable trade-offs between business interests and data protection, but its overall effectiveness. The regulation relies heavily on consent as a mechanism for data control, yet research suggests that individuals are *not always willing or capable of thoroughly evaluating their choices*. This dilemma presents a significant challenge: if consent is ineffective, what alternative mechanisms could ensure individuals retain control over their personal data? To date, no clear solution has been identified, leaving experts at an impasse.

In response to these challenges, businesses have had to adapt by integrating data protection measures into their operational processes. Over the past decade, companies have restructured their practices, ensuring that marketing departments work closely with data protection officers. Organisations now conduct *internal checks* before launching campaigns, implement consent management platforms, and engage external auditors to verify GDPR compliance. This approach reflects a broader transformation in corporate governance, where *privacy considerations are embedded into business strategies to uphold trust and regulatory adherence*.

Consent fatigue -> Consent fatigue occurs when users are bombarded with numerous consent requests, leading them to either mindlessly accept or ignore them entirely. This phenomenon reduces the effectiveness of consent mechanisms and can diminish user trust in data privacy practices. Common causes of consent fatigue are excessive exposure to pop-ups and cookie banners on multiple websites, overly complex and confusing legal language, intrusive or disruptive banners that interfere with the user experience and lack of control and transparency leading to a lack of engagement with consent requests. To reduce consent fatigue we can use clear, concise and user-friendly language in consent request to explain data usage, we can minimise unnecessary consent prompts and request consent only when required, provide granular control so users can easily choose their preferences and what they consent to or we can store and remember user preferences to prevent repeated consent requests on subsequent visits. Reducing consent fatigue ensures that users remain engaged, make informed choices, and trust how their data is handled, ultimately supporting GDPR compliance and ethical data practices.

A responsible marketing approach ensure GDPR compliance while maintaining user trust and engagement -> some strategies for companies comprehend:

- *Ensuring compliance and user trust*
- *Privacy by design* -> Integrate data protection from the start.
- *Use Consent Management Platforms (CMPs) for easy compliance.*
- *Regularly audit consent mechanisms and marketing strategies.*
- *Stay informed about GDPR updates and best practices.*

Marketing increasingly relies on profiling and automated decision-making to enhance customer experiences and optimise business strategies. There are different techniques:

- **Profiling** -> analysing personal data to evaluate characteristics like preferences, interests and behaviours
- **Automated Decision-making** -> using algorithms to make decisions without human intervention

This matters because it helps companies personalise marketing strategies and raises privacy concerns that require GDPR compliance. Some examples of profiling and automated decision-making comprehend:

- *Product recommendations* -> online retailers analyse the user's browsing history and past purchases to suggest relevant products. (Example: Amazon's "Recommended for You" section)
- *Targeted advertising* -> social media platforms use demographics, interests, and browsing activity to display personalised ads (Example: Facebook ads based on search history)
- *Credit scoring* -> Lenders use automated decision-making to assess loan applications based on financial data (Example: Credit rating agencies calculating creditworthiness)

While these techniques improve user experience and efficiency, they also raise privacy and fairness concerns. The GDPR rants specific rights to ensure transparency and fairness in profiling and automated decision-making. The key rights comprehend:

- *Right to Objects* -> data subjects can refuse profiling or automated decisions that significantly affect them (i.e. credit scoring, job applications)
- *Right to Human intervention* -> if an important decisions is made automatically, data subjects have the right to request human review and challenge the decision.

This prevents unfair or discriminatory outcomes and ensures individuals have control over their data. Those right are not absolute: there are **exceptions** where profiling and automated decision-making may still be allowed:

- *Contract Performance* -> Necessary to fulfil a contract (e.g., automatic approval for online loan applications)
- *Legal Authorisation* -> When required by law (e.g., fraud detection systems in banking).
- *Explicit Consent* -> When users provide informed, clear consent (e.g., opting into personalised ads).

In this case, the best practice for companies is to clearly inform data subjects about these exceptions and their rights.

To sum up, the best practises to ensure compliance and ethical use are:

- **Transparency and control** -> Clearly communicate how data is used and provide opt-out options.
- **Data minimisation** -> Only collect data necessary for the specific purpose, avoiding excessive data gathering.
- **Fairness and non-discrimination** -> Ensure profiling and automated decisions do not result in unfair treatment.
- **Human oversight** -> Maintain human intervention in high-impact decisions to prevent biases and errors.

By respecting GDPR rights, marketers can use profiling and automation responsibly, ensuring both compliance and customer trust. Responsible use of these technologies enhances making effectiveness without compromising individual rights.

Data security -> Under GDPR, organisations must implement technical and organizational measures to protect personal data from unauthorised access, loss, or damage (Article 32 GDPR). The key focus areas are:

- *Technical and organisational measures* to ensure data protection
- *Data protection impact assessment (DPIA)* as a risk management tool
- *Accountability and compliance* to uphold GDPR obligations

Data security is not just a legal requirement, it is fundamental to maintaining *trust and ethical business practices*. Security measurers should be tailored to the risks associated with data processing. Some common strategies are:

- **Technical measures**
  - *Encryption* -> Converts personal data into unreadable formats for unauthorised users. (i.e. Encrypting customer credit card data prevents unauthorised access in case of a breach)
  - *Access Controls* –> Limits who can access personal data based on roles and responsibilities.
  - *Regular Data Backups* –> Ensures data recovery in case of cyberattacks or system failures.
  - *Pseudonymisation & Anonymisation* –> Protects individual identities in datasets.

- **Organisational measurers**
  - *Employee training* -> educating staff of GDPR responsibilities and cybersecurity best practises
  - *Internal policies and audits* -> regular assessments to identify and mitigate security risks.

A **Data Protection Impact Assessment (DPIA)** is a proactive tool that helps organisations identify, assess, and mitigate privacy risks before processing personal data. Required under *Article 35 of the GDPR*, a DPIA ensures that data processing activities align with privacy regulations, minimising potential risks to individuals' rights and freedoms. A DPIA is mandatory when data processing is likely to pose a high risk to individuals. This includes:

- *New technologies* -> implementing AI, facial recognition or machine learning where privacy risks are uncertain
- *Sensitive data processing* -> handling health data, biometrics or genetic information, which requires strong safeguards
- *Large-Scale monitoring* -> using CCTV surveillance, location tracking, or behavioral monitoring.
- *Profiling and automated decisions* -> employing credit scoring, hiring algorithms, or targeted marketing that could significantly affect individuals.
- *Data matching and combining* -> merging data from multiple sources to build comprehensive individual profiles

Imagine an e-commerce company implementing an AI- driven targeted advertising system that personalises product recommendations based on user behaviour. Since this involves profiling and

behavioral tracking, the company must conduct a DPIA to evaluate potential risks, such as excessive surveillance, bias in recommendations, or unauthorised data sharing. By conducting a DPIA, businesses can ensure compliance, protect user privacy, and build trust with their customers.

A data protection impact assessment (DPIA) follows a structured approach to ensure that privacy risks are identified and addressed before processing personal data. The key steps in DPIA comprehend:

1. **Describe the processing** -> clearly outline the purpose, scope, and context of the data processing activity. Identify what data is being collected, why it is needed, and how it will be used.
2. **Assess necessity and proportionality** -> justify why the data processing is essential -> we need to ask “is this data collection truly necessary?” “Could the objective be achieved with less intrusive methods?”
3. **Identify potential risks** -> evaluate how processing could impact individuals’ rights and freedoms. We need to consider risks such as unauthorised access or misuse of data, unfair profiling or discrimination and loss of control over personal information
4. **Implement mitigation measurers** -> introduce safeguards to minimise risks and protect user privacy. This could include data minimisation (collecting only what is strictly necessary), anonymisation or pseudonymisation to reduce identifiability and enhanced security measurers, such as encryption and strict access controls

Some of the benefits of DPIA are:

- *Proactive risk management* -> identifies privacy risks before implementation
- *Improved compliance* -> ensurers GDPR adherence
- *Stakeholder engagement* -> encourages transparency and accountability

I.e. a mobile app collecting location data for personalised offers should conduct a DPIA to access privacy risks.

DPIA si important for different reasons:

- **Proactive Risk Management** -> Identifies and addresses privacy risks before they become a problem
- **Stronger GDPR Compliance** -> Helps organisations stay aligned with legal obligations and avoid penalties.
- **Increased Accountability** -> Demonstrates a commitment to data protection and accountability.
- **Stakeholder Engagement** -> Enhances transparency and accountability, ensuring data subjects and regulators trust the organization’s data practices.
- **Improved decision-making** -> Informs decisions about data processing activities and ensure they are lawful and ethical.

I.e. A mobile app that collects location data for personalised offers must conduct a DPIA to evaluate privacy risks. The company should assess: Whether users are aware their location is being tracked, if privacy-friendly alternatives (such as asking for consent only when needed) can be used and what security measures will protect the data from being misused or accessed unlawfully. By following these steps, businesses can integrate data protection into their processes, ensuring that they not only comply with GDPR but also build a privacy-first marketing approach.

In sum, the best practises for ensuring data security and accountability are:

- *transparency and control* -> Clearly communicate how data is collected and protected.
- *Data Minimisation* -> Limit collection to what is strictly necessary.
- *Regular Risk Assessments* -> Conduct DPIAs for new processing activities.
- *Employee Training* -> Ensure all staff understand GDPR compliance measures.
- *Maintain Accountability* -> Keep thorough documentation of security policies and DPIA results.

Data security is not just about regulatory compliance, it is a crucial element of ethical marketing and consumer trust. Organisations that implement strong security practises will not only avoid penalties but also build long-term customer loyalty. Accountability in the GDPR can be found under Article 5(2) of the GDPR, that says that organisations must do more than just follow data protection rules—they must also prove they are compliant. This principle of accountability requires businesses to take active steps to ensure data is handled lawfully, securely, and transparently. This means that data controllers are not only responsible for protecting personal data, but they must also be able to *demonstrate compliance through documentation, policies, and proactive measures*.

Accountability is important because of different factors:

- *Transparency and trust* -> when businesses can prove they are handling data responsibly, it builds trust with customers and stakeholders.
- *Legal protection* -> Demonstrating compliance helps prevent fines and legal consequences in case of audits or data breaches.
- *Stronger Data Governance* -> a structured approach to accountability ensures that data protection is embedded in daily business operations, reducing the risk of security incidents.

I.e. a company implementing data protection policies, employee training and breach notification protocols can quickly demonstrate GDPR compliance if audited by a regulatory authority.

Key Accountability measurers to demonstrate compliance include:

- *Documenting data processing activities* -> Maintaining detailed records of processing operations, including legal bases and data categories
- *Implementing data protection policies* -> develop and enforce internal policies for handling personal data securely
- *Training staff* -> conduct regular GDPR training sessions for employees

- *Data breach notification* -> ensure mechanisms are in place to promptly report data breaches to authorities and affected individuals (Articles 33 & 34 GDPR).

i.e. A company maintains a record of processing activities (ROPA) detailing how it collects and processes customer data

"The Provider undertakes to process the personal data provided by the Data Controller exclusively for the purposes specified in this contract and in compliance with the provisions of Regulation (EU) 2016/679 (GDPR). In particular, the Provider undertakes to:

- *Implement appropriate technical and organizational measures to ensure the security of personal data, confidentiality, and integrity, in accordance with Article 32 of the GDPR.*
- *Appoint a data protection officer (DPO) if required by Article 37 of the GDPR.*
- *Assist the Data Controller in fulfilling its obligations to respond to requests from data subjects pursuant to Chapter III of the GDPR.*
- *Inform the Data Controller without undue delay of any personal data breaches pursuant to Article 33 of the GDPR.*
- *Cooperate with the Data Controller and the supervisory authority in the event of inspections or investigations relating to the processing of personal data.*
- *Ensure that personnel authorized to process personal data are subject to a duty of confidentiality pursuant to Article 28(3)(b) of the GDPR.*
- *Not transfer personal data to a third country or to an international organization without the prior written authorization of the Data Controller and in compliance with Chapter V of the GDPR.*
- *Return or delete all personal data at the end of the provision of services, unless otherwise instructed by the Data Controller.*
- *Maintain complete records of all personal data processing activities carried out on behalf of the Data Controller.*

The Data Controller reserves the right to conduct audits and inspections at the Provider's premises to verify compliance with the provisions of the GDPR."

Contracts with data processors -> when a company outsources data processing to third-party providers, it must ensure they comply with GDPR. Essential elements in a data protection clause include:

- *purpose of processing* -> the processor may only process data for contractually defined purposes
- *Security measurers* -> the processor must implement technical and organisational safeguards
- *DPO appointment* -> the processor must appoint a data protection officer (DPO) if required
- *Data breach notification* -> any data breach must be reported without undue delay
- *Cooperation with authorities* -> the processor must assist in GDPR compliance audits and investigations
- *Confidentiality obligations* -> employees handling personal data must maintain strict confidentiality
- *International transfers* -> data cannot be transferred outside the EU without explicit authorisation
- *Data retention and deletion* -> the processor must return or delete personal data after service termination

I.e. a marketing firm outsourcing email campaigns must include GDPR clauses in its contracts with email service providers.

Data breach notification obligations -> a data breach occurs when personal data is lost, stolen, or accessed without authorisation, compromising confidentiality, integrity or availability.
Notification requirements (Article 33 GDPR):

- *Report to supervisory authority* within 72 hours of discovering the breach

- *Include details* such as nature of the breach (I.e. unauthorised access, accidental deletion), number of affected individuals and data records, potential consequences for individuals and mitigation measures taken to reduce harm

Looking at when to notify individuals (Article 34 GDPR), if the breach poses a high risk to individuals' rights and freedoms. It must include a clear explanation of the breach, contact details for further information and recommended protective actions for affected individuals.
I.e. A lost unencrypted laptop with customer data triggers mandatory notification, whereas an encrypted database breach may not.
Within the most common data breach scenarios we can find:

- *Lost or stolen devices* -> a marketing manager loses a company laptop containing customer data
- *Phishing attacks* -> a staff member falls for an email scam, compromising login credentials
- *Malware infections* -> a malware attack grants hackers access to customer databases
- *Accidental disclosure* -> an intern sends an email containing customer details to the wrong recipient
- *Hacking incidents* -> cybercriminals exploit website vulnerabilities to steal personal data

In order to prevent breaches, there are severals things that could be done:

- *Encrypt sensitive data* -> secure customer data on all devices
- *Train employees* -> regular cybersecurity awareness programs
- *Strong access controls* -> restrict access to sensitive information
- *Software updates* -> regular patches to fix security vulnerabilities
- *Use Anti-malware tools* -> protect company systems from cyber threats

There are several risks of failing to comply with GDPR:

- *financial penalties* (article 83 GDPR) -> fines up to €20 million or 4% of global turnover and compensation claims from affected individuals (article 82 GDPR)
- *Reputational damage* -> negative publicity and loss of customer trust and difficulty attracting investors or business partners
- *Legal and Operational risks* -> investigations and enforcement actions by data protection authorities, potential class action lawsuits from affected individuals, suspension of data processing activities, disrupting business operations and mandatory data audits and compliance checks

i.e. A company fined for failing to notify authorities about a data breach affecting thousands of customers

Some best practises for GDPR compliance and accountability include:

- *Embed data protection un business culture* -> train employees and foster GDPR awareness
- *Implement robust security measurers* -> use encryption, access controls and risk assessment

- *Maintain transparency* -> clearly communicate data processing practices to individuals
- *Regular compliance audits* -> monitor and review GDPR policies regularly
- *Consult legal and data protection experts* -> ensure up-to-date compliance with evolving regulations

Organisations that prioritise accountability and security don't just avoid fines, they build trust, protect their reputation and foster sustainable, ethical data-driven marketing.

International data transfers -> the GDPR (Chapter V) restricts the transfer of personal data outside the European Economic Area (EEA) unless adequate protection is ensured. Business operating globally myst navigate strict regulations to ensure data privacy and compliance. Companies can transfer data outside the EEA through *adequacy decisions* (Article 45 CGPR) -> the European Commission assess a country's data protection laws and grants an adequacy decision if they provide sufficient safeguards.

I.e. Switzerland, New Zealand have adequacy decisions, allowing seamless data transfers.

Moreover, we need to consider:

- *Standard contractual clauses* (SCCs) (Article 46(2)(c) GDPR) -> pre-approved legal contracts used when transferring data to countries without an adequacy decision. Ensures contractual safeguards between data exporters and importers
- *Binding corporate rules* (BCRs) (Article 47 GDPR) -> legally binding internal corporate policies for multinational companies transferring data within their corporate structure. Offer flexibility but requires approval by data protection authorities
- *Other mechanisms* (Article 49 GDPR) -> in specific cases, data transfers may be based on *explicit consent* from individuals and *necessity for contract performance* (i.e. airline booking systems sharing data internationally)

i.e. a global e-commerce company uses SCCs to transfer customer data to its US-based customer service provider.

Under the GDPR, the transfer of EU citizens' data to the United States is permitted only if the data is processed in compliance with GDPR standards. However, legal challenges have arisen regarding data privacy in international transfers. Following the September 11th attacks, U.S. companies were required to provide data to national security agencies for counterterrorism efforts. This led to a landmark case in which an Irish citizen, Mr. Schrems, contested the U.S. National Security Agency's (NSA) handling of his data, arguing that its surveillance practices violated the GDPR. The European Court of Justice ruled in his favour, concluding that U.S. data processing practices were incompatible with EU privacy laws.
This case highlighted the broader challenge of ensuring data protection when transferring information between jurisdictions that do not adhere to the GDPR.
The regulation establishes two primary mechanisms to enable lawful data transfers:

1. *Contractual Agreements* –> If an EU-based company shares data with a foreign entity, such as a Brazilian business partner, a contract must be in place requiring the recipient company to comply with GDPR standards.
2. *Internal Corporate Rules* –> If the foreign entity is a subsidiary of an EU-based company, internal ethical codes must be implemented to ensure GDPR compliance.

These mechanisms reflect the European Union's commitment to enforcing data protection beyond its borders, a phenomenon referred to as the "*Brussels Effect*." This principle underscores the EU's influence in extending its regulatory standards internationally, ensuring that the fundamental right to data protection is upheld even outside its jurisdiction.

The Schrems II case and its impact

The Schrems II ruling, issued by the *Court of Justice of the European Union* (CJEU) in 2020, has a a major impact on international data transfer. It significantly altered how companies handle transfers of personal data between the EU and non-EEA countries, particularly the United States. The Schrems II was a landmark ruling due to:

- *Privacy shield invalidation* -> the ruling struck down the EU-US privacy shield, a widely used mechanism that previously allowed data transfer between the EU and the US
- *US Surveillance concerns* -> the court found that US surveillance laws did not provide GDPR-equivalent protections, raising concerns about government access to EU personal data
- *Stronger Compliance Requirements* -> as a result, companies can no longer rely on the privacy shield and must ensure alternative safeguards when transferring data to non-EEA countries

After Schrems II, some things changed:

- *Stronger Assessment of SCCs* –> Companies using Standard Contractual Clauses (SCCs) must now assess the legal framework of the destination country to determine whether additional safeguards are needed.
- *Increased Responsibilities for Data Importers* –> Organisations receiving data from the EU must demonstrate that they can uphold GDPR-level protections.
- *Greater Scrutiny of International Transfers* –> Data protection authorities are more vigilant, especially regarding transfers to the US and other high-risk jurisdictions.
- *Negotiation of a New EU-US Data Transfer Framework* –> In response to Schrems II, efforts have been made to develop a new transatlantic data transfer agreement that aligns with GDPR.

i.e. A European software company using a US-based cloud provider can no longer assume that data transfers are automatically compliant. Instead, they must conduct a data transfer impact assessment (DTIA), evaluate the legal risks of US surveillance, implement supplementary security measures, such as encryption or data localisation strategies.
By adapting to these changes, companies can continue transferring data globally while maintaining GDPR compliance.

Marketers should handle international data transfer:

- *Assess data transfers* -> identify when personal data is transferred outside the EEA
- *Choose the right mechanism* -> use adequacy decisions, SCCs or BCRs based on the destination country
- *Implement additional safeguards* -> encrypt data and assess the destination country's surveillance laws
- *Monitor legal developments* -> stay informed on changes to adequacy decisions and emerging regulations

Marketers handling international customer data must ensure GDPR compliance while enabling seamless business operations. Proper data transfer mechanisms protect both business and consumers, ensuring trust, security, and regulatory compliance.

Trademarks

A trademark is: A *property right upon a mark* (that is to say, a sign) that is gained via either registration or use, and that is traditionally employed in order to identify and distinguish the goods of one manufacturer, or seller, from the goods manufactured, or sold, by other producers: and that, more recently, is also employed because of its selling power. A property right/intellectual right means that the object of the right belongs to a particular person/company and, in the case of trademarks, it means that nobody can use it without your consent. Trademarks nowadays are important because they can increase the value of a product/service -> sign of power and increase price.

If you are the owner of a sign, i.e. if you are a trademark holder, you are the only one to:

1. **Positive meaning** -> decide who will use the trademark, how she will use it, how much she will pay for using it -> *brand licensing* -> we can give for a certain period of time the authorisation to a third party to use the trademark in exchange for money (monetise the trademark)
2. **Negative meaning** -> bring a legal action against who uses your trademark without your consent and, thus, get remedies against who infringes your trademark right -> *Infringement*

Having a legal protection means that right holders can obtain these remedies against infringers:

- *Cease and desist orders*
- *The order to collect goods from trade*
- *The order to destroy counterfeited products*
- *The order to destroy machineries*
- *Compensation for damages*
- *Publication of the judgement*
- *Penalty payments*

Mark / sign -> anything that can be put on a product (good or service does not matter) and be separated from it without changing the characteristics of the product -> Any word, name, logo, symbol, tagline, design, letter, shape, color, sound, movement, smell … or any combination thereof. So the decision not to get a trademark, not to register a sign as a trademark, is a quite silly decision. Every time we are creating a company or a product, the best thing we can do is to register the sign for that company, for that product, as a trademark, to make money out of it, and to protect our sole use of that sign.

The law forbids the registration as a trademark of:

- A shape which results from the nature of the goods themselves -> *functional shape*
- A shape of goods which is necessary to obtain a technical result -> *functional shape*
- A shape which gives a substantial value to goods, I.e. when consumers buy the product because of its shape -> *ornamental shape*

In legal terms, the head of a Philips razor cannot be registered as a trademark because it serves a *functional* purpose rather than acting as a *distinctive sign*. Trademarks are meant to identify the origin of a product and can be renewed indefinitely, while **patents**, which protect inventions, have a limited duration of 20 years to ensure innovation benefits society. A fundamental reason why functional shapes cannot be trademarked is that they are *inseparable from the product's function.* Unlike a logo (such as the Apple symbol on a computer, which can be removed without affecting functionality), the shape of a razor head is essential to its use. If removed, the razor would no longer perform its function. The same logic applies to other functional product shapes, such as nutcrackers or crackers, where the form is directly tied to their intended purpose. Thus, granting trademark protection to such shapes would create an *unfair monopoly, restricting competition indefinitely*.

You can get a trademark via either *registration or use* -> this is the case of common law trademarks or unregistered trademarks. A trademark can be acquired either through registration or through use. The key distinction lies in the legal presumption of ownership.

1. *Registered Trademark* (Case A):
   - The registrant is presumed to be the trademark owner.
   - In case of infringement, the burden of proof falls on the alleged infringer (C) to demonstrate that no violation occurred.
   - Registration grants protection even if the trademark owner has not yet commenced business operations.

2. *Trademark Acquired Through Use* (Case B):
   - Ownership is established through continuous use within a specific region.
   - In case of infringement, the burden of proof lies with the trademark user (B) to show that their rights have been violated.

- Protection is limited to the geographical area where the trademark has gained recognition through use.

This distinction explains why legal advisors recommend registering trademarks, as registration provides broader and more immediate protection. In an infringement case, the burden of proof differs depending on how the trademark was acquired.

1. Registered Trademark Holder (A): Ownership is legally presumed, meaning A does not need to prove they are the rightful owner. A must present facts demonstrating C's infringement, while C bears the burden of disproving those claims.
2. Trademark Acquired Through Use (B): B must first establish ownership by proving continuous and recognised use of the trademark and B must also demonstrate that an infringement occurred.

A registered trademark serves as *formal proof of ownership*, similar to an identification document, whereas an unregistered trademark requires the owner to *substantiate their claim in court*.

We need to take into consideration the *territorial scope* of registration:

- *National registration* -> one application -> one national trademark
- *EU wide registration* -> one application -> one EU wide trademark
- Broader territorial registration
  - *Paris convention* -> multiple applications -> multiple national trademarks to be filed by 6 months
  - *Madrid convention* -> one application -> multiple national trademarks

So, at the initial stage, every trademark is national. Registration typically begins in a single country, but international protection can be expanded through several mechanisms:

1. **Paris Convention** -> After registering a trademark in one country, the owner has six months to extend protection to other countries that are signatories to the Paris Convention. This allows for international expansion while maintaining the original filing date.
2. **European Union Trademark (EUTM)** -> A single application to the EU Intellectual Property Office grants protection across all 27 EU member states. This simplifies the process for businesses operating within the EU.
3. **WIPO (Madrid System)** -> A single application through the World Intellectual Property Organisation (WIPO) enables protection in multiple countries at once. Applicants can select specific countries where they seek trademark protection.

The choice of method depends on the desired *coverage and administrative complexity*. The Paris Convention remains in use as a flexible option for expanding trademark protection after an initial filing.

Thanks to registration you can get:

- *Nationwide protection instead of local protection* -> Indeed, the geographical scope of both common law trademarks and unregistered EU trademarks is limited to those places where these trademarks have been used.
- *Evidentiary presumption* -> registration in prima facie evidence of: (a) the validity of the trademark, (b) the registrants' ownership, and (c) the exclusive right. To be sure, the trademark's validity can be questioned in courts arguing for the absence, at the moment of the registration, of the requirements for it.
- *Warning function* -> ®

The registration of a sign as a trade mark *must always be applied for in relation to certain goods or services*: the goods and services for which the protection of the trade mark is sought to be identified by the applicant with *sufficient clarity and precision* to enable the competent authorities and economic operators, on that basis alone, to determine the extent of the protection conferred by the trade mark. Goods and services in respect of which trade mark registration is applied for shall be classified in conformity with the system of *classification established by the Nice Agreement, which is an international treaty*. The use of general terms shall be interpreted as including all the goods or services clearly covered by the literal meaning of the indication or term. If the application concerns only some of those goods or services, the applicant is required to specify which of the goods or services in that class are intended to be covered.

A trademark can be acquired through *registration*, which is the most effective method, or through *use*, which is common in countries like the United States and, in specific cases, Italy. Unregistered trademarks typically belong to small businesses with **local** recognition rather than nationwide protection. To secure broader protection, trademarks can be registered at a *national, EU-wide, or international level* under agreements such as the Paris Convention or the Madrid Convention, which operate under the *World Intellectual Property Organisation (WIPO)*. Registration is preferable to use-based acquisition, as it grants nationwide protection and a legal presumption of ownership, whereas use-based trademarks are limited to the regions where they are actively used. Additionally, a registered trademark allows the use of the **® symbol**, signalling its protected status. The registration process involves submitting an application to a patent and trademark office, specifying the class of products and services for which protection is sought. It is essential to use clear and precise terminology, as general descriptions will be interpreted based on their literal meaning.

In addition, to get the registration your mark must meet and maintain during the duration of the right four requirements:

1. **Distinctiveness** -> The sign must be capable of identifying the goods or services of a particular business.
2. **Lawfulness** -> It must comply with legal regulations.
3. **Absence of deceptiveness** -> It should not mislead consumers.

4. **Novelty** -> It must be unique and not conflict with existing trademarks.

Distinctiveness

- ***Fanciful trademarks*** -> invented, made-up signs without any relation to the good that they distinguish -> i.e. Kodak or Exxon -> very strong distinctiveness
- ***Arbitrary trademarks*** -> already existing signs which are not normally associated with the good that they distinguish -> I.e. Ivory Soap
- ***Suggestive trademarks*** -> signs that suggest something about the real features of the product, without being really descriptive -> i.e. crush (orange juice company) -> less distinctiveness because it is rooted in an ensemble
- *Descriptive signs cannot become trademarks* -> example of descriptive signs comprehend:
  - Marks which are descriptive of the characteristics of the products / services
  - Marks of common use in business or language (Iper; Super; Mega; Extra; Deluxe; Standard)
  - Generic names of products/services

A sign can loose or acquire distinctiveness over time. Thus, entrepreneurs must invest or keep on investing in the distinctiveness of their trademarks. Distinctiveness is so important because, on the one hand, *entrepreneurs* are interested in *characterising their goods* (i.e. products & services) so that consumers can recognise them and who produce them over time; on the other hand, *consumers* are interested in *reducing their search costs over time;* i.e. the costs that they have to sustain over time in order to find goods that satisfy their needs and desires. Therefore, legislators are interested in distinctiveness because they work for establishing a one to one relationship between entrepreneurs and their goods. Trademarks serve a crucial role in identifying and distinguishing goods and services in the marketplace. Entrepreneurs use trademarks to help consumers recognise their products, ensuring that customers associate a particular sign with a specific business. The fundamental function of a trademark is to indicate the origin of goods and services, and its effectiveness depends on distinctiveness -> the ability of a sign to differentiate products from competitors. Distinctiveness varies in degree. Some trademarks, like Kodak for cameras, have *strong distinctiveness* because they bear no semantic connection to the product. Others, like Crush for orange juice, have a weaker distinctiveness, as the word relates to the product's characteristics. A trademark's distinctiveness is often determined by its *combination of elements*, such as name, symbols, colours, and shapes. Some trademarks, particularly descriptive signs (e.g., "Bottle" for bottles or "Shoe World" for a shoe store), lack inherent distinctiveness and cannot be registered unless they acquire distinctiveness over time. This phenomenon, known as **secondary meaning**, occurs when prolonged use and public recognition transform a generic term into a trademark (e.g., "Holiday Inn" for hotels). Conversely, trademarks can *lose distinctiveness when they become generic*, meaning consumers start using the brand name as a general term for a product category (e.g., "Nutella" for chocolate spread or "Lycra" for stretchy fabric). To retain trademark protection, companies must actively counteract this generalisation through advertising and brand reinforcement. Protecting distinctiveness is essential

because trademarks *enhance market efficiency* by providing consumers with reliable information about product *quality* and *origin*. By preserving a clear association between a brand and its goods, trademarks encourage competition, reward good entrepreneurs, and ensure that the market functions as an effective selective mechanism.

In addition, if this one to one relationship lasts over time, two further virtuous mechanisms occur:

- the firm succeeds in owing its merits and has the incentive to guarantee (and, in case improve) the quality of its goods -> *quality effect*
- The market can work in an efficient way -> *efficiency effect*

General trademarks -> Used for a wide portfolio of products, signalling a common source.
Specialised trademarks -> designed with marketing in mind, they instantly communicate key features of a specific product

Lawfulness

Trademarks cannot be contrary to public order and/or decency. Hence, offensive signs, such as swear words or racially derogatory images, or blasphemous logos cannot become trademarks!
The lack of lawfulness may also intervene later -> Washington Redskins – a NFL team – lost their team name trademark recently after the USPTO ruled that the name was insensitive to Native Americans. As a result, the team can no longer sue those who create and sell counterfeit Redskins merchandise. The Redskins organisation has appealed.
A trademark must comply with *legal and ethical standards*, meaning it *cannot be contrary to public order or decency*. Signs associated with terrorism, crime, or offensive content, such as symbols of extremist groups, cannot be registered as trademarks, as they violate fundamental societal values. Similar to distinctiveness, the lawfulness of a trademark may *evolve over time* due to societal and cultural changes. For instance, the Washington Redskins trademark, once legally accepted, later lost its validity due to changing perceptions of racial sensitivity. Conversely, trademarks related to sexual content, previously considered indecent, may now be more acceptable as societal norms shift. Thus, lawfulness is a *dynamic criterion*, subject to changing cultural attitudes and legal interpretations.

Absence of deceptiveness

A trademark cannot be deceptive. It cannot mislead consumers as to the nature, the features, and the origin of the goods and services that it addresses. That's the reason why it is better to use trademarks conveying fanciful messages, i.e. messages that are not connected with the actual properties of the products at stake … unless you are 100% sure of the soundness of these features. A trademark must not be deceptive, as trademarks serve to *convey accurate information that helps consumers make informed choices*. A trademark is considered deceptive if it *misleads* consumers about the nature, characteristics, or origin of a product or service. For instance,

arbitrary trademarks like *Kodak* are never deceptive because they have *no inherent connection to the products they represent*. However, suggestive trademarks can become deceptive if they *imply false attributes*.

There is a test to be done in order to determine the absence of deceptiveness:

- Does the trademark misdescribe something about the product/service?
- If so, is a purchaser likely to believe that the misdescription actually describes the product/service?
- If so, is the misdescription likely to affect a purchaser's decision to buy the product/service?

Some example of deceptiveness include:

- Cotonelle for toiler paper without cotton
- Shooting star organic as a trademark for dietary supplements, although they are not organic.
- Treehouse vegan restaurant for a restaurant that doesn't primarily serve vegan food

One should avoid disclosing misleading information about non-essential aspects that do not impact consumer interests. However, in practice, this rarely occurs. When creating a trademark, companies have limited space to communicate their key messages and therefore focus *only on crucial information for consumers*. The legal test requires assessing whether a misdescription is likely to deceive purchasers and influence their decisions. In reality, if false information is included in a trademark, it is typically done with the intent to mislead consumers, as businesses would *not invest time and resources in incorporating inaccuracies unless they sought to deceive*. Ultimately, the test is satisfied in the three specified cases.

Novelty and infringement

The rules governing novelty also govern infringement. The idea is that sigs that cannot enter the system because they are not new cannot circulate within the system either and vice-versa. Thus, you can read these rules in parallel.

Novelty	Infringement
A sign can be registered as a trademark only when: 1. It is not **identical** to an earlier sign, used/ registered for **identical** products; 2. It is not identical or **similar** to an earlier common sign, used/registered for identical/ similar products, if the claimed registration of that sign would **cause confusion** among customers, suppliers and consumers; 3. It is not identical or similar to an earlier **famous sign**, if the claimed registration would allow the would-be trademark owner to take a **free ride** on the fame of the earlier sign, or to **tarnish** its reputation, and/or to **blur away** its uniqueness.	In the course of trade, the trademark owner is entitled to prevent all unauthorised third parties from using: 1. Any sign which is **identical** in relation to goods or services which are **identical** with those for which an earlier trade mark is registered; 2. any sign where, because of its identity with, or **similarity** to, an earlier trademark and the identity or similarity of the goods or services covered by the earlier trademark and the sign, there exists a likelihood of confusion on the part of the public; 3. any sign which is **identical** with, or **similar** to, an earlier trade mark in relation to goods or services which are **not similar** to those for which the trade mark is registered, where the latter has a **reputation** and where use of that sign without due cause takes **unfair advantage** of, or is detrimental to, the **distinctive character** or the **repute** of the earlier trade mark

Famous trademarks and selling power -> a trademark can evolve beyond its origin function to become a **status symbol**, influencing consumer preference. Furthermore, trademarks may hold **selling power**, meaning that they have gained widespread recognition due to high product distribution or large advertising investments. Thus, these trademarks can leverage their reputation to expand into new markets or industries. Famous trademarks enjoy **enhanced legal protection** beyond their specific industry, preventing unauthorised use that might tarnish or dilute their value, or take a free ride on it.

There are several other further functions of trademarks:
- **Communication function** -> a trademark serves as a promotional tool
- **Advertising function** -> protects a company's investment in brand recognition
- **Investment function** -> shields a brand's value from unfair exploitation by competitors

Risk of confusion -> trademark confusion does not exist when the signs are clearly different, the products/services are completely unrelated and the similarity is minor, and the product/services are different. To assess confusion risk, key factors include:
- Visual, phonetic and conceptual similarities between trademarks

- Product/service similarities (market analysis)
- The distinctiveness of the earlier trademark
- Consumer perception and impression

By tradition, courts rely on a set of standards to determine whether consumers will likely be confused:

1. How *distinctive* the senior user's mark is.
2. The level of *similarity between the trademarks* in question. When considering the similarity between the two marks, they must be compared in their entirety. This often includes checking the sound, connotation, and appearance of both. If the marks are deemed to be similar in many aspects the court may rule that they are too similar and likely to cause confusion between customers.
3. The level of *similarity between the products or services* the trademarks in question represent. The basis for infringement is that a consumer may mistakenly purchase one item thinking that they were purchasing another. Therefore, for a case trademark infringement to occur, the products must be similar enough that similar trademarks could cause confusion. For example, the bleach called Clorit could be easily confused with Clorox bleach, though Lexus cars and Lexis computer database services are not likely to be confused.
4. The chance that the senior user will eventually *expand further* into the industry of the junior user.
5. Whether the junior user adopted the mark in *bad faith*, that is, by knowing that it was infringing someone else's trademark
6. *Actual evidence* that customers have been *confused* by the similar marks
7. The level of buyer sophistication in the marketplace in question -> The average consumer benchmark

Overall, novelty is a critical requirement in trademark law, ensuring that only *new and distinctive signs can be registered*. To conceptualise this, one can think of trademark law as a "kingdom" where entry is granted only to those signs that meet specific criteria. If a sign does not fulfil the novelty requirements, it cannot be registered as a trademark. Moreover, if a *trademark is already in use but was not examined for novelty, it may still be deemed infringing if it fails the novelty test post facto*. The fundamental principle is that all signs entering the trademark system must be new. If a trademark that does not meet this standard is already registered, it may be considered counterfeit or subject to invalidation. To determine whether a trademark is novel, legal systems apply three key tests:

1. **Identity with an Earlier Registered Sign** -> A trademark application will be rejected if the proposed sign is *identical* to an earlier registered trademark for the *same category of goods or services*. **Example:** If a company applies to register "Coca-Cola" for beverages, the application will be denied because the name is already protected for that category. If the product categories are different, however, identity alone does not necessarily lead to rejection

(e.g., "Coca-Cola" for a different industry like electronics might pass unless it violates other rules).

2. **Similarity and Consumer Confusion** -> If a proposed trademark is *similar* to an existing one and is intended for *identical or closely related goods or services*, it may still lack novelty if consumers are likely to be confused about its origin. The confusion test considers factors such as pronunciation, appearance, and meaning of the marks, as well as the nature of the products. **Example**: Registering **"Coco-Cola"** for beverages would likely be denied because it closely resembles "Coca-Cola" and could mislead consumers. However, registering **"Coco-Cola"** for transistors might be accepted because electronic components are unrelated to soft drinks, reducing the likelihood of confusion.

3. **Famous Trademarks and Free Riding** -> A trademark may be denied if it *closely resembles a well-known trademark*, even if the goods or services are entirely different. This is to prevent unfair advantage, brand dilution, or damage to reputation. There are three key concerns with famous trademarks:

    1. **Free Riding** -> If a company registers a mark similar to a famous brand (e.g., "Coca-Cola" for T-shirts), it could unfairly benefit from the established brand's reputation.
    2. **Tarnishment** -> If a mark is used for controversial or low-quality products, it could harm the reputation of the original trademark (e.g., using "Coca-Cola" for weapons).
    3. **Blurring** -> If a famous trademark's distinctiveness is weakened due to widespread use in unrelated industries, its strength as a brand could diminish.

The Role of Timing in Trademark Registration -> Trademarks operate on a *first-to-register* system in most jurisdictions. If a company registers a trademark first, later applications for the same or similar names may be denied. Some legal systems allow a *six-month priority period*, meaning that once a trademark is registered in one country, the applicant has six months to apply for protection in other jurisdictions without losing novelty. **Example:** If "Super Bianco" is registered in Italy in January 2025, the owner has until June 2025 to apply for the same trademark in France without anyone else claiming novelty in that period.

Traditional Trademarks vs. Famous Trademarks -> Traditional trademarks are protected only if there is a likelihood of confusion with an earlier mark. Famous trademarks have extended protection beyond confusion and can block registration of similar marks even if they are used for different types of products.

In the **1980s and 1990s**, as brands like Ferrari, Coca-Cola, and Gucci became *globally influential*, legal frameworks expanded to recognise that trademarks do more than indicate product origin—they also serve as advertising tools, status symbols, and investment assets. As a result, modern

trademark law now includes protection against *dilution, reputation damage, and unfair commercial exploitation* of famous marks.
Novelty is a crucial requirement in trademark registration, ensuring that new trademarks are not identical or confusingly similar to existing ones. While standard trademarks must pass a consumer confusion test, famous trademarks receive *broader protection* against unfair competition, brand tarnishment, and dilution. Understanding these principles helps businesses navigate the trademark registration process effectively and avoid legal disputes.

Indeed, for common trademarks, if you own a common trademark, you can claim its infringement when someone – the "*infringer*" – uses a sign that is identical or similar to your own trademark for competing products, i.e. products which are identical or similar to your own products, as long as this unauthorised use entails a *likelihood of confusion*. If consumers can tell your goods (i.e. cars) from somebody else's goods (i.e. lipsticks) by looking at the kind of needs that these goods satisfy, you do not need a trademark to make any differentiation! Therefore, you do not need to protect such a trademark against unauthorised uses.
If you own a famous trademark, you can claim its infringement when someone uses a sign that is identical or similar to your own trademark even for products that are not identical or similar to your own products, and even independently from the likelihood of confusion, if the infringer:

1. *Is taking an unfair advantage from such an unauthorised use* -> Adidas filed a suit against clothing retailer Forever 21, claiming that the retailer's three-stripe design on products constitutes a counterfeit product. Adidas claims it has put millions into branding the three-stripe design and holds a trademark on it.
2. *Is acting in detriment to* :
   - The reputation of the famous trademark (**Tarnishment**)
   - The distinctive unique character of the famous trademark (**Blurring**)

GUCCI-GUESS BATTLE

Gucci signs

Guess Sign

Gucci claimed that Guess infringed its trademarks. Guess counterclaimed that Gucci's "GS" were not distinctive … but generic and out of use -> a sign that does not meet the requirements for the registration as a trademark must be declared null and void

Guess won the cause

In some cases unauthorised uses of someone else's trademark do not consist in infringements. By and large, it happens when the trademark in question is used in a mere nominative/descriptive way **without malice or bad faith**, i.e. fairly and in good faith. For instance, there is no infringement if you use someone else's trademark:

- *that happens to be identical to your name and surname*
- *to explain consumers whether your spare parts are compatible with a specific branded durable good*
- *in comparative advertising* (clearly in US)
- *For non commercial purposes* -> in news reporting and news commentary or in parodies (clearly US – free speech)

Louis Vuitton Malletier vs. My Other Bag, 674 FED. Appx. 16(2nd CIR. 2016)

My Other Bag (MOB) sells simple canvas tote bags with the text "My Other Bag…" on one side and drawings meant to evoke iconic handbags by luxury designers, such as Louis Vuitton, Chanel, Fendi, on others. MOB's totes are a play on the classic "my other car…" novelty bumper stickers, which can be seen on inexpensive, beat up cars across the country informing passersby – with tongue firmly in cheek – that the driver's "other car" is a Mercedes (or some other luxury car brand). Louis Vuitton was perhaps unfamiliar with the "my other car… " trope or maybe it could not take it as a joke. In either case, it brought claims against MOB for **infringement** and **blurring**

Once you get the registration, for ten years (that you can renew perpetually) you become the owner of the sign and thus you become the only one entitled to:

- **To protect the value and your sole use of the trademark** -> You become the only one entitled to bring a legal action against who uses your trademark without your consent and, thus, get remedies against counterfeiters. -> The name of this action is **infringement action** … and this unless someone proves that your trademark is invalid, by bringing an **action (counterclaim) for invalidity**
- **To make money out of it** -> You become the only one entitled to decide who will use the trademark; how she will use it; how much she will pay for using it-> **Brand licensing** is a viable and profitable strategy possible as long as you own registered trademarks upon your signs.

Overall, we can say that when a party seeks to register a trademark, the Patent and Trademark Office (PTO) evaluates the application by verifying its distinctiveness, lawfulness, absence of deception, and novelty. Upon approval, the applicant becomes the legal owner of the trademark, granting exclusive rights to its use. Any unauthorised usage of the registered trademark constitutes infringement. There are different types of trademark infringement:

1. **Identical Signs for Identical Products** -> The most blatant form of infringement occurs when an identical trademark is used on identical products without authorisation. For instance, the unauthorised use of luxury brand names such as Fendi, Chanel, Hermès, and Louis Vuitton on counterfeit handbags constitutes a clear case of infringement. These brands, being highly exclusive, would not be legitimately sold through unauthorised street vendors.

2. **Regional Trademark Rights** -> Trademark rights can also arise through *use* in a specific geographical area, even without formal registration. For example, if a business in Bari has

acquired rights to the name "Super Bianco" through local use, another party attempting to use the same name in Bari would be infringing. However, if "Super Bianco" is used in Milan, where no local rights exist, no infringement would occur. If the Bari-based business later registers the trademark and expands into Milan, it must modify the name (e.g., "Super Bianco Stamp") to avoid infringement.

3. **Similar Signs and Consumer Confusion** -> Infringement may also occur when a trademark is *similar but not identical* to an existing mark, provided that consumer confusion is likely. Courts evaluate this based on the *likelihood of confusion*, rather than requiring actual confusion. For example: "Coca-Cola" for candies would likely infringe Coca-Cola's trademark, as consumers might assume an affiliation. "Coca-Cola" for electronic components would likely not infringe, as there is no reasonable consumer confusion.

Courts assess trademark infringement based on multiple factors, including:

- **Visual, phonetic, and conceptual similarities between the trademarks.**
- **Similarity between goods or services** ->the more related the products, the higher the likelihood of confusion.
- **Distinctiveness of the senior trademark** ->highly distinctive or well-known trademarks receive broader protection.
- **Likelihood of expansion** ->if the senior trademark holder is likely to expand into a new product category, confusion may be assumed.
- **Bad faith adoption** ->evidence that the junior user knowingly copied the trademark strengthens infringement claims.
- **Actual consumer confusion** ->market surveys and consumer perception studies are often used as evidence.

Famous trademarks receive extended protection beyond confusion-based infringement. Unauthorised use may constitute:

- **Unfair Advantage (Free Riding)** -> Exploiting the reputation of a famous brand for commercial gain (e.g., Adidas vs. Forever 21, where Adidas successfully argued that Forever 21's use of three stripes on clothing unlawfully benefited from Adidas' brand recognition).
- **Tarnishment** -> Associating a well-known brand with controversial or degrading content (e.g., "Victor's Secret" infringing on "Victoria's Secret").
- **Blurring** -> Weakening a trademark's distinctiveness by excessive commercialisation (e.g., Pierre Cardin's over-licensing, which diminished its prestige).

Trademark disputes are resolved through *court proceedings*, where infringement actions can be brought. Judges determine infringement on a case-by-case basis, using legal and market analyses to assess potential confusion or harm to the senior trademark owner.

By maintaining *strong trademark enforcement and strategic branding*, businesses can protect their intellectual property and prevent unauthorised exploitation of their trademarks.

In cases where a well-known trademark, such as Ferrari for luxury sports cars, already exists, a potential conflict may arise when the same name is used for another prestigious product, such as champagne. While there may be no direct consumer confusion, since automobiles and champagne belong to distinct markets, one could argue that the champagne producer is unfairly capitalising on the reputation of the Ferrari brand. However, under Italian and European Union law, every individual has the *constitutional right to use their surname in business*. This principle allows entrepreneurs to register trademarks based on their own names, *even if they coincide with existing famous trademarks*. This was the case with the Ferrari champagne producer, whose surname was Ferrari, thereby granting him the right to register and use it as a trademark despite Ferrari's established presence in the automobile industry. Nonetheless, legal provisions require that such a trademark be *sufficiently distinct in its visual presentation to avoid consumer confusion*. The Ferrari champagne trademark, for instance, differs significantly in font, color, and design from the Ferrari automobile brand. This differentiation ensures that both trademarks can coexist without misleading consumers. Crucially, the principle of *good faith* is essential in such matters. If an individual were to change their surname deliberately to exploit an existing brand's reputation, this would not be considered legitimate use. Thus, while individuals may use their surname in business, they must ensure that their branding is sufficiently distinct and that their actions are in good faith.

In the marketplace, many products are composed of *multiple components*, some of which may be sold separately as spare parts or accessories. To ensure consumers can identify whether a particular accessory is *compatible* with a given product, manufacturers often reference the trademark of the original brand. For example, when purchasing a phone case, consumers typically rely on packaging that explicitly states compatibility with specific brands such as Apple or Samsung. The use of another company's trademark in this context is *legally permissible*, provided it serves *solely to indicate compatibility and does not mislead consumers regarding the origin of the accessory*. It is essential that the use of the trademark does not create confusion or suggest that the accessory is produced, endorsed, or officially affiliated with the original brand. Furthermore, the principle of good faith applies. The presentation of the trademark must clearly communicate that it is being used to indicate compatibility rather than to imply ownership or brand association. This principle extends beyond physical goods to digital products, where interoperability must be transparently conveyed without infringing upon intellectual property rights.
The use of third-party trademarks is permitted in several contexts, provided it is done in good faith and does not seek to unfairly benefit from the reputation of the original brand. In the United States, *comparative advertising* allows the use of another company's trademark, though this is subject to stricter legal scrutiny. Additionally, trademarks can be used *freely in news reporting,*

commentary, journalism, and artistic works, as long as their use is for informative or expressive purposes rather than commercial exploitation. For instance, journalists reviewing a Chanel product may reference and even reproduce the Chanel trademark without legal repercussions, regardless of whether their assessment is positive or critical. Similarly, artistic works, such as photography capturing everyday life, may incidentally include recognisable trademarks without infringing upon intellectual property rights. *Parody* also constitutes a legally recognised exception. A notable case involved a tote bag that humorously referenced Louis Vuitton by depicting an illustration of a luxury handbag with the phrase "My Other Bag." Despite being a commercial product, courts ruled in favour of the parody, determining that its satirical message outweighed any potential commercial exploitation. However, such cases are assessed *individually*, and the legal distinction between parody and unauthorised commercial use remains complex. Overall, trademark owners have exclusive rights that can be *renewed indefinitely every ten years*. These rights allow for brand protection and commercial opportunities, such as brand licensing and merchandising, which will be further explored in subsequent discussions.

Trademarks and Domain name -> With the rise of the Internet, trademark protection has faced new challenges, particularly in relation to domain names, keyword advertising, and the potential dilution of brand identity. While this issue was more contentious a decade ago, it remains relevant in digital commerce and online marketing -> a domain name acts as a business identifier online, similar to a store sign in the physical world. A second-level domain (ie. “brandname.com") is is the core branding element. If a domain name closely resembles a registered trademark, it may infringe the registered trademark if there is confusion. If two companies happen to have the same registered trademark, the connected domain names goes to *the first which asked for it*.

A domain name consists of three parts: the prefix (e.g., "www"), the central domain name (which may include a trademark), and the suffix (e.g., ".com", ".edu", or country-specific domains like ".it" for Italy). The fundamental principle is that third parties cannot register domain names that incorporate someone else’s trademark without authorisation. For instance, only Giorgio Armani or his company may legally register "www.armani.it." The unauthorised registration of a domain name containing a trademark constitutes trademark infringement, particularly when the name closely resembles a well-known brand. However, complications arise when *two entities hold legitimate trademark rights to the same word*. For example, both Ferrari (the automaker) and Ferrari (the Italian sparkling wine producer) could seek to register “www.ferrari.it." In such cases, domain names are typically assigned on a first-come, *first-served basis* by the Internet Corporation for Assigned Names and Numbers (ICANN). The second claimant must modify their domain name (e.g., adding a distinguishing word like "wines" or "cars") to differentiate it from the first registered domain. A similar dispute occurred in the U.S. between United Airlines and United Van Lines, where the airline secured "www.united.com," while the moving company had to add "vanlines" to its domain name.

Another digital trademark issue concerns the use of *brand names as keywords in online advertising*. Search engines allow businesses to purchase keywords that trigger their ads when users search for specific terms. The legal question is whether a third party can *lawfully purchase a trademarked term as a keyword to direct traffic to its own website*. The general rule is that this practice is permissible if done in a descriptive and non-misleading manner. For instance, an independent distributor selling genuine Chanel shoes may purchase "Chanel" as a keyword to inform consumers that they stock the brand. However, a retailer selling counterfeit Chanel products, or one that does not offer Chanel items at all, would be infringing on the trademark. This principle aligns with the rationale behind permissible trademark use in spare parts marketing -> businesses may use trademarks to indicate *compatibility or product availability, but not to mislead consumers or exploit brand recognition unlawfully*.

Using trademarks as *search engine keywords* (ie. Google Ads) without the trademark owner's consent is generally allowed by the EU Court of Justice unless it misleads consumers or damages the trademark's functions (origin, advertising, investment). Trademark violation occurs when:

- the ad confuses users about whether the advertiser is affiliated with the trademark owner
- The ad leads to websites selling counterfeit products
- Famous trademarks cannot automatically claim infringement just because they are used as keywords

A related concern is whether widely recognised trademarks can *lose their distinctive character and become generic descriptors for an entire product category* (a process known as "*trademark vulgarisation*"). Some argue that brands like "Chanel" or "Nutella" have become synonymous with high-end fashion or hazelnut spread, respectively, allowing competitors to use these terms generically. However, trademark law protects brands from vulgarisation as long as the trademark owner actively maintains and promotes the mark's distinctiveness. As long as companies continue to invest in advertising and enforcement, their trademarks remain legally protected, regardless of how consumers colloquially use the term.

One of the complexities of digital trademark enforcement is that consumers are often unaware of the behind-the-scenes keyword advertising strategies employed by businesses. Since *keyword purchases are not directly visible to users, some initially questioned whether this constituted trademark infringement*. However, courts have generally ruled that the unauthorised use of trademarks in keyword advertising constitutes infringement when it misleads consumers or unfairly diverts traffic from the rightful trademark owner. Allowing such practices could lead to a significant number of consumers being directed to unrelated or deceptive websites, undermining the integrity of trademark protection. In conclusion, the principles of trademark law extend to the online environment, ensuring that *brands maintain control over their identity in digital spaces*. Domain name disputes, keyword advertising, and the risk of brand dilution require ongoing legal scrutiny to balance fair competition with the protection of intellectual property rights.

Regarding Hashtags, somebody can use someone's trademark as an hashtag or as a meta tag if it does it in a descriptive way but it can't if this causes confusion or leads to counterfeited products. A recent topic of debate in trademark law concerns the use of hashtags featuring well-known brand names on social media platforms such as Instagram. Users frequently include hashtags like #Adidas or #Ferrari to increase visibility, often in the context of sharing personal experiences, such as purchasing a new pair of Adidas shoes or enjoying a meal at McDonald's. From a legal standpoint, such uses *do not constitute trademark infringement*, even if the user benefits financially from their content. The key reason is that these hashtags serve a *descriptive function*, reflecting real-life events rather than misleading or commercially exploiting the brand. Personal accounts of consumer experiences, accompanied by brand-related hashtags, are considered legitimate and permissible under trademark law. However, infringement arises when *businesses use trademarks as hashtags to attract consumer attention unfairly*. For example, if a retailer uses #Chanel to promote their shoe collection but does not actually sell Chanel products, this would constitute a trademark violation. Conversely, if the retailer genuinely offers Chanel shoes, the use of the hashtag remains lawful, as it truthfully describes the available products. In summary, the use of trademarks in hashtags is generally acceptable when it accurately describes real experiences or products. However, commercial entities must ensure that such usage does not mislead consumers or falsely associate their business with a well-known brand.

Both keyword advertising and hashtags must be used in a way that *respects trademark rights*. Fair use applies when the trademark accurately describes a product being sold or an authentic consumer experience. However, misleading use intended to divert consumer attention unfairly is considered infringement.

The Piaggio case

Piaggio's iconic «Vespa» LX

«Ves» model

«Revival» model

«Cityzen» model

Piaggio **filed a complaint** against ZNEN's «Cityzen», «Revival» and «Ves» models, exhibited at a fair trade, for the **infringement** of its Italian and EU three-dimensional trademark

ZNEN **counterclaimed** and **responded** by requesting:

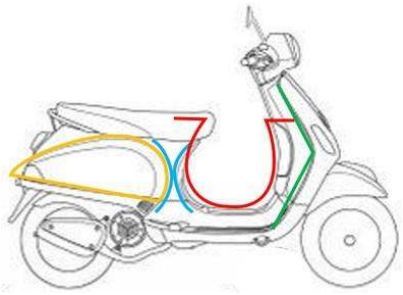
- **A declaration of invalidity** of Piaggio's three-dimensional trademark due to:

- *Lack of distinctive character*, as it consists of basic shapes and features typical of scooters and has been vulgarised, particularly by Lambretta;
- *The standard shape of the scooter*, which is dictated by technical and functional considerations, and which adds substantial value to the product.

- **A declaration of non-infringement** of Piaggio's three-dimensional trademark.

The Italian court hold that the main 4 features of the piaggio's shape are *distinctive*, because they have remained the same since the first model dated 1945:

- Arrow-shaped front shield profile
- The inverted Ω between the saddle and the front shield
- The X between the lower edge of the saddle and the rear fairing
- Cheek of the rear bodywork shaped like an elongated teardrop (identified by the CTE)



ARROW-SHAPED FRONT SHIELD PROFILE

THE INVERTED Ω

THE X BETWEEN THE SADDLE AND THE FRONT SHIELD

It is therefore considered that the distintive character of Piaggio's registered trademark derives from the constant presence, in Vespa scooters, of four individualising features, since their origin (1945).

These four characteristics identify the overall shape of the Vespa covered by the registered three-dimensional trademark, and constitute its «heart», clearly visible (even by the mere examination of the registered drawings) and original, and distinguish it from other scooters into the market, determining its traceability to the manufacturer Piaggio»

The Italian court hold that the Piaggio's shape *did not loose its distinctive character* because:

- *Vulgarisation should be excluded* -> The assessment should be based on models currently available in the Italian market, with no consideration given to discontinued models such as Lambretta.
- *the Vespa's shape was still very popular* -> A demographic survey confirmed its strong recognition among Italian consumers.

The Italian court hold that the *Piaggio's shape was a sign*. It:

- *was not the only possible shape* -> There are scooters without at least 1 of the Vespa's features
- *was not a shape required to obtain a technical result* -> The same result could be achieved without the reproduction of the arrow, the inverted omega or the x
- *was not a shape giving substantial value to the product* -> The Piaggio's design is not the only element that drives the purchase (price, fuel consumption, technical characteristics,…)

According to the court, The **"Ves"** model is a counterfeit product. Its overall appearance closely resembles the Vespa, incorporating elements such as mirrors, seat profile, and mudguard—features that are not inherently distinctive. Additionally, its name, "Ves," deliberately evokes "Vespa," reinforcing the imitation.

In summary, the case revolves around Piaggio's claim that a Chinese manufacturer, ZNEN, infringed on its Vespa scooter design by producing visually similar scooters and selling them in international markets, including Italy. Piaggio argued that the shape of the Vespa is protected as a *three-dimensional (3D) trademark*, meaning its distinctive design elements are legally recognised as identifying Piaggio as the source of the product. The central argument was that ZNEN's scooters bore a strong resemblance to Vespa models, leading to a likelihood of *consumer confusion*, as customers might mistakenly believe that the Chinese scooters were manufactured or authorised by Piaggio. Piaggio's claim was based on three key points:

1. *Ownership of a 3D Trademark* -> Piaggio asserted that the overall shape of the Vespa, which has remained consistent since 1945, had acquired *distinctive character* over time. It argued that this shape functions as a trademark, enabling consumers to associate it directly with the Piaggio brand.
2. *Likelihood of Consumer Confusion* -> Piaggio contended that the similarities between the ZNEN scooters and Vespa models were substantial enough to mislead consumers into thinking the products were related. Given that both were small motorbikes (scooters), the resemblance was sufficient to constitute infringement.
3. *Protection Against Unauthorised Use* -> By selling a product that closely mimicked the Vespa's shape, ZNEN was allegedly taking unfair advantage of Piaggio's brand recognition and reputation without authorisation.

The Italian court ruled in favour of Piaggio, rejecting ZNEN's defences. The ruling was based on several findings:

1. *Recognition of Distinctive Features*
2. *The court ruled that these distinctive elements had been present in all Vespa models over decades and were sufficient to grant the shape a unique identity.*
3. *Consumer Recognition & Market Surveys* -> A demographic study conducted in Italy confirmed that the Vespa's shape was still widely recognised by consumers, supporting Piaggio's argument that the shape functioned as a trademark.
4. *No Functional Necessity* -> The court determined that Piaggio's design was not dictated by technical necessity. While the Vespa's shape contributed to its aesthetics, there were multiple alternative designs that could achieve the same technical function (e.g., moving on two wheels while seated). Therefore, the shape was protectable as a trademark.
5. *No Vulgarisation of the Trademark* -> ZNEN's argument that the shape had lost distinctiveness due to other manufacturers, such as Lambretta, was dismissed. The court noted that Lambretta had stopped production decades ago, meaning it no longer influenced modern market perception.

As a result of the ruling:

- All ZNEN-manufactured scooters imported into Italy were *seized at customs* and prevented from being sold.
- The court recognised Piaggio's rights over the Vespa's distinctive design and ruled that ZNEN's scooters were *infringing copies*.
- However, because ZNEN's *production facilities were in China*, the Italian ruling could not enforce the destruction of manufacturing equipment.

This case highlights several key points in intellectual property law:

- **Protection of 3D Trademarks** -> Shapes can be trademarked if they acquire distinctiveness over time, even in industries where form and function often overlap.
- **The Challenge of Proving Functionality** -> Manufacturers accused of infringement often try to argue that the shape of a product is necessary for its function, but courts require strong evidence to support such claims.
- **International Enforcement Limits** -> National court rulings can restrict imports and sales within their jurisdiction, but enforcing intellectual property rights across borders (e.g., in China) can be challenging.

A related discussion in the case involved the difference between trademarks and patents. If a company develops a highly functional or aerodynamic shape (such as in car or motorcycle design), the most effective legal protection is through **patent law**, which grants exclusive rights for 20 years. After that period, the design becomes *public domain*, whereas a trademark (if maintained) can last indefinitely. This distinction is crucial for industries where innovation plays a major role, such as Formula 1, where aerodynamic advancements are often patented rather than trademarked.

In conclusion, Piaggio successfully defended its Vespa shape as a protected trademark, leading to the prohibition of Ben's infringing scooters in Italy. The case reinforces the importance of brand identity in design and highlights the legal complexities involved in proving trademark distinctiveness, functionality, and infringement in the automotive and consumer goods industries.

Darjeeling case

Looking at the background, the *Tea Board of India* holds a **Geographical Indication (GI)** and a **certification trademark** for "Darjeeling," exclusively associated with tea cultivated in the Darjeeling region of India. This designation ensures that only tea from this area can be marketed under the "Darjeeling" name, preserving its unique identity and quality. *Delta Lingerie*, a French company, sought to register "Darjeeling" as a trademark for women's lingerie and related products in the European Union. The Tea Board opposed this registration, arguing that using "Darjeeling" for lingerie would *mislead consumers* by exploiting the established reputation of Darjeeling tea, thereby *diluting its distinctiveness*. The case progressed through various stage:

1. *Opposition by The Tea Board* -> The Tea Board contended that the "Darjeeling" mark's use for lingerie would take unfair advantage of the renowned tea's reputation, leading to consumer deception.
2. *Decisions by EUIPO and General Court* -> Both bodies ruled in favour of Delta Lingerie, stating that the connection between tea and lingerie was too remote for consumer confusion to occur.
3. *Appeal to the Court of Justice of the European Union (CJEU)* -> The Tea Board escalated the matter, but the CJEU upheld the earlier decisions, concluding that the use of "Darjeeling" for lingerie did not mislead consumers or exploit the tea's reputation.

The case of Darjeeling highlights the complexities of geographical trademarks and the limits of their protection. The Tea Board of India had registered "Darjeeling" as a certification trademark to indicate that only tea produced in the Darjeeling region of India could be marketed under that name. This follows the principle of geographical indications (GIs), which *protect product names associated with specific regions* (e.g., Champagne for sparkling wine from France). The European Court of Justice (ECJ) and the EU Intellectual Property Office ruled against the Tea Board, holding that: There was no consumer confusion (people would not reasonably assume a connection between Darjeeling tea and a lingerie brand), there was no dilution (the use of Darjeeling in a different product category did not weaken its significance as a tea-related geographical indication) and the name Darjeeling would still remain exclusively associated with tea, as its geographical importance and reputation were well established. The ruling confirmed that while geographical trademarks can protect product authenticity, their *scope is not absolute*. A name like Darjeeling cannot monopolise all industries, and its use for unrelated goods, where confusion is unlikely, does not amount to infringement. The decision balances brand protection with market freedom, ensuring that geographical indications are not overly restrictive.

Lidl vs. Tesco (2023)

Lidl, the German discount supermarket chain, has a well-known logo featuring a yellow circle on a blue background with red elements. In 2020, Tesco, a major UK supermarket chain, introduced its “Clubcard Prices" campaign, which used a yellow circle on a blue background to highlight discounts. Lidl sued Tesco in the UK High Court for trademark infringement. Lidl argued that Tesco's use of the yellow circle was *confusingly similar* to its own logo, even though Tesco did not include the word “Lidl." Lidl claimed that Tesco was trying to *benefit from its reputation as a discount retailer* by making customers subconsciously associate Tesco’s promotions with Lidl’s low-price image. Tesco defended itself by arguing that a simple yellow circle *was too generic (deprived of distinctiveness)* to be a valid trademark and that customers were unlikely to be confused. n April 2023, the UK High Court ruled in favour of Lidl, agreeing that Tesco had infringed Lidl’s trademark. The court ordered Tesco to stop using the yellow circle in its Clubcard promotions. Tesco later appealed but was unsuccessful.
In particular:

- **Acquired Distinctiveness** -> The court acknowledged that while a yellow circle is a basic shape, Lidl had used it consistently as part of its branding for decades. Because of this long-term use, UK consumers had come to associate the yellow circle on a blue background specifically with Lidl’s discount supermarket brand
- **Consumer Recognition & Actual Confusion** -> The court found evidence that Tesco’s use of a similar yellow circle on a blue background for its Clubcard Prices campaign caused consumer confusion. Some customers mistakenly believed Tesco's discounts were linked to Lidl’s pricing, which suggested that the yellow circle had brand significance beyond just being a simple shape.

The Lidl vs. Tesco case involved trademark infringement over Tesco’s use of a yellow circle on a blue background in its promotions. Lidl argued that Tesco copied its branding to mislead consumers into associating Tesco’s discounts with Lidl’s low prices. Tesco claimed the design was generic and lacked distinctiveness. The UK High Court ruled in favour of Lidl, stating that the design had acquired distinctiveness through long-term use and had caused consumer confusion. Tesco was ordered to stop using the yellow circle, and its appeal was unsuccessful. This case highlights how a *simple shape and colour combination can acquire distinctiveness through long-term association with a brand*. Even if a design appears generic, if consumers strongly associate it with a specific company, it may be protected under trademark law.

Nike vs MSCHF (2021)

MSCHF, a Brooklyn-based art collective, collaborated with rapper Lil Nas X to create a limited-edition sneaker called **"Satan Shoes“**, by modifying Nike Air Max 97s to feature satanic imagery,

pentagrams, and even a drop of real human blood in the sole. Only *666 pairs* were made, selling at **$1,018** each. Even though Nike was not involved in the creation of these shoes, the design still prominently featured the Nike *Swoosh* logo. Many consumers believed Nike had endorsed or collaborated on the shoes. Nike quickly sued MSCHF for *trademark infringement and dilution*, arguing that the unauthorised modifications created confusion among consumers make them believe that Nike was associated with the *controversial product*. Nike also claimed that the shoes *damaged its brand reputation*, as some customers even called for a boycott. MSCHF initially argued that the shoes were *works of art* and protected by the First Amendment – freedom of expression. However, the court sided with Nike, granting a *temporary restraining order*, stopping further sales. Instead of dragging the case through a lengthy court battle, MSCHF *settled with Nike*, offering refunds to customers who wanted to return their Satan Shoes.

The use of a trademark in artistic works is *protected by free speech unless*:
- The use is explicitly misleading
- It has no artistic relevance beyond exploiting the brand.

In this case, the court ruled that MSCHF's use of Nike's trademark was *explicitly misleading:* indeed, many consumers actually believed Nike was involved. Furthermore, the court determined that MSCHF was engaging in commercial activity-> *selling physical goods, not just making an artistic statement.* The case would be different if Nike shoes were included in purely expressive works (like paintings or films) -> Andy Warhol's artwork and James Bond's use of Aston Martin, where trademarks were used descriptively or had significant artistic value, avoiding infringement.

Exercises on trademarks

Exercise 1

TechGlow, a German company, owns the EU trademark "LumiTech" for electronics devices. The company has been using the trademark since 2015 across multiple EU countries. In 2023, BrightWare, a Spanish startup, begins using the name "LumiTech" for smart LED bulbs across the EU.

Solution 1

TechGlow could bring an infringement action against BrightWare, arguing that the latter is unlawfully using an identical or similar trademark for similar products, thereby creating a *likelihood of confusion* among EU consumers. The case would likely fall under the second hypothesis of infringement, which requires:

1. *Identical or similar names* –> Both companies are using "LumiTech."
2. *Similar products* –> Smart LED bulbs fall within the broader category of electronic devices.
3. *Likelihood of confusion* –> Consumers may associate BrightWare's products with TechGlow, assuming they originate from the same company or are affiliated.

Potential Defences and Counterclaims by BrightWare

1. *No likelihood of confusion*: BrightWare could argue that consumers would not reasonably confuse its smart LED bulbs with TechGlow's electronic devices. This defence would depend on consumer perception and market practices -> whether consumers typically purchase such products from the same type of retailers.
2. *Geographical Argument*: BrightWare might claim that TechGlow has never actively used the LumiTech trademark in Spain, so there is no real consumer confusion in that market. However, this argument would be weak because an EU trademark grants its holder exclusive rights across all EU countries, regardless of where they actively trade.
3. *Invalidity of the Trademark*: BrightWare could challenge TechGlow's trademark by arguing that "LumiTech" lacks distinctiveness. They might claim that "Lumi" is a generic term for light-related products and that "Tech" is commonly associated with technology, making the name descriptive rather than distinctive. TechGlow could counter this by proving that the trademark has acquired distinctiveness through years of use.

Interplay Between Infringement and Novelty Arguments -> BrightWare's challenge could take two forms:

- *Opposition to TechGlow's claim of infringement*: Arguing that there is no likelihood of confusion.
- *Invalidity Action*: Claiming that TechGlow's trademark should not have been granted because it lacks distinctiveness.

Conversely, TechGlow could also take two approaches:

- *Infringement action in court*: Arguing that BrightWare is unlawfully using the LumiTech name.
- *Opposition to BrightWare's trademark registration*: If BrightWare attempts to register LumiTech in Spain, TechGlow could oppose it before the Spanish Patent and Trademark Office, citing lack of novelty.

TechGlow has a strong case for trademark infringement under EU law, while BrightWare's best defences would focus on lack of consumer confusion or an invalidity claim. The case would hinge on whether LumiTech is sufficiently distinctive and whether consumers are likely to be misled by the coexistence of both trademarks in the market.

Exercise 2

DeliciaBites a French company, owns an EU trademark for "ChocoDelight" covering confectionery products. SweetTreats, a Belgian food blogger, writes an online article titled desserts (not all of which are DeliciaBites products). The blog also contains affiliate links to third-party sellers.

Solution 2

DeliciaBites could initiate an *infringement action* against the Belgian food blogger, arguing that the latter's use of the term "Choco Delight" is unauthorised and creates a likelihood of confusion among consumers. The primary claim would be that the blogger is using an *almost identical name for similar products* (chocolate-based desserts), potentially leading consumers to believe that the

food blog is affiliated with or endorsing DeliciaBites' products. Given the identical wording with only minor variations (e.g., pluralisation), DeliciaBites could even frame the case as *double identity infringement*, where both the name and the product category are the same.

Defence by the Food Blogger -> The Belgian food blogger could counter the infringement claim by arguing that the use of "Choco Delight" is *descriptive*, rather than functioning as a trademark. The key legal argument would be that trademark infringement requires the use of a *protected sign "as a trademark"*, rather than in a descriptive or journalistic manner. The blogger could claim that the name was used solely to describe a *general category* of chocolate-based desserts, rather than to indicate the commercial origin of any specific product.

However, DeliciaBites could challenge this defence by asserting that the blogger is not merely using "Choco Delight" descriptively, but rather to *gain commercial advantage by monetising the article* through affiliate links. If the use of the term helps *drive traffic and generate revenue,* DeliciaBites might argue that this constitutes an *exploitative, unauthorised commercial use* of its trademark rather than a neutral journalistic reference.

To determine whether the use is *truly descriptive or commercial*, courts would examine factors such as:

- The *context* in which the term is used (e.g., whether it appears in a neutral, informative manner or is used to attract commercial engagement).
- Whether the blog reproduces DeliciaBites' branding elements (e.g., fonts, colours, logos).
- The *degree of influence* that the trademarked name has on consumer behavior -> whether readers are misled into associating the article with DeliciaBites' products.

Counterclaim: Invalidity of the Trademark -> As a further legal strategy, the food blogger could file a counterclaim asserting that the "ChocoDelight" trademark itself is *invalid* due to a *lack of distinctiveness*. The argument would be that "Choco" is an abbreviation of "chocolate" and "Delight" is a generic term used to describe desserts, making the phrase *descriptive rather than uniquely identifying*. If successful, this claim would render DeliciaBites' trademark unenforceable, preventing it from claiming exclusive rights over the term. To support this argument, the blogger could present evidence that:

- The term "Choco Delight" is commonly used in the industry to describe chocolate-based desserts.
- The blog post explicitly separates the words "Choco" and "Delight," reinforcing that it refers to a category of desserts rather than a specific brand.
- Multiple chocolate-based dessert brands use similar descriptive terms, further proving that the phrase lacks the distinctiveness required for trademark protection.

Additional Considerations -> If DeliciaBites wishes to argue *unfair advantage*, it would need to demonstrate that "Choco Delight" has *significant brand recognition* and that the blogger is intentionally leveraging its reputation. The *misleading nature* of the blog post could also be scrutinised to determine whether it creates consumer confusion regarding the origin of the listed products.

Overall, the dispute revolves around whether "Choco Delight" is being used in a *trademark sense or as a descriptive term*. If the court determines that the blogger's use is purely descriptive, the infringement claim will likely fail. However, if DeliciaBites can prove that the blogger's use commercially exploits the trademark, the company may have a stronger case. Additionally, the validity of the trademark itself remains a key question -> if the phrase is deemed too generic, DeliciaBites may not have enforceable rights over it at all.

Brand licensing and merchandising

As its core, contract law governs agreements between parties seeking to arrange their respective interests, whether divergent or converging. In the context of *intellectual property law*, a key contractual mechanism is the *trademark licensing agreement*.
A trademark license in and agreement between a trademark owner (the *licensor*) and a third person (the *licensee*) whereby the licensor permits the licensee to use her trademark, usually specifying the scope and the terms of the license:

- *Products*
- *Territory* (where the trademark can be use)
- *Market channel* (through which the licensed products may be distributed)
- *Duration*

This kind of agreement defines the *scope of use*, ensuring that the trademark is utilised within legally and commercially acceptable boundaries. If a licensee fails to comply with the agreed terms, they immediately become an *infringer*. This means that the unauthorised use of the trademark, even by a previously authorised party, constitutes trademark infringement. Thus, *compliance with the contract's conditions* is crucial to avoid legal consequences.
Numerus trademark licenses can co-exist at the same time, because trademarks are intellectual goods. Unlike material goods (such as land or real estate), intellectual property rights are *non-depletable*. This characteristic allows trademark holders to *grant multiple licenses simultaneously* without diminishing the trademark's value. By contrast, physical property is subject to wear and finite availability -> if a piece of land is leased to multiple individuals over time, excessive use may degrade its value. However, trademarks, patents, and copyrights can be licensed repeatedly without suffering a loss in economic utility. The primary motivation behind licensing intellectual property is *financial gain*. Trademark holders monetise their assets by granting licenses in exchange for compensation, typically in the form of *royalties or licensing fees*. This approach

maximises the commercial potential of trademarks while ensuring controlled and legally compliant use by third parties.
There are several advantages of brand licensing. Trademark licensing presents *mutual benefits* for both the licensor (the trademark owner) and the licensee (the third party acquiring usage rights). The decision to enter a licensing agreement is driven by strategic, financial, and market expansion considerations.

The *licensor* can:

- *Monetise the value of its trademark (via fees)* -> Licensing allows the trademark owner to generate revenue through fees or royalties, capitalising on the brand's commercial potential.
- *Decentrasse and differentiate her offer, as so to reduce business risks* -> Through strategic partnerships, the licensor can expand the product range without developing expertise in multiple industries. For example, a water bottle brand may license its name to juice or soda manufacturers, broadening its market reach.
- *Enlarge her geographic market, again as so to reduce business risks* -> Licensing agreements enable the licensor to expand into new geographical regions where they may lack direct distribution networks. For instance, a brand originating in one country may license its name to distributors in foreign markets.
- *Better characterise her supply: reaffirm via licensing core brand values allows consumers to embrace the brand as part of their everyday lives*
- *Strengthen the fame and popularity of the trademark, by increasing its spread* –> Licensing helps maintain a consistent brand image across different markets and sales channels, ensuring uniform customer perception.
- *Cost & Risk Sharing* –> Rather than bearing the entire cost of expansion and marketing, the licensor shares the financial burden and business risks with licensees.
- *Giving to each point of sale the same image (franchising)*
- *Achieve all these results by limiting its costs*

The *licensee* can:

- *increase the spread of her products/services, by making them either more recognisable or more appealing* -> If the licensed trademark is already well-known, the licensee gains instant market credibility and consumer trust, which can boost sales
- *Acquire know-how* -> Even if the trademark is not globally recognised, the licensor often possesses industry expertise, client networks, and operational knowledge, which the licensee can leverage.
- *Reduced Business Risks* –> The licensee minimises the risks associated with building a new brand from scratch, as they rely on the established reputation and commercial strategies of the licensor.

- *Market Penetration & Competitive Advantage* -> By associating with an established brand, the licensee gains an edge over competitors, accelerating their market entry and enhancing product visibility.
- *Lower Initial Investment* –> The licensee avoids the high costs of brand development, marketing, and customer acquisition, which are typically required for launching a new business or product line.
- *Achieve these results by limiting its costs*

A well-structured licensing agreement should *balance the interests of both parties*, ensuring that both the licensor and licensee benefit from the collaboration. If the licensee's expertise significantly enhances the brand's reputation, adjustments such as reduced fees or profit-sharing arrangements may be negotiated. Conversely, if the licensor's brand value significantly contributes to the licensee's success, licensing fees may be higher. Ultimately, trademark licensing is a strategic tool for business growth, enabling both parties to capitalise on existing strengths, minimise risks, and expand market influence.

On the other hand, there are several risks for the *licensor*:

- *No royalties*
- *Loss of control*
  - Blurring away the trademark's uniqueness, I.e. make consumers feel that anybody can afford the brand
  - The licensee's products are inconsistent with the concept associated to the trademark, so that its value is tarnished and twisted
  - Market confusion, I.e. if the extension overlaps the original too closely the core brand loses definition, its strategy position is weakened, and loyal consumers feel that their beloved brand has changed and lost its core values
  - The quality of the licensee's products is lower than that of the licensor's products: If the product isn't good enough, early success will lead to consumer disappointment, price discounting, bargain basement distribution, red faces, cheapened core brand and … more consumer deception … which is one reason why the licensor's trademark can be declared invalid (if the licensor does not do anything as a reaction)

The risks for the licensee are:

- *Very high license's costs*
- *Impossibility to have enough business to recoup her investments*
- *Impossibility to have enough time to recoup her investments*
- *Absence of help from the licensor*
- *Management of unsold goods* -> storage cost

Overall, one of the primary risks for a licensor is the potential for the licensee to fail in maintaining the quality standards outlined in the contract. This can lead to *reputational damage* for the

trademark and the company as a whole. If the quality of the products or services associated with the licensed trademark deteriorates, it may *mislead consumers*. This misrepresentation can provide grounds for legal challenges, including an action for invalidity, which could ultimately lead to the loss of trademark protection. Another significant risk for licensors is *financial instability or non-compliance by the licensee*, particularly if the licensee fails to make the agreed-upon payments. To mitigate this risk, licensors often require an *upfront payment* (a lump sum or an entry fee) alongside royalty-based payments that are calculated based on the licensee's sales revenue. This ensures that the licensor remains engaged in the success of the licensed product, maintaining a vested interest in the promotion and distribution efforts.

For the licensee, one of the key disadvantages is the potential for *financial dependency* on the licensor. Long-term licensing agreements can limit the licensee's ability to establish its own brand identity and develop independent trademarks. Economic dependence on a trademark may also create vulnerabilities if the licensor decides not to renew the contract or imposes stricter conditions in subsequent agreements. Moreover, the *high costs of licensing fees* can pose a substantial burden on licensees. If the sales projections do not materialise as expected, the licensee may struggle to cover the expenses associated with the agreement. Additionally, the absence of sufficient support from the licensor, such as a lack of know-how or inadequate marketing cooperation, can hinder the licensee's ability to generate successful sales. A further issue arises in *managing inventory*, particularly at the expiration of the licensing agreement. If the licensee has unsold stock bearing the licensor's trademark at the end of the contract term, they are legally prohibited from selling those products, as doing so would constitute trademark infringement. This can result in financial losses due to unsold inventory and additional storage costs.

Overall, while licensing agreements present mutual opportunities for both parties, they also involve *substantial risks related to control, financial commitments, and legal compliance*. Thus, both the licensor and the licensee must choose properly whether to enter into a licensing agreement as well as its terms and conditions:

- *Minimun fee*
- *Royalties*
- *Definition of a style guide*
- *The request of a sample and of a final product before marketing*
- *Quality control monitoring and auditing*
- *Advertising and other costs connected to promotion*
- *Exclusivity*
- *Termination - renewal*
- *Management of the unsold*
- *Infringement - litigation*

To mitigate these risks, licensing agreements typically contain key contractual clauses designed to protect both parties:

1. ***Financial Provisions***:
    1. Minimum Fee and Royalties: A combination of an upfront minimum fee and sales-based royalties ensures financial stability for both parties.
    2. Payment Structure: Payments are structured to balance the licensor's desire for immediate compensation with the licensee's need to manage financial risk.

2. ***Brand Protection and Usage Guidelines***:
    1. Style Guide Compliance: Licensors provide comprehensive style guides outlining precise usage instructions for their trademarks (e.g., brand colours, logo placement, and product specifications).
    2. Quality Control and Auditing Rights: The licensor may require pre-market approval of products, ongoing quality monitoring, and audits of the licensee's facilities to ensure compliance with brand standards.

3. ***Marketing and Advertising Requirements*** -> Joint Promotional Efforts: Licensees often request that the licensor participate in or financially support advertising campaigns to enhance product sales.

4. ***Exclusivity Clauses***
    1. Market Exclusivity for Licensees: To secure a stable business, licensees may negotiate exclusive rights to sell the licensed product within a particular territory or market segment.
    2. Territorial Exclusivity in Durable Goods: For products like automobiles and home appliances, territorial exclusivity prevents intra-brand competition (i.e., competition among distributors of the same brand) and ensures that pre-sale services (such as product education and demonstrations) are not compromised by price-cutting competition.

5. ***Termination and Renewal Terms***
    1. Automatic Renewal Provisions: Some agreements automatically renew unless explicitly terminated by either party.
    2. End-of-Contract Inventory Management: Provisions may allow the licensee to sell off remaining stock through discounted channels to mitigate financial losses while preventing trademark infringement.

6. ***Infringement and Litigation Clauses*** -> Jurisdiction Selection (Forum Shopping): Licensing agreements specify the governing legal framework and jurisdiction for dispute resolution, considering factors such as differences in how courts interpret "misleading trademarks" and "decency standards."

While licensing agreements offer numerous advantages, they also pose considerable risks that must be *managed through well-structured contractual terms*. Proper negotiation of financial

arrangements, exclusivity clauses, brand protection measures, and termination provisions can help both licensors and licensees maximise benefits while mitigating potential downsides.

What happens if the licensee *fails to respect the terms and conditions of the contract*? It depends. The holder of a trademark may invoke the rights conferred by that trademark against a licensee who contravenes any provision in her licensing contract with regard to:

- *Its duration*
- *The form covered by the registration in which the trade mark may be used*
- *The scope of the goods or services for which the license is granted*
- *The territory in which the trade mark may be affixed*
- *The quality of the goods manufactured or of the services provided by the licensee*

If the licensee fails to comply with the terms and conditions of the contract, the consequences depend on the *nature of the breach*. If the violation concerns fundamental aspects of the contract, such as the duration of the license, the scope of use, the designated territory, or the quality standards, it constitutes an *infringement*. In such cases, the licensor has the right to take *legal action*, which may include seeking injunctions, the destruction of unauthorised goods, or imposing financial penalties. However, if the breach pertains to other contractual obligations, such as payment deadlines, shipment terms, or marketing commitments, the licensee is merely in *breach of contract, not an infringer*. The licensor may seek remedies such as *damages, contract enforcement, or termination, but cannot claim trademark infringement*.

In other words, the licensee who fails to comply with these terms and conditions is an **infringer**. Differently, the licensee who fails to comply with other terms and conditions is a **breacher**. Against breachers, we can claim contract's execution and damages, while against infringers we can ask to cease and desist orders, the order to collect goods from trade, the order to destroy counterfeited products, the order to destroy machineries, compensation for damages, publication of the judgement and penalty payments.

EU exhaustion principle -> a trademark holder cannot prevent the circulation of its products once it (or someone it has authorised) has placed them on the EU market. Therefore, within the EU market, parallel import (which involves legally importing authentic, branded products into one country from another where they are marketed at a lower price, is allowed. However, there is an exception to this principle -> when the further commercialisation of the branded product involves a significant modification of it, the exhaustion principle does not apply.
The EU does not recognise international exhaustion. This means that if a branded product is lawfully sold outside the EU/EEA, the trademark holder can still oppose its parallel importation into EU/EEA.

So, regarding the principle of exhaustion, once a trademarked product has been *lawfully placed on the market within the EU* (or the European Economic Area), the trademark owner *loses the right*

to control its further distribution. This means that after the first authorised sale, the product can circulate freely within the EU, and the trademark holder cannot prevent resale. For instance, if a retailer purchases a batch of discounted goods in Poland and sells them in France at a lower price, the trademark owner cannot use intellectual property law to block this practice. However, if the reseller *alters the product*, such as repackaging it in a way that harms the brand's reputation, the trademark owner may oppose further distribution.

We can give an example of parallel imports in EU
Velora, a premium sportswear brand, holds an EU trademark for its high-end running shoes. The company follows a strict pricing strategy to maintain its brand's exclusivity and prestige across EU markets
Velora sells its latest "V-Run Pro" running shoes in France through an exclusive distributor at a premium price. However, the same shoes are sold at a significantly lower price in Poland due to a local promotional campaign.
A Polish retailer, SportTrade Polska, lawfully purchases a large batch of V-Run Pro shoes in Poland at the discounted price and then imports them into France, where it sells them for far less than the price set by Velora's French distributor.
Velora attempts to block SportTrade Polska from reselling the shoes in France, arguing that: The discounted sales in Poland were *intended only for that market*; the parallel import disrupts its pricing strategy in France and *damages its brand's exclusivity*.
However, under EU law, once Velora has placed its trademarked goods on the market anywhere in the EU/EEA, it *cannot stop further resale* within the EU/EEA. Since the V-Run Pro shoes were first sold within the EU (in Poland) with Velora's consent, its *trademark rights are exhausted*. Velora cannot prevent SportTrade Polska from reselling them in France, even if it disrupts its pricing strategy.
In other words: SportTrade Polska can *legally resell* the shoes in France despite Velora's objections and Velora cannot rely on its trademark rights to block parallel imports within the EU, as exhaustion applies after the first legitimate sale in the EU/EEA. The only exception would be if Velora could prove that SportTrade Polska *altered the products in a way that damages the brand's reputation*, such as repackaging the shoes incorrectly or misleading consumers.

Indeed, the exhaustion principles does not apply if there are legitimate grounds for the trademark owner to oppose the further circulation of goods. "*Legitimate ground*" arises in cases where a *selective distribution system exists* and the manner in which the third party invoking exhaustion markets the product without the holder's consent causes significant harm to the image of the trademark. A selective distribution system is a distribution system where the supplier undertakes to *sell the contract goods or services, either directly or indirectly, only to distributors selected on the basis of specified criteria* and where these distributors undertake not to sell such goods or services to unauthorised distributors within the territory reserved by the supplier to operate that

system. It must concern certain categories of products, like luxury goods (involving the need to remunerate large investments) or high-tech items (requiring specific assistance for the buyer). Other scenarios falling under the hypotheses include:

- *Variations or alterations of the product* (i.e. tampering or alterations occurring after the product has been placed on the market)
- *Removal of the trademark or other indications on the product packaging*
- *Repackaging or relabelling of the product*

Selective distribution contracts introduce additional complexity. If a producer imposes *restrictions* on which retailers may sell its products, a wholesaler that violates these terms breaches the contract but does not commit trademark infringement. The producer can take legal action for breach of contract, potentially barring the wholesaler from future sales or seeking damages, but *cannot demand the destruction of goods or impose penalties as it could in an infringement case*.

An example of parallel imports outside EU is: Fashion brand LuxMode owns and EU trademark for its luxury handbags. The company sells its products in various EU countries and also in Switzerland, a non-EU country. LuxMode maintains strict pricing policies, ensuring that its products remain premium in the EU market. A Swiss retailer SwissTraders Ltd. legally purchases LuxMode handbags in Switzerland at a discounted price and then imports them into Germany without LuxMode's permission. Hence, in Germany, SwissTraders is capable to resell the handbags at a lower price than LuxMode's authorised German retailers. LuxMode argues that its trademark rights allow it to prevent SwissTraders from selling the handbags in the EU without its authorisation. The company claims that the lower-priced imports harm its luxury brand image and disrupt its EU pricing strategy. It is true that, under the exhaustion principle, once LuxMode has put its trademarked goods on the EU market, or consented to their sale within the EU market, it cannot stop further resale within it. However, Switzerland does not belong to the EU. Since the handbags were first sold outside the EU (in Switzerland) LuxMode could still object to their resale in the EU, unless it had previously consented to their distribution in Switzerland.

Exhaustion does not apply to parallel imports from outside the EU. If a product is first sold in Switzerland, for example, a buyer cannot freely resell it within the EU without the trademark owner's consent. Similarly, the licensor must actively monitor the licensee's use of the trademark. If the licensor tolerates unauthorised use without taking action, it risks weakening its trademark rights. This principle aligns with the need to *prevent trademark dilution*, ensuring that misleading or unauthorised usage does not erode consumer trust.

What if the licensor does not do anything against the infringer? If the licensor (trademark owner) does not do anything against the licensee that is using its trademark without being compliant with the contract, she runs two risks:

1. *The risk of loosing money and reputation*

2. *The risk of loosing the trademark for its "new" misleading use* -> this risk is high when the licensee impairs the quality of the licensed goods and services

Example of trademark license

The grant of the license -> subject to the terms and conditions of this License, Licensor hereby grants to Licensee the (exclusive?) right to use the Entity (i.e. a trademark, the name or the image of a fictional or a real character) within the territory of ___ and solely to manufacture?, sell?, distribute?, advertise?, the following products: ___

Exclusivity -> Licensor shall not grant to anyone else…the right to use the Entity within the Licensed Territory and for the Licensed products

Beyond the boundaries of the License -> other than as expressly set forth in this License, Licensee has absolutely no right, title for interest in or to the Entity or the use thereof. Licensee acknowledges that it is only acquiring the right to use the Entity in connection with the Licensed Products, within the Licensed territory, for the Term set forth in the Agreement and subject to the terms hereof.

Licensed territory -> Licensee shall not, directly or indirectly, sell, market, distribute or deliver, the Licensed Products outside of the Licensed Territory without prior written and discretionary consent of Licensor. Licensee shall not knowingly, directly or indirectly, sell, distribute or otherwise deliver or cause to be sold, distributed or delivered, the Licensed Products to any individual or entity who intends to, or is likely to, or to whom Licensee reasonably believes might, sell the Licensed Products outside the Licensed Territory

Right of the Licensor -> Nothing contained herein shall in any way restrict or prohibit Licensor from licensing, marketing, manufacturing, selling or distributing the Licensed Products outside the Licensed Territory.

Approval regarding other products/territories -> Licensee acknowledges that Licensor may grant additional licenses in the future for territories, products and categories not presently licensed and not within the scope of this License. Permission of Licensor for Licensee to manufacture or distribute the Licensed Products within an area, which is not, in the opinion of the Licensor, within the scope of the License, shall not constitute a waiver of the right of Licensor to later disapprove any distribution area.

Duration -> the initial term of this License is 3 Years

Effects of the license after termination -> upon termination of the License, Licensee shall cease all use of the Entity in any territory and for any product

Renewal -> Licensee has the option to extend the term of this License for an additional period of five (5) Years ("Option Period"). Said option must be exercised by providing written notice to

Licensor at least six (6) months and no more than nine (9) months, prior to the end of the Initial Term. Said option may only be exercised if Licensee is in full compliance with its obligations under this Agreement as of the time of exercise of the option and as of the date of commencement of the Option Period. In the event of any extension or renewal of this Agreement as provided herein, all terms and conditions of this Agreement shall remain in full force and effect, except as otherwise set forth in this Agreement. Should Licensor, at any time, exercise its right under this Agreement to terminate the rights of Licensee hereunder, thereafter Licensee shall not have any option to extend the term of this Agreement.

No right to register -> Licensee shall not apply anywhere in the world, to register any copyright, trademark or trade name that in any way mentions or uses the Entity, or anything which is confusingly similar to the Entity licensed hereunder, without the express prior written consent of the Licensor

Best Efforts -> Licensee shall use its best efforts to manufacture, market, sell, distribute and advertise the Licensed Products in order to meet the demand for the Licensed Products in the Licensed Territory and to uphold, protect and defend the image and reputation of the Licensed Products and the integrity of the Entity.

Advertisement Payment Sharing -> As payment for advertising, Licensee shall pay to Licensor an amount equal to ___ percent of Licensee's Net Sales. Licensee shall spend at least ___ for advertising and/or public relations to "launch" the Licensed Products during 2012. All advertising used by Licensee must be approved in writing by Licensor, in its sole and absolute discretion, prior to its publication, exhibition or other use.

Royalty payments -> In consideration for the license granted pursuant to this Agreement, the Licensee shall pay to Licensor, each month, an amount equal to seven (7%) percent of the Net Sales of the Licensed Products (“Royalty”)

Advance payment of Royalty -> concurrently with the execution of this Agreement, the Licensee shall pay ti Licensor a non-refundable advance in the amount of ___

Guaranteed Minimum Net Sales -> During the Initial term of this Agreement Licensee guarantees that its Net Sales shall be in the amount set forth on Schedule “A” during each year

Guaranteed Minimum Royalty Payment -> Regardless of whether or not Licensee achieves the required Guaranteed Minimum Net Sales, Licensee shall pay to Licensor a Guaranteed Minimum Royalty Payment for each Year during the term hereof, in accordance with the terms of Schedule "A" attached hereto (the "Guaranteed Minimum Royalty”).

Control over the licensed products -> Licensee agrees that Licensor shall be entitled to reasonably determine whether a particular style or design of a Licensed Product may be offered for sale by Licensee in accordance with some specific requirement specified herein. Licensee

agrees that it will not manufacture, market, sell, distribute and advertise, either directly or indirectly, any style, design or product which Licensor in its reasonable discretion disapproves.

Product standards -> Licensee shall not sell, distribute or otherwise market the Licensed Products unless they are of the highest standards and quality and unless each product has received the prior written approval of Licensor prior to distribution thereof, subject to the terms and conditions of this Paragraph

Approval of design concept -> As soon as Licensee has developed a design for a Licensed Product that it desires to produce, sell and market, Licensee shall submit three (3) design samples or drawings thereof if samples are not available, at no cost to Licensor, of said product, along with color and fabric samples, if applicable, to Licensor for approval, along with one (1) complete set of all promotional and advertising material associated therewith. Within five (5) working days following the receipt of any design sample, Licensor shall either approve or disapprove the product or indicate changes to be made. Failure by Licensor to so note approval, disapproval or changes within said five (5) working days shall be deemed approval. In the event changes are required, Licensee shall be required to resubmit the revised design sample or drawings thereof if samples were not originally submitted, for approval with the recommended changes.

Inspections -> The licensor and its authorised agents and representatives shall have the right, upon reasonable notice, to visit licensee's place(s) of business at all reasonable times and to review the products, advertisements and marketing materials of the licensee.

Audit -> Licensee shall keep complete and accurate books and records at its principal place of business covering all transactions relating to this Agreement. Licensor and/or its duly authorised representatives shall have the right, at reasonable business hours and upon reasonable notice, at the place where such records are normally maintained, to inspect, audit, examine and make copies of such books and records and all other documents and material in Licensee's possession or control regarding any transactions relating to this Agreement.

Annual and quarterly financial statements -> not later than one hundred twenty (120) days after Licensee’s fiscal year-end,(or calendar year-end as the case may be), Licensee shall furnish Licensor with an audited annual financial statement which shall include an income statement and a balance sheet of the Licensee prepared in accordance with generally accepted accounting principles consistently applied. In addition, within sixty (60) days of the end of each calendar quarter during the term of this License, Licensee shall furnish Licensor with quarterly financial statements prepared in accordance with generally accepted accounting principles. In the event an audited statement is not prepared by Licensee, Licensee shall nevertheless furnish Licensor with its unaudited financial statements, certified to be correct by the Chief Executive Officer or Chief Financial Officer of Licensee.

Merchandising -> there is no piece of law where we can find a definition of what merchandising is. We have elicited the notion of merchandising from the practice -> A merchandising contract is an agreement in which the owner of a popular entity grants a third party permission—against remuneration—to use it for marketing goods and/or services that are distinct from those for which the entity originally gained success.
The first cases of merchandising go back to the beginning of the 20th century, when in the United States, the image of Jodie Maggio, who was a baseball player, started being reproduced on several T-shirts sold to the supporters of the New York Yankees, that was the team of Jodie Maggio. The practice of merchandising involves *leveraging the popularity of well-known individuals or fictional characters to market and sell products*. Historically, famous figures such as Shirley Temple, a child actress with distinctive blonde curls, saw their likenesses reproduced in dolls to appeal to consumers. Similarly, the commercial industry has utilised the names and images of celebrities to *increase the desirability and perceived value of various products*, including inexpensive items like T-shirts and toys. This strategy was further adopted in the 1980s by companies like Walt Disney, which capitalised on the *widespread recognition of characters* such as Mickey Mouse and Donald Duck to sell everyday products, generating additional revenue. Over time, the legal community established the concept of a **Merchandising Contract**, which is a formal agreement granting a third party the right, typically in exchange for remuneration, to use a well-known entity's name, image, or likeness to market products or services unrelated to the entity's original industry. Ultimately, merchandising allows companies to *exploit the selling power of popular figures and characters*, ensuring that such agreements generate financial gains for the rights holders. A Merchandising Contract is a legal agreement in which the owner of a well-known entity grants a third party the right to use that entity's image, name, or likeness to market products or services in exchange for remuneration. The key elements of a Merchandising Contract include:

1. **A Popular Entity with Selling Power** –> The entity must have significant public recognition and influence, making it valuable for marketing purposes.
2. **Merchandising Classes** –>The contract must specify the categories of products or services that will bear the entity's name or likeness, typically outside its original field of success.
3. **Permission to Use the Popular Entity** –> The owner must grant explicit rights to the third party, with usage conditions and financial compensation outlined.

From a legal perspective, the ability to grant such permission implies that the owner holds an *exclusive right* over the popular entity. This right ensures that only the owner can control its commercial use and authorise third parties to exploit it. The legal term for this exclusive control is crucial in intellectual property and contract law.

There are 3 kinds of merchandising:

- *Fictional character* -> character merchandising -> This involves the commercial use of fictional characters such as Mickey Mouse, Donald Duck, or Iron Man.

- *Real character* -> personality merchandising -> This applies when a well-known person, such as a celebrity or athlete, is used for marketing products.
- *Famous brand* -> brand merchandising -> subcategory of trade licensing -> This involves the use of well-established brand names and logos to market products, often as part of trademark licensing.

There are several rights underlying *character merchandising* -> successful entities = image or fictional character name, which may be the subject of the following property rights: *copyright or trademark rights* -> copyright consists of a series of rights of economic use that arise with the realisation of the work by author among the exclusive rights of economic use, the one with the greatest practical impact for merchandising is that of reproduction

Moreover, there are different rights underlying *personality merchandising* -> successful entity = image or name of famous person. They may be the subject of the following exclusive rights:

- *Copyright / image right* -> the protection of the image of the natural person may extend to include elements not directly referable to the person himself, such as clothing, ornaments, make-up and other things that by their peculiarity immediately recall in the viewer's perception precisely that character to which those elements are now inextricably linked
- *Right to the name*
- *Trade mark rights* -> if well-known, may be registered or used as a trade mark only by or with the consent of the right holder...: personal names, signs used in the artistic, literary, scientific, political or sporting fields

Owners of fictional characters, such as Marvel with Iron Man, primarily rely on **copyright law** for protection. Copyright grants exclusive rights over any representation of a character, ensuring that its *image is safeguarded across different media formats*. Unlike trademark protection, which can be more static, copyright applies broadly to any adaptation or reproduction of the character's image. However, character names are generally **protected under trademark law** rather than copyright. This is because courts worldwide typically do not recognise a single name as sufficiently creative for copyright protection. Consequently, companies register character names as trademarks and issue *trademark licenses* for their use, while *copyright licenses* cover the visual depiction of the characters.

- **Brands** are protected under *trademark law*, which governs brand merchandising and ensures that brand names and logos remain distinct in commerce.
- **Famous individuals** rely on a combination of *privacy rights* and *publicity rights* to control the use of their name and likeness.

In public places, privacy rights are limited, allowing journalists and photographers to capture and publish images of public figures. However, in private settings (e.g., a celebrity's home), privacy rights apply more strictly, preventing unauthorised photography or publication. Publicity rights grant famous individuals control over the commercial use of their name and image, preventing

unauthorised endorsements or merchandising. These legal frameworks ensure that merchandising contracts are enforceable and that rights holders can maintain control over the commercial use of their intellectual property.

When a public figure's image is used commercially without their consent, the primary legal concern shifts from privacy rights to personality rights. In public places, the *right to inform the public* often prevails over privacy rights. Journalists and photographers can lawfully capture and publish images of public figures, even without their consent. However, this principle does not extend to private settings such as a celebrity's home, where privacy rights remain protected, and unauthorised photography or publication constitutes a violation. If an image of a famous person is used for *commercial purposes*, such as being printed on a T-shirt or included in advertising, the individual can claim a *violation of their personality rights*. Personality rights, which originated in the United States and have been adopted in various legal systems, grant celebrities control over the commercial use of their name, image, and likeness. These rights are distinct from the general right to protect one's reputation, which applies to all individuals, regardless of fame. While media outlets can profit from publishing images of celebrities under the principle of the right to inform, this exemption does not extend to commercial merchandising or endorsements. The legal distinction lies in the *purpose of the use*: news reporting and public interest justify publication, whereas commercial gain requires authorisation. Celebrities can assign different aspects of their personality rights through contractual agreements, often dividing rights over their image, name, and distinctive attributes among different agencies or companies. These agreements are typically *time-limited* and structured to ensure control over branding and commercialisation. Private individuals cannot commercially exploit a celebrity’s image without consent. While selling a photograph to a media organisation may be permissible if it serves a newsworthy purpose, selling an image for merchandising or advertising without authorisation infringes on personality rights. In essence, public figures relinquish certain privacy protections due to the public’s interest in their lives, but they maintain *exclusive rights over the commercial use of their image and identity*.

There is an ongoing debate about the legality of paparazzi activities. Some argue that following celebrities to obtain images is acceptable, while others contend that the deliberate orchestration of blackmail operations crosses the line into criminal behavior. The determining factor often lies in the *level of organisation* and the intent behind obtaining and leveraging such photographs. On a related topic, there are now technological methods to prevent unauthorised photography, such as scarves that distort facial recognition in images taken with a flash. Whether these devices infringe upon journalistic freedoms remains a subject of legal discussion, but they are comparable to wearing disguises, which is generally permitted. Additionally, public figures who serve as brand ambassadors are subject to *contractual obligations*. If a celebrity representing a brand, such as Samsung, is photographed using a competitor’s product in a public setting, this could violate their sponsorship agreement and lead to contract termination. However, if the image was taken in a private setting where no one had the right to capture it, the celebrity may be able to challenge its

use. In the realm of intellectual property, disputes over the *ownership of widely recognised symbols*, such as the smiley face, highlight the importance of copyright and trademark protections. The original creator's rights depend on factors such as authorship, employment status, and the degree of originality in the design. Some argue that highly recognisable images should be part of the public domain, but legal protections often remain in place when sufficient creativity and novelty are present. Ultimately, legal protections for names, images, and reputations vary depending on whether the subject is an individual, a fictional character, or a brand. Trademarks are commonly used to protect names, while personality rights safeguard a person's likeness. Understanding these distinctions is essential in cases involving licensing, merchandising, and publicity rights.

Exercises on licensing

An Italian company, TopSport Srl, has signed an exclusive merchandising deal with Zlatan Ibrahimovic, granting them the rights to sell official jerseys, merchandise, and other products featuring his name and image in the Italian market. The agreement includes a 3-year image rights license with specific territorial restrictions. At the same time, a Spanish company, Futbol Global SL, has secured a similar license for the Spanish market, allowing them to sell official Ibrahimovic-branded products exclusively in Spain. However, an indipendent retailer SportFan Italia, has been purchasing large quantities of Ibrahimovic's official jersey from Futbol Global SL at a lower price in Spain ad importing them into Italy, selling them at a lower cost than the officially distributed products from TopSport Srl.

Advertising and promotion

We can rely on different strategies in order to promote our products, advertising, sponsorship, and as a subcategory of advertising, also behavioural advertising. We can also develop public relations, engage in loyalty programs, or use other kind of techniques, such as word of mouth referrals, user-generated content, but our goal for the future classes will be going through the rules regarding advertising and sponsorship, and also the kind of contracts we can conclude, in order to create an advertising campaign or a sponsorship agreement.

In this course, we'll focus on:

- Advertising -> general concepts, misleading practises/adv, aggressive advertising, comparative advertising and discriminatory advertising
- Some rules relating to the working of online advertising -> I.e. behavioural advertising
- Sponsorship agreements and ambush marketing

Advertising -> the making of a representation in any form in connection with a trade, business, craft or profession in order to promote the supply of goods or services. Advertising is a way to make promotion of goods or services and it may be made in any form, including a simple message to the extent it serves to the scope of promotion of the relevant good or service.

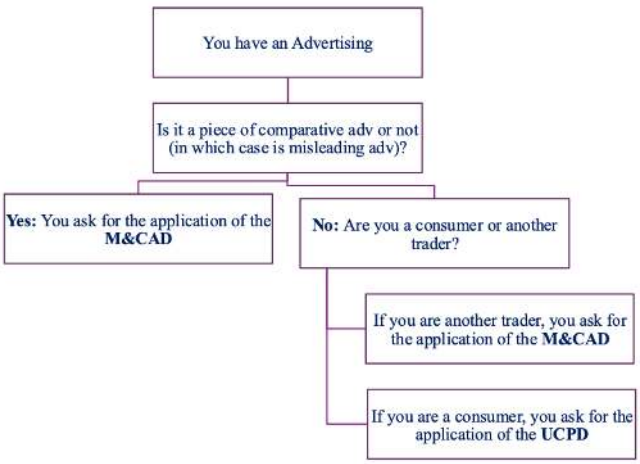
The law adopts a notably broad definition of advertising, encompassing any form of communication or representation intended to promote the sale of products or services. This includes both *direct* methods, such as purchasing ad space in print or digital media, or broadcasting commercials, and *indirect* approaches, where no specific product is mentioned but brand visibility and association with certain values or ideals are enhanced. An illustrative example is Benetton's controversial advertising campaigns, which, despite not directly promoting its clothing products, served to reinforce brand identity and awareness, thus qualifying as advertising under legal standards. Given this expansive interpretation, it is essential to understand that advertising is subject to numerous regulations. While these may initially appear complex, they are principally governed by **two EU directives**, which establish overarching principles applicable across all member states. However, each member state retains the authority to translate these general norms into more detailed rules tailored to specific categories and national contexts.

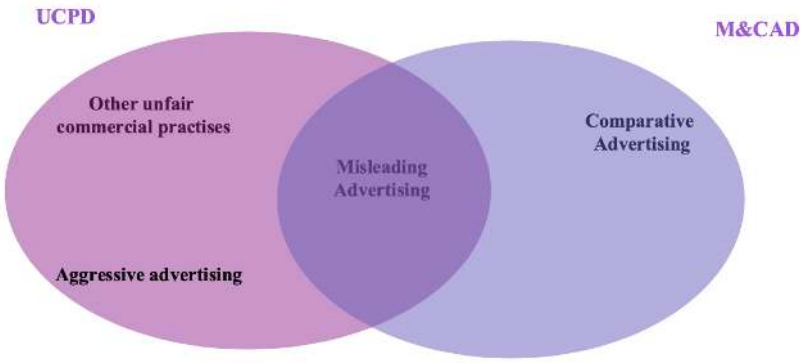
The EU legal framework and scope of application -> there are 2 main EU directives so to ensure so called “harmonisation” (with the intent to ensure a set of common principles and rules that guarantee the same minimum level of protection across the entire EU):

1. *Misleading and comparative advertising directive - M&CAD* -> Eu rules protecting *traders* against misleading and comparative advertising. *Subjective requirement*: it applies in B2B relationships. *Objective requirement*: it covers both misleading and comparative advertising

2. *Unfair Commercial practices directive - UCPD* -> EU rules protecting consumers from unfair practices before and after a commercial transaction. *Subjective requirement:* it applies in B2C relationships. *Objective requirement:* it covers also other unfair commercial practices (not only advertising) and aggressive advertising, but it does not cover specifically comparative advertising (comparative advertising is covered in the context of misleading advertising when it is misleading, but not separately)

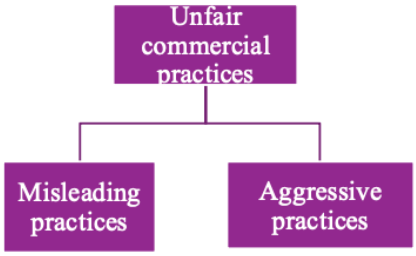
This raises the question - when should each directive be applied? To answer the question, follow the algorithm below:





As said, UCPD prohibits unfair commercial practices (any act, omission, course of conduct or representation, commercial communication, including advertising and marketing) in general (misleading advertising is only one of them).

Despite their different scopes, both directives rest on shared principles: advertising must be *truthful, transparent, and based on verifiable facts*. Misleading or deceptive communication is prohibited, regardless of whether it targets businesses or consumers. Comparative advertising falls exclusively under the B2B directive, while aggressive advertising is addressed solely in the B2C directive. Misleading advertising is covered by both. In determining which directive applies, one must first ascertain whether the message qualifies as advertising, and if so, whether it is comparative in nature. Comparative advertising automatically invokes the B2B rules, while non-comparative advertising is subject to either directive depending on the nature of the audience. This legal structure ensures a consistent standard of fairness and clarity in commercial communication throughout the European Union.



Practices that are:
(i) contrary to the requirements of **professional diligence**; and
(ii) are **likely** to **materially distort** the economic behavior of the **average consumer** whom they reach, or to whom they are addressed

Trader -> any natural or legal person who is acting for purposes relating to his trade, business, craft or profession and anyone acting in the name of or on behalf of a trader

Product -> any good or service including immovable property, digital service and digital content, as well as rights and obligations

Consumer -> any natural person who is acting for purposes which are outside his trade, business, craft or profession
Professional diligence -> is the standard of special skill and care which a trader may reasonably be expected to exercise towards consumers, commensurate with honest market

practise and/or the general principle of good faith in the trader's field of activity

To materially distort the economic behaviour of consumers means using a commercial practise to appreciably impair the consumer's ability to make an informed decision, thereby causing the consumer to take a transactional decision that he would not have taken otherwise.

According to the EU Court of Justice, the average consumer is a consumer who is *reasonably well-informed* and reasonably observant and circumspect, taking into account social, cultural and linguistic factors, **but** taking into account particularly vulnerable consumers (see below). The average consumer test is not a statistical test. National courts and authorities will have to exercise their own faculty of judgement, having regard to the case-law of the Court of Justice, to determine the typical reaction of the average consumer in a given case.

To summarise, the B2C Directive on unfair commercial practices governs both misleading and aggressive marketing strategies in consumer-facing transactions. Its scope is deliberately broad, extending beyond traditional advertising to encompass any *act, omission, conduct, or communication*, whether commercial, promotional, or representational, *that may influence consumer behavior*. This includes, but is not limited to, advertising and marketing activities. The directive applies exclusively to relationships between *traders* and *consumers*. A trader is defined as any natural or legal person acting for purposes related to their trade, business, or profession, including representatives acting on their behalf. A consumer, conversely, is an individual who engages with goods or services outside of a professional context, playing a passive role in the market. The directive also adopts an expansive understanding of "product," covering physical goods, services, digital content, and associated rights and obligations. At the core of the directive is the prohibition of unfair commercial practices, which are categorised into *misleading* and *aggressive* practices. Misleading practices are those that violate standards of professional diligence and are likely to *materially distort the economic behavior* of the average consumer. This means influencing a consumer's decision to act in a way they would not have otherwise, such as persuading them to purchase a product under false pretences. This kind of manipulation undermines consumer autonomy and, more broadly, the integrity of the market. Importantly, the directive *does not require actual harm to occu*r in order for enforcement to take place; it is sufficient that the practice is *likely to cause economic distortion*. This preemptive approach reflects the principle that a well-functioning market depends on the circulation of accurate and honest information, enabling consumers to make informed choices. The figure of the "average consumer" is a theoretical construct based on a reasoned understanding of typical consumer behavior within a given market -> there is no fixed or singular definition. Ultimately, the directive seeks to protect consumer interests and ensure that market competition remains *fair and transparent* by holding traders accountable for deceptive or coercive commercial behavior.

Commercial practices which are likely to materially distort the economic behavior only of a clearly identifiable group of consumers who are particularly vulnerable to the practice or the underlying product because of their mental or physical infirmity, age or credulity in a way which the trader could reasonably be expected to foresee, shall be taken into account to determine the perspective of the average member of that group. However, this is without prejudice to any common and legitimate advertising that is clearly an exaggerated statement or a statement which is not meant to be taken literally, which are not to be considered as misleading.

In determining whether advertising is misleading, you must look at:

- *the content of the advertising (including any omission)* -> an omission of material information that causes or is likely to cause him to take a transactional decision that he would not have taken otherwise
- *The presentation of the advertising (i.e. the way this content is displayed)*
- *The combination of the two* -> this is what we call material information -> being the information that appreciably impair the buyers' ability to take informed decision, thereby pushing buyers to take decisions that they would not have taken otherwise.

And all of this according to either:

1. In B2C relationships (UCPD), the average consumer
2. In B2B relationships (M&CAD) the prospected buyer

According to the M&CAD, in determining whether advertising is misleading, all of its features shall be taken into account - in particular any information it contains concerning:

1. The *characteristics of goods or service*, such as their availability, nature, execution, composition, method and date of manufacture or provision, fitness for purpose, uses, quantity, specification, geographical or commercial origin or the results to be expected from their use, or the results and material features of tests or checks carried out on the goods or services
2. The *price or the manner in which the price is calculated*, and the conditions on which the goods are supplied or the services provided
3. The *nature, attributes and rights of the advertiser*, such as his identity and assets, his qualifications and ownership of industrial, commercial or intellectual property rights or his awards and distinctions.

As mentioned before, similar elements are considered also by the UCPD in determining whether advertising is an unfair commercial practise under its scope of application, the only additional element is the consumer's rights, including the right to replacement or reimbursement.

THE PROHIBITION – UCPD VS. M&CAD

UCPD - main misleading practices

In B2C relationships …

a commercial practice that

- contains false material information and that is, hence, untruthful or in any way, including overall presentation, deceives or is likely to **deceive** the average consumer; and

- causes or is likely to cause the average consumer to take a transactional decision that he would not have taken otherwise.

1. False information (also omission) - Not only content, but also presentation

2. Potential element matters

3. The economic impact matters

4. Differences

In B2B relationships …

any advertisement which, in any way, either in its wording or presentation,

- **deceives** or is likely to deceive the persons (natural or legal person) to whom it is addressed or whom it reaches; and

- by reason of its deceptive nature, is likely to affect their economic behavior, and/or is likely to injure a competitor.

-Displaying a quality mark or equivalent without the necessary authorisation

- Claiming that a trader/ a product was approved by a public or private body when he/it is not
- Making an invitation to purchase products at a specified price and then: refusing to show the advertised item to consumers or refusing to take orders for it or deliver it with a reasonable time or demonstrating a defective sample of it, with the intention of promoting a different product (fishing)
- Falsely stating that a product will only be available for a very limited time (or that it will be available on particular terms for a very limited time) so to introduce an immediate decision
- Presenting rights given to consumers in law as distinctive features of the trader's offer
- Promoting a product similar to a product made by a particular manufacturer so to deliberately to mislead the consumer into believing that the product is made by that manufacturer
- Using editorial content in the media to promote a product where a trader has paid for the promotion without making that clear in the content (advertorial)
- Providing search results in response to a consumer's online search query without clearly disclosing any paid advertisement or payment specifically for achieving higher ranking of products within the search results (lack of transparency)
- Stating that reviews of a product are submitted by consumers who have actually used or purchased the product without checking that they originate from such consumers
- Submitting or commissioning another person to submit false consumer reviews
- Describing a product as "gratis", "free", "without charge" or similar if it is not.

SOME EXAMPLES

«***Book now***

Book by midnight on Monday. Travel in April. One way fare starting from EUR 10.
Subject to terms and conditions»

Think as you were in the marketing team of this travel agency

QUESTIONS ARE:
1. Are you giving the material information needed?
2. Is the information written in small fonts enough?

The answer to the above questions is **NO!!!**

You cannot provide misleading information about the **total amount which has to be paid** or misleading advertising of **"free" offers that are not so.**

Terms and conditions without specifying what they are is not a clear message. On the contrary, it is misleading and lacks of fundamental information for the consumers - it represents an omission of material information likely to influence the decision of an average consumer.

SOME EXAMPLES

(*): «*compared to the average of the most sold classic chips. The comparative table is available at www.sancarlo.it*».

QUESTIONS ARE:

1. Is the information re -30% of fats enough?
2. It this information presented in a correct way?
3. Is this advertising misleading or not?

The famous Italian producer of chips was sanctioned by the Italian Competition Authority (the AGCM) – which in Italy is entrusted with the power of forbidding unlawful advertising – for using suggestive words, such as "**Light**", attributing to the chips nutritional characteristics that were imprecise and also based on an unclear comparison without specifying the names

The producer then changed the message contained in the packaging, tv spots, web and other kind of advertising.

In this new version, the explanation is right next to the claim and the comparative table is more precise.

SOME EXAMPLES

The claim: «*With 4 GB of memory, expandable up to 32 GB, to accommodate applications, music, photos, videos and documents in quantity*»

A ONE MILLION EURO FINE AGAINST SAMSUNG ITALY FOR "MISLEADING INFORMATION" ON THE MEMORY OF SMARTPHONES E TABLETS

Samsung has been sanctioned by Italian Competition Authority (the AGCM) for providing misleading information on the memory of its smartphones and tablets.

The AGCM has judged this practice to be «*in conflict with due professional diligence, through the dissemination of misleading information and the omission of significant information, thereby substantially distorting the economic behaviour of the average consumer*».

Indeed, the real available capacity was significantly lower than the one indicated in the advertisements.

To determine whether an advertising claim is misleading, you must consider both the *content of the message and the way that content is presented*. Misleading advertising arises when the combination of these elements creates a *false impression* that could materially influence the behavior of the average consumer or buyer. This means that the information conveyed, or omitted, must be capable of altering a consumer's economic decision, like whether to purchase a product or not. Material information refers to *any detail that could significantly impact a purchasing decision*. This includes aspects like price, key features of the product, the reputation of the seller, or the rights that come with the purchase (such as return policies). Not disclosing relevant details, or presenting them in a way that downplays their significance, can be just as misleading as providing false information. In business-to-consumer (B2C) scenarios, the standard is based on how the *average consumer would react*. In business-to-business (B2B) settings, the focus is on the *prospective buyer*, typically a trader or professional. Despite the different target audiences, the principle remains the same: whether the ad causes or is likely to cause a decision that would not have been made if the consumer or buyer had the full, truthful picture. Examples of misleading practices include claiming that a product carries a quality certification without authorisation, suggesting that a trader has been approved by an authority when they haven't, or

advertising a product at a specific price without actually making it available. It is also misleading to falsely create urgency, such as pretending a deal is only valid for a short time, or to present legally required consumer rights as special features of the seller's offer. Further examples involve using editorial content or influencer posts to promote products without clearly disclosing that the content is paid, prioritising search results based on payment without informing the consumer, or displaying consumer reviews that haven't been verified. Claiming that something is "free" when it actually involves a cost is also deceptive.
A common case is airline ads promoting fares like "€10 – Book Now," with the real conditions only revealed in fine print. Even if the terms are technically present, the overall presentation may still mislead consumers. What matters is the *first impression* and whether that impression reasonably leads someone to take an action they wouldn't have taken otherwise.
Another example involves a bag of chips labeled "50% less fat," where the comparison is vague and only explained via a footnote referring to an external website. The average consumer may not understand or access the benchmark, making the claim misleading despite the inclusion of the fine print.
In all cases, the underlying rule is that consumers must be given *clear, upfront, and honest information*. Misleading practices undermine trust and can be punishable even if no harm has yet occurred. The law is concerned with *preventing negative economic impact by ensuring transparency*. It is not enough to provide correct information somewhere in the ad, it must be presented in a way that the average person can understand at first glance.
Another case involved Samsung, which advertised a phone with "4GB memory, expandable to 32GB," suggesting this space was fully usable for apps, music, and photos. In reality, that was misleading, and Samsung was fined €1 million by the Italian competition authority for providing incorrect and incomplete information that could mislead the average consumer. Another example focused on misleading promotions such as limited-time offers on products (e.g., 70% off boots). Questions were raised about when such offers become misleading—for instance, if the same offer is repeated frequently, if the advertised product quickly runs out without notice, or if essential details like available sizes and colors are not disclosed. The general rule is that *failing to inform consumers of such limitations may amount to omitting material information*, especially if it influences a consumer's decision.

Fishing -> an advertisement which creates the impression that the consumers is getting a personal message. In practise, the consumer gets an invitation to purchase goods or services at a specified price and then it is distracted/attracted to another good or service, with the intention of promoting such different product. Fishing constitute a misleading practise under the UCPD. An example of Fishing could be a case that took place in the Netherlands where teenagers received fake Valentine's Day texts that tricked them into entering personal data and unknowingly signing a contract. This was considered deceptive and exploitative, especially since it targeted emotionally vulnerable, underage individuals.

Case Mondadori – Philips – Unifarm

- Article on Belen Rodriguez's maternity published in the Italian magazine "***Chi***".
- The article includes two images: one about a specific kind of powdered milk and another one about a sippy cup.
- In addition, there are some products' descriptions. They say: ***«powdered milk enriched with natural Bifidus, which helps to maintain a robust and healthy digestion»***; the sippy cup is ***«made with Polietersulfone for toddlers, minimizes the amount of air which is breathed and avoids colics and irritability»***.

QUESTIONS ARE:

1. Is this advertising?
2. Is this lawful?

The article is to be intended as an advertisement, since it contains two separate photos of products which have no connection with the article itself.

This phenomenon is called **Editorial advertising or «Advertorial».** This is commonly an unfair commercial practice has it uses editorial content in the media to promote a product where a trader has paid for the promotion without making that clear in the content.

24

Hidden advertising / lack of transparency -> there is an increase in so-called hidden advertising. This is made especially in the form of product reviews written by employees of the producer of the reviews product or appraisals of products in blogs or via YouTube by people who *seem to be consumers but are paid by the producer to do so* (so-called "viral" and "buzz" advertising). It seems that this kind of hidden advertising is very difficult to detect. Even if, for example, a product review looks suspicious, it will be very difficult that the reviewer was paid by a business to write the review. A particular kind of hidden advertising has bemuse particularly common in the recent years with the raise of bloggers and influencers and the spread of so called "*influencer marketing*" -> Cases were presented in which celebrities and influencers appeared in magazine articles or social media posts promoting products, but it was later revealed they were paid for those appearances. Some cases include influencers promoting fashion collections *without disclosing sponsorships*. These are considered illegal hidden advertisements because they exploit consumer trust in editorial or personal content. In response, Italy implemented specific influencer guidelines (updated in 2024) requiring clear labels like "#ad" or "provided by brand" when content is sponsored. While these rules apply more strictly to popular influencers (with over 1 million followers), the general directive applies to *all* influencers—*transparency is always mandatory regardless of audience size*.

Influencer marketing -> it is a recent phenomenon involving influential web personalities, also known as bloggers or influencers sharing photos, videos and comments on blogs and social media platforms (like Facebook, Instagram, TikTok or Twitter) to show support or approval for specific brands, thereby creating an advertising effect. The Italian Competition Authority (AGCM) sent letters of "**moral suasion**", emphasising that advertising should be unmistakably identified as such and offering general guidelines for conduct. Testimonials should:

- *Ensure the promotional intent is evident by using indicators like hashtags #advertising, #ad, #sponsored*
- *Incorporate the sentence: "Product provided by: ___ " along with the name of the sponsoring brand into posts.*

Brands engaging these testimonials / sponsors are required to ensure clear warnings are included regarding the promotional nature of the content shared across social media platforms.
In turn, the Italian Advertising Self-Regulatory Institute focused on influencer marketing, aiming to ensure that promotional messages shared online via posts, Instagram stories and videos were clearly identifiable as such. As a consequence, it modified the "*Digital Chart Regulation on Recognising Commercial Communication on the Internet*", commonly referred to as the "**Digital Chart** (2016)", on the rules for online commercial communication. The Digital Chart issued by the Italian Advertising Self-Regulatory Institute in 2016 has so far represented the main tool of the Institute in fighting non-transparent digital marketing communications. The Digital Chart was just a set of guidelines and recommendations to ensure a transparent digital marketing communication. If influencers are endorsing products or services for commercial purposes, it's necessary to disclose it.

For posts -> in the beginning of the post, make it clear with one of these phrases: "Advertisement", "Promoted by... brand", "Sponsored by... brand", "In partnership with... brand", and/or. In the first three hashtags, ensure one of these phrases is included for immediate recognition: #Advertisement, #Sponsored by... brand, #ad paired with #brand.

For Stories and the like -> If the content at hand has a limited lifespan, like Stories, one of these statements must be clearly overlaid on the visual elements of each promotional piece.

When a company sends a product to an influencer for inclusion in their online post, two things are necessary:

1. *the influencer should accompany the message with the statement "product provided by ... brand", or similar*
2. *the company must inform the influencer of this requirement.*

We apply these guidelines to influencers providing content in Italian or content explicitly aimed at users in the Italian territory. An influencer is someone who meets the following cumulative criteria:

1. He/she provides a service constituting and economic activity, involving the provision of content, created or selected by him/her, that inform, entertain or educate and is capable of generating income either directly through commercial agreements with producers of goods and services or indirectly through monetisation agreement applied by the platform or social media used
2. He/she holds editorial responsibility over the content, meaning effective control over their creation/selection/organisation

3. The service offered is accessible to the general public via social media or other video-sharing platform services

Additionally, in order for these guidelines to apply to influencers the following criteria should be met. The influencer shall:

1. Have combined follower count of at least one million across all their platforms and social media channels
2. Have posted a minimum of 24 pieces of content in the preceding year
3. Have maintained an average engagement rate of 2% or higher over the last 6 months on at least one platform or social media channel

According to the Guidelines, influencers' content must comply with the following 7 rules:

1. **Crime prevention** -> Content must not contain any instigations or provocations to commit crimes or glorify them. It should not convey messages that absolve the author or hold the victim responsible for violence, hatred, discrimination, or any form of secondary victimisation.
2. **Respect for Human Dignity** -> Content must avoid expressions that could spread, incite, propagate, justify, minimise, or legitimise violence, hatred, or discrimination, and must not offend the human dignity of any group or individual.
3. **Protection of Minors** -> Content must not harm the physical, psychological, or moral development of minors.
4. **Tobacco – alcohol – medicines – gambling** -> Any form of commercial communication for cigarettes and other tobacco or nicotine-based products, alcoholic beverages aimed specifically at minors, prescription medicines, and gambling is strictly prohibited.
5. **Sponsorships** -> Sponsored content must be clearly recognisable, displaying the sponsor's name, logo, or other distinguishing marks at the start or end of the program. It should not promote the purchase or use of the sponsor's or any third-party products or services, especially through explicit promotional references.
6. **Product Placement** -> Followers must be made aware of any product placements with clear identification. Placement of cigarettes and other tobacco or nicotine-based products, specific medicines, or medical treatments available only by prescription within Italian territory is not allowed.
7. **Hidden advertising is strictly prohibited** -> Subliminal techniques must be avoided in both informational or entertainment content creation and commercial communications.

It is mandatory to adhere to the rules governing commercial communication disseminated through the internet, covering aspects such as *recognisability, endorsements, videos, event invitations, user-generated content, editorial content, sponsored search results, recommended content, apps featuring advertising content, and promotional games*. If the guidelines are violated, administrative fines apply:

- from €10.000 to €250.000 for beaches of advertising transparency rules
- from €30.000 to €600.000 for breaches concerning the protection of fundamental rights.

The rules and penalties applicable to unfair commercial practices are always preserved.
Lastly, we can explain the Chiara Ferragni *Pandoro* case. Ferragni promoted a branded Pandoro suggesting the higher price would go to a children's charity. However, investigations showed she neither donated her own profits nor ensured that the markup went to the charity. Only a modest, unrelated donation had been made by the manufacturer. The Italian Competition Authority ruled this campaign was misleading, especially as internal emails revealed Ferragni's legal team had warned her that the claims could be deceptive—yet she continued with the campaign. This was seen as a serious breach of consumer trust. The Italian Competition Authority (AGCM) sanctioned companies linked to Chiara Ferragni and Balocco for unfair commercial practice. The advertising and the posts were inducing the consumers to believe that by purchasing the Balocco's Pandoro and so joining the Pandoro Pink Christmas campaign, they would have contributed to the collection of funds necessary to the financing of the equipment for the hospital. In fact, the donation, amounting to €50,000, had instead already been made by Balocco alone months earlier. Also, that was not proportional to sales of Balocco Pandoros during the Christmas campaign.
Aggressive advertising -> is part of the unfair commercial practices -> A commercial practice shall be regarded as aggressive if, in its factual context, taking account of all its features and circumstances, by *harassment, coercion, including the use of physical force, or undue influence*, it significantly impairs or is likely to significantly impair the average consumer's freedom of choice or conduct and thereby *causes him or is likely to cause him to take a transactional decision that he would not have taken otherwise*. There are 3 main elements to take into consideration:

1. The aggressive element
2. Potential element matters
3. The economic impact matters

Consumers should never be compelled to make decisions they would not have otherwise taken freely. This principle underpins the concept of *aggressive advertising*, which goes beyond misleading advertising by focusing on the moment of decision-making and assessing whether the consumer was *subjected to undue influence, including forms of coercion or even violence*. Such practices are pursued legally even in the absence of actual harm, as the intent is to prevent potential harm and uphold strict standards.
Three critical elements define oppressive advertising:

1. **Economic impact**, which justifies regulatory attention to advertising;
2. **The aggressive component**, distinguishing it from misleading advertising that primarily involves false or incorrect information;
3. **Potential harm**, whereby enforcement is triggered even before actual harm occurs.

In evaluating whether harassment, undue influence, or coercion has occurred, authorities consider various contextual factors—timing, location, persistence of communication, use of threatening or abusive language, and the exploitation of a consumer's vulnerabilities or misfortunes.
Illustrative examples include aggressive sales tactics such as repeated unsolicited phone calls or manipulating consumers' emotions by implying they lack the knowledge to make sound financial

decisions. The use of intimidation, condescension, or legal threats to deter contract termination also falls under this category. Fundamentally, aggressive advertising exploits *information asymmetries and aims to override consumer autonomy through pressure, manipulation, or fear.* Aggressive adv includes creating complex procedures to exit contracts, threatening legal action, or emotionally manipulating consumers, for example, by telling them that not buying a product could cost the salesperson their job. Businesses may also use tactics like entering a consumer's home and refusing to leave, requiring unreasonable documentation for insurance claims, or targeting children in advertising to pressure parents indirectly.

In determining whether a commercial practise uses harassment, coercion, including the use of physical force, or undue influence, account shall be taken of:

1. *Its timing, location, nature or persistence*
2. *The use of threatening or abusive language or behaviour*
3. *The exploitation by the trader of any specific misfortune or circumstance of such gravity as to impair the consumer's judgement, of which the trader is aware, to influence the consumer's decision with regard to the product*
4. *Any onerous or disproportionate non-contractual barriers imposed by the trader where a consumer wishes to exercise rights under the contract, including rights to terminate a contract or to switch to another product or another trader*
5. *Any threat to take any action that cannot legally be taken*

In other words, a behaviour which takes advantage of a weakness or a difficult situation of the consumer

The main aggressive practices comprehend:

- Creating the impression that the consumer cannot leave the premises until a contract is formed
- Conducting personal visits to the consumer's home ignoring the consumer's request to leave or not to return except in circumstances and to the extent justified, under national law, to enforce a contractual obligation
- Making persistent and unwanted solicitations by telephone, fax, e-mail or other remote media except in circumstances and to the extent justified under national law, to enforce a contractual obligation
- Requiring a consumer who wishes to claim on an insurance policy to produce documents which could not reasonably be considered relevant as to whether the claim was valid, or failing systematically to respond to pertinent correspondence, in order to dissuade a consumer fro exercising his contractual rights
- Including in an advertisement a direct exhortation to children to buy advertised products or persuade their parents or other adults to buy advertised products for them
- Explicitly informing a consumer that if he does not buy the product or service, the trader's job or livelihood will be in jeopardy

- Creating the false impression hat the consumer has already won, will win, or will on doing a particular act win, a prize or other equivalent benefit, when in fact either there is no prize or other equivalent benefit, or taking any action in relation to claiming the prize or other equivalent benefit is subject to the consumer paying money or incurring a cost.

One case study focuses on TikTok and the so-called “French scar” challenge, which encouraged teenagers to harm themselves. This content spread widely on the platform, prompting outrage from parents who questioned why TikTok didn’t prevent it. At that time, *Italian law had no clear rules on platform content moderation*. However, TikTok had publicly stated in its guidelines that it was a safe platform for minors. The Italian Competition Authority argued that these claims amounted to *misleading advertising*. TikTok, by claiming to ensure safety while allowing harmful content, failed to act with the necessary diligence. TikTok’s defence was that it *wasn’t a trader since users don’t pay for access*. The authority rejected this, stating that users "pay" with their attention and personal data, creating an economic relationship. TikTok also claimed that content was user-generated and protected by *free speech*. Nonetheless, because TikTok had committed to safety through its public guidelines, it was held accountable for not living up to that promise. Additionally, the authority found TikTok’s *recommendation algorithm to be aggressive*. Once a user viewed harmful content, the algorithm pushed similar content, reinforcing exposure. Even though this wasn’t a person intentionally being aggressive, the *system’s design had aggressive effects*. The ruling emphasised that aggression in this context doesn’t require intent; repeated harmful promotion is enough. As a result, TikTok was required to change its recommendation system in Italy for underage users. Now, when minors log in, they must choose between a *profiling-based recommendation system or a general one*, giving them (or their guardians) more control.

THE FRENCH SCAR CHALLENGE CASE

The following video became viral on TikTok - so called “French Scar Challenge”:

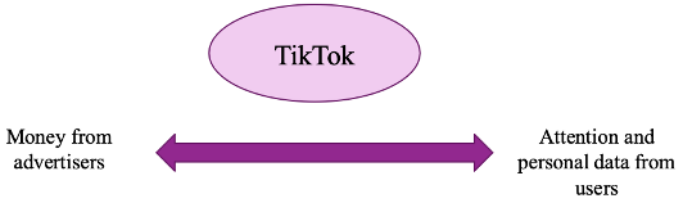
TIKTOK ACCUSATION

According to the accusation, TikTok has:
- disseminated content capable of threatening the psycho-physical safety of children and adolescents
- violated the obligation of diligently applying its own Guidelines: Linee guida della community | TikTok
- put in practice insufficient control and monitoring measures
- unduly conditioned users by reproducing content that exploits the vulnerability of certain consumer groups;

TIKTOK DEFENCE ARGUMENTS

TikTok has replied that:
- there is no economic behavior at hand, no economic relationship;
- users uploaded that content themselves with no responsibility of TikTok;
- it has done its best to delete dangerous contents.

THE ECONOMIC RELATIONSHIP



If TikTok hadn't laid out those guidelines, it could have *avoided its accountability*. By pledging a safe environment to its users, TikTok took on that responsibility. TikTok's "*automated review*" of contents did not prevent the spread of the mentioned videos on the platform. According to TikTok, the "French scar challenge" would not fall under the category of "self-harm," which only includes physical injuries qualifying as such from a legal standpoint. TikTok decided to take moderation measures for videos related to the French scar only after they gained media attention. These measures *did not result in content removal but were only limited their dissemination*, focusing only on some videos selected by TikTok or reported by users. Therefore, from the gathered evidence, gaps in the tools used for content monitoring also emerged, limiting the effectiveness of the moderation process outlined in the Guidelines. Algorithmic profiling-based recommendation system resulted in an undue conditioning of the consumers. It is not sufficient for TikTok to provide:

- users with ways to partially opt-out of the recommendation system
- the possibility of employing an alternative "recommendation system" not based on profiling.

This is due to:

- the manner in which this alternative was introduced and proposed to consumers
- the fact that users are not informed of the existence and effects of this option, as there is no indication of this new possibility and its implications
- the fact that users can only exercise this alternative option through specific active behavior.

In the end, TikTok was sanctioned for aggressive practice by the Italian Competition Authority (AGCM) -> The company has *failed to implement appropriate mechanisms to monitor content published on the platform*, particularly those that may threaten the safety of minors and vulnerable individuals. Moreover, this content is systematically re-proposed to users as a result of their algorithmic profiling, stimulating an ever-increasing use of the social network.

ANOTHER EXAMPLE – SAMSUNG CASE

The Italian Competition Authority (AGCM) sanctioned SAMSUNG on the methods of advertising and managing several promotional events characterised by the promise of assignment of products and/or rebates in case of purchase of the advertised goods.

The Authority identified a first misleading and aggressive commercial practice, considering that the advertising messages did not clearly show essential information, as the information regarding the nature of the promotion, the restrictions, conditions and modalities to obtain the promised prize/benefit and that the participation procedures were particularly burdensome.

With regard to **aggression**:

- ✓ the procedures adopted were such as to hinder consumers in the request and in obtaining the promised prize/benefit, as a set of, sometimes repetitive fulfilments were imposed, to be met within a short time;
- ✓ in some cases, customers were repeatedly asked to provide additional documentation (vendor's declarations, original receipts and labels);
- ✓ moreover, without an internet connection (or appropriate tools such as smartphones or pc) and/or a sufficient level of computer literacy, the customer could not be able to achieve all the intended steps.

The Authority also found aggressive the commercial practice linked to the collection of their customer personal data for marketing purposes.

Specifically, the consumer, who had purchased the promoted product in order to obtain a prize/rebate/gift, could not avoid to:

(1) subscribe to the Samsung People platform; and
(2) provide a series of personal information that fell beyond the prize-competition itself and the scope of consent to data processing for marketing purposes as well.

There are private ordering rules (i.e. rules of the national associations of advertisers) forbidding discriminatory claims. We focus on discriminatory advertising, particularly the sexualization of women in ads. Even though the law doesn't directly address this, advertising associations in Europe have developed *ethical codes* that forbid violent, racist, or sexist messaging. Violating these codes doesn't lead to public sanctions, but it can hurt a company's reputation within the industry. For example, it's possible to find an ad where a boy, after drinking an energy drink, becomes a hardworking student, while a girl becomes a princess -> reinforcing gender stereotypes. These examples show that despite progress, advertising still struggles with outdated and offensive portrayals.

Comparative advertising -> we are in B2B relationships and comparative advertising is an important instrument if you're involved with a company's marketing, especially if that company has one pr more key competitors -> it's a marketing strategy. Comparative advertising is a promotion strategy where differences between a business and its direct competitors are identified to persuade customers to try a certain product. Comparative advertisements emphasise how your company's products and services are better than similar ones available on the market. From a legal standpoint, comparative advertising is any advertising that explicitly or by implication identifies a competitor, or goods and services offered by a competitor -> it allows recognising the competition addressed via some features that usually identify the competition (its name, its trademarks, its slogan).
Indeed, in everyday life we acknowledge that comparative advertising is designed to *highlight the advantages of the goods or services offered by the advertiser as compared to those of a competitor*. In order to achieve this objective, the message of the advertisement must necessarily *underline the differences* between the goods or services compared by describing their main characteristics.

Comparative advertising may be virtuous and cause beneficial effects to the market:

1. *It enables advertisers to demonstrate the merits of their products* -> good for entrepreneurs
2. I*t improves market transparency and the quality of information available to consumers enabling them to make well-founded and more informed decisions relating to the choice between competing products/services* -> Good for consumers and for the whole society
3. *It can stimulate a fair competition between suppliers of goods and services to the consumer's advantage* -> Good for entrepreneurs

In the past, EU legislators use to believe that to make comparisons between competitors was unfair, mainly because to signal competitors' faults, even indirectly, was deemed to be unjust. Even nowadays, when comparative advertising is admitted, EU legislators forbid evocative comparative advertising -> comparative advertising cannot try to influence consumers via beautiful images on behalf of one competitor but in detriment of the other one -> it has to be

strictly objective, it cannot try to exploit psychological mechanisms, it has to be almost "scientific" meaning:

- it has to confirm objective facts
- It has to be specific

In EU comparative advertising is allowed if the following requirements are all met:

1. *It objectively compares one or more material, relevant, representative and verifiable features of those goods* -> comparative advertising cannot be evocative
2. *It compares goods or services meeting the same needs, intended for the same purpose, or share the same geographical origin*-> comparative advertising cannot be evocative
3. *It is not misleading* -> as for any other kind of advertising
4. *It does not create confusion among traders, between the advertiser and a competitor or between the advertiser's trademarks, trade names, or distinguishing marks, goods or services and those of a competitor* -> as for any other kind of advertising
5. *It does not discredit or denigrate the trademarks, trade names, or other distinguishing marks, goods, services, activities, or circumstances of a competition* -> it cannot imply denigration
6. *It does not take unfair advantage of the reputation of a trademark, trade name or other distinguishing marks of a competitor or of the designation of origin of competing products* -> it cannot promote free riding
7. *It does not present goods or services as imitations or replicas of goods or services bearing a protected trademark or trade name* -> it cannot promote free riding

(*): «*compared to the average of the most sold classic chips. The comparative table is available at www.sancarlo.it*».

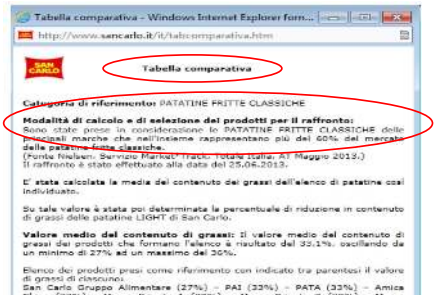
The famous Italian producer of chips was sanctioned by the Italian Competition Authority (the AGCM) for using suggestive words, such as **Light**, attributing to the chips nutritional characteristics that were imprecise and also based on an unclear comparison without specifying the names of the other producers used to make the comparison.

LET'S FOCUS ON THAT…

Comparative Table

Calculation and selection method of products to make the comparison:

«*Classic chips of the main brands together representing more than 60%*



The long-time rivalry between Pepsi and Coca-Cola, known as the "Cola Wars" is one of the most fascinating case studies in the history of marketing.

They have engaged in mutually-targeted marketing campaigns for the direct competition between each company's product lines - Bing Videos

Pepsi challenge/Pepsi Now! Commercial - 1983

In 1975, Pepsi launched the Pepsi Challenge, in which people were asked which cola they preferred in blind taste tests.
The campaign suggested that consumers preferred Pepsi over Coca-Cola based solely on taste.
The Pepsi Challenge was more than a marketing campaign; it was a cultural phenomenon that made choosing a cola with an exciting and interactive experience.
This was considered a crucial moment for the history of marketing.

Overall, we focused on comparative advertising, defined as marketing that explicitly or implicitly *compares one product to another*. In the EU, such advertising is allowed but tightly regulated. Its primary benefit is *enhancing consumer choice by providing clear, factual comparisons, thus fostering competition*. However, many European businesses, influenced by a historical culture of cooperative entrepreneurship (like medieval guilds), are cautious about comparative advertising. They view direct comparison as *potentially unfair or damaging to reputations*, especially if it appears to mock or discredit competitors. Under EU law, comparative advertising must meet several strict criteria: it must be *objective, based on verifiable facts, non-misleading, and not discredit the competitor or cause consumer confusion*. The comparison must concern products that serve the same purpose and come from the same geographical market. Importantly, advertisements must *not use emotional appeal, famous personalities, or suggest superiority through implication* (such as portraying one actor as more attractive or "cool" than another). There are several U.S. examples, such as the Apple vs. PC and Samsung vs. iPhone campaigns, that are unlawful under EU law. These often rely on humor, stereotype, or personal appeal rather than factual, objective comparison. For instance, using a famous, stylish actor to represent Apple and a plain character to represent PC subtly conveys superiority not based on features but on *status and identity*. Under EU standards, this constitutes unfair advertising. Moreover, we focused on a cross-border issues, such as whether a U.S. ad broadcasted on YouTube could be challenged under EU law. Theoretically, platforms could be *required to remove content that violates EU advertising standards, just as they are obliged to take down illegal or harmful materials*. However, enforcement in digital spaces remains complex and evolving. Overall, the EU model prioritises *consumer protection and market fairness* over creative freedom or aggressive marketing tactics.

Behavioural advertising -> is a form of interactive media adverting, together with the contextual advertising and the segmented advertising.
Contextual advertising ->is typical of search engines and derives from the search keywords, the previous search query, or the user's IP address indicating its likely geographical location.
Segmented advertising -> is typical of websites of registered users. It selects the adv on the basis of an ex-ante profiling, i.e. on known characteristics of the data subject (age, sex, location, etc.), which the data subject has provided to the website at the sign -up or registration stage.

Overall, Behavioural advertising is a sophisticated form of *web-based, interactive advertising* that relies on *user profiling*. It involves the ongoing, real-time collection of personal data across various websites, enabling advertisers to *tailor advertisements to individual users* based on their online activity. This goes beyond segmented or contextual advertising, as it aggregates data from multiple sources to create highly personalised marketing content for users each time they browse the internet. From a legal standpoint, the primary concern with behavioural advertising is its *use of personal data*. This raises questions regarding the lawfulness of such practices under data protection and privacy regulations. Although highly effective from a commercial perspective,

allowing advertisers to efficiently reach their target audience, behavioural advertising also carries risks, such as *potential violations of privacy, aggressive marketing tactics, and the manipulation of consumer behaviour*.

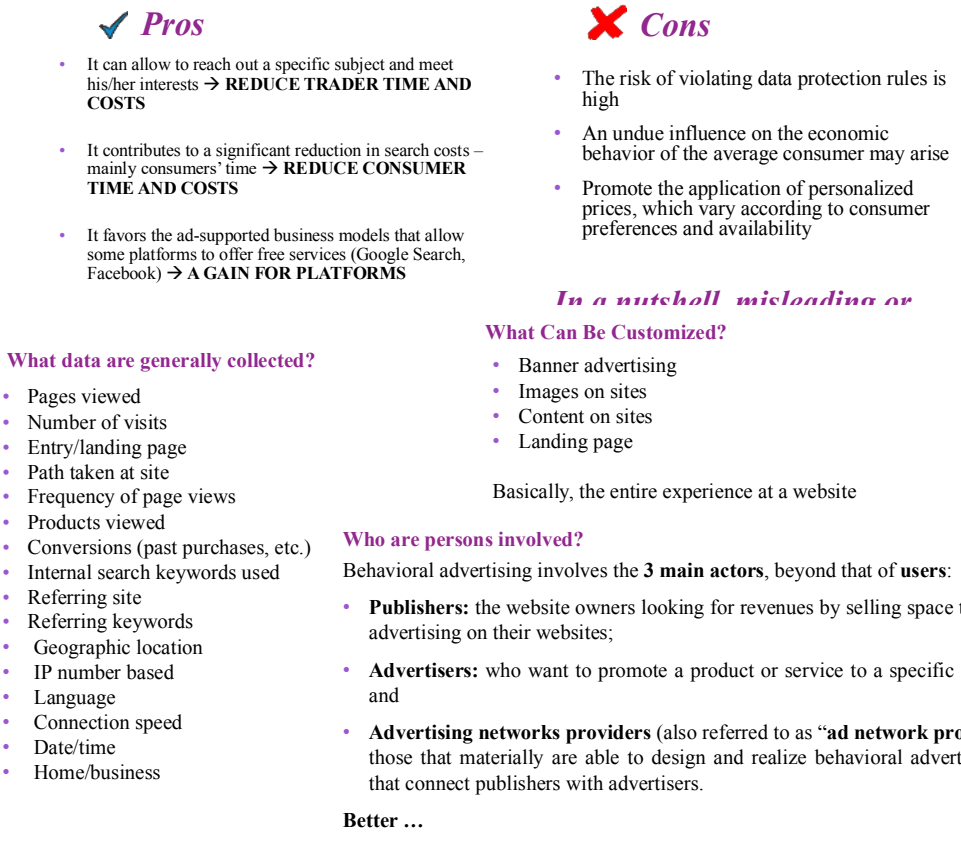
Behavioral advertising is based on very detailed descriptions of individuals' online life, with many of the websites and specific pages they have viewed, how long they viewed certain articles or items, in which order, etc. behavioural advertising entails:

- *The tracking of users' internet habits while they surf on the internet*
- *The building of profiles over time*
- *The use of these profiles to provide internet users with advertisement that match their interests*

Hence behavioural advertising requires:

- *Basic internet technology* allowing "advertising network providers" to track data subjects (i.e. individuals) across different websites and over time
- *Gathering and collecting information regarding these data subjects*

Behavioral adv is "*dynamic*" (not static) and it is based on day-by habits of the users. It is a very sophisticated and powerful instrument. Dynamic pricing adjusts prices in real time based on demand and supply (e.g., Uber fares), a practice generally accepted in economics. Personalised pricing, however, sets different prices for the same product based on individual consumer profiles, such as income, age, or purchasing behaviour, often enabled through data collected for behavioural advertising. While personalised pricing can be beneficial for companies in terms of profit maximisation, it raises ethical concerns from a consumer standpoint due to potential unfairness and price discrimination. The discussion invites critical reflection on whether such practices should be restricted, given their implications for consumer rights and market transparency.



Advertising network exist to aggregate and match the demand of advertisements coming from advertising to the supply of advertising space coming from publishers. The peculiarity of behavioural advertising is that this matching is done on the basis of individuals profiles, which indeed are created by advertising networks via specific *software and technologies*. Generally advertising network use a *central advertising server* for tracking data subjects, collecting and elaborating the material information, and selecting what specific advertisement can match the interests of individuals.
Basically, it happens that the publisher *reserves visual space* on its website to display an advertising and relinquishes the rest of the advertising process to one or more advertising network providers. The advertising network providers are responsible for *distributing advertisements to publishers with the maximum effect possible*. The advertising network that they govern is - i.e. the more numerous their clients are - the more sources of information they have t profile individuals' behaviours. The advertiser typically negotiates with one or more ad networks to sell their advertisements. A publisher may have *several contracts with different advertising networks*, for example by reserving different places on the website for different advertising networks. Advertiser may just ask ad networks to find places for their ads, *without knowing the identity of the publishers*. Typically, the ad network provider places a *tracking cookie* (i.e. small text files sent by a web server to web browsers, collecting information) on the terminal equipment of the internet users (that we can also call "Data subjects"), when they first access a website offering an advertisement of its network. In other words, once a user makes its first access to the network of websites that a specific Ad network controls, the individual is in!!! He starts being profiled Therefore, along time, these cookies associated to the equipment of the user will enable the ad network to *recognise him*, to see whether he uses or returns to any of the web sites of its network. Such repeated visits will enable the ad network provider to build a profile of the visitor. Because these tracking cookies are placed by a third party that is distinct from the web server that displays the main content of the webpage (i.e. the publisher) they are often referred to as "*third party cookies*".

In addition to advertising networks, behavioural advertising might also be delivered through *onsite advertisement.* With this method, the advertiser indicated to the publisher its *intended audience target* based on criteria that may go beyond demographic information such as the traditional triplet of "age range, gender and country" to much more *precise criteria* (such as keywords or interests). The publisher then takes care of displaying the advertisement to the chosen target, implementing the targeting technology and controlling the ad placement and distribution. In this case, the publisher acts also as an advertising network. Onsite advertisement is, hence, a game of two. There is no advertising network… more precisely, the advertising network is the publisher. It is used in some social network platforms, such as Facebook, allowing users to be targeted through their interests.

According to article 5(3) of the E-privacy directive an advertising network provider who wishes to gain access to the information stored in a user's terminal equipment is allowed to do so if it has *obtained the user's informed consent to get such access*. Exempted cookies are:

- User input cookies (session-id), for the duration of a session of persistent cookies limited to a few hours in some cases
- Authentication cookies, used for authenticated services, for the duration of a session
- User centric security cookies, used to detect authentication abuses, for a limited persistent duration
- Multimedia content player session cookies, such as flash player cookies, for the duration of a session
- Load balancing session cookies, for the duration of session
- Customisation persistent cookies, for the duration of a session (or slightly more)
- Third party social plug-in content sharing cookies, for logged in members of a social network

Overall, taking about behavioural advertising, we refer to a sophisticated form of online advertising that relies on the *profiling of users* through data collected during their web activity. This advertising method aims to personalise content by analysing individual user behaviour, preferences, and characteristics. It falls under the broader category of **interactive advertising**, which includes *segmented, contextual, and behavioural formats*.

Behavioural advertising typically involves **three key actors**:

1. **Publisher** –> the owner of the webpage (e.g., *The New York Times*).
2. **Advertiser** –> the company that creates and promotes products or services.
3. **Advertising Network (Ad Network)** –> the intermediary that collects user data through cookies, profiles users, and facilitates the targeted placement of ads across various publishers' pages.

In some cases, such as Google, the publisher and the ad network are the *same entity*, creating a two-party model. From a *legal standpoint*, behavioural advertising raises important questions, particularly concerning *data protection* and *consumer rights:*

- *Consent* is a fundamental requirement under the *ePrivacy Directive*: cookies used for advertising purposes must be accepted explicitly by the user.
- *Technical cookies* (used to ensure website functionality) do not require consent, whereas *profiling cookies* (used for personalisation) do.
- Publishers and ad networks often include *contractual clauses to avoid liability for misleading or unlawful advertising*, placing responsibility on the advertising agencies that create the content.

Additionally, we discussed **personalised pricing**, where prices differ based on a consumer's individual profile. While it can allow access to goods for lower-income users, it raises fairness concerns. Legally, *personalised pricing is not prohibited* unless it results from violations of data protection regulations. Authorities have yet to challenge it under unfair competition or antitrust

law, though consumer advocates have expressed opposition. Furthermore, we discussed on the legitimacy of data-for-access models, where users must accept cookies (i.e., give up personal data) to access content. While this practice may be acceptable if clearly disclosed and alternatives are provided (such as payment via currency), it raises questions about *freely given consent and transparency*.

Sponsorship -> there is no legal definition of sponsorship -> Sponsorship is *not expressly regulated under civil law* but has developed through commercial practice over the past 30–40 years. It refers to a contractual relationship in which one party (the sponsor) provides financial or material support to another party (the sponsored) in exchange for the promotion of the sponsor's brand, image, or products -> we ought to have a look at what happens in business reality. There are 3 different types of sponsorships in the business reality. Sponsorship may be implemented in 2 different ways - either financing or paying a fee in connection with a particular event or a celebrity.
Suppose that a company wants to enhance its social reputation. It can establish a direct link between its name/activity/image and:

1. *A cultural or sportive event highly appreciated by the community*
2. *A great and famous event*
3. *A very famous person (testimonial)*

So, there are 3 primary types of sponsorship:

1. **Major Event Sponsorship**: Involves supporting large-scale, high-visibility events such as the Olympic Games or international concerts.
2. **Local or Cultural Sponsorship**: Targets smaller, community-based events like children's sports tournaments or the restoration of cultural heritage, aiming to build goodwill with local communities.
3. **Personal Sponsorship**: Involves individuals (testimonials) such as athletes or celebrities, whose image and public recognition are leveraged to promote a brand.

There are two different ways to make sponsorship:

1. *Financing* a particular event, usually a cultural or sport event, which has a positive impact on public
2. *Paying a fee* in connection with a particular event, usually a cultural or sport event or to a celebrity, which has a positive impact on public

A sponsorship agreement is the agreement whereby a party - the sponsor- obtains, in exchange for either money or other kinds of equipping, the right to establish an association between its name/activity/image/brand and either an event organised and managed by another party - the sponsee- or a famous person - the testimonial.

The sponsor will succeed in associating a high social value to its name/image/activity or increasing the celebrity of its brand -> brand recognition or reputation or affiliation with an event's goodwill or with a celebrity.
The organiser of the events, the sponsee, will succeed in obtaining either funds or material and tools (equipping) necessary to realise the event. In particular, sponsors are essential to the commercial success of large-scale events.
Conversely, such events provide sponsor with several advantages such as on-site signage, other on-field exposure, other promotional rights in the stadium or in arena including inventory on the billboard, audio mention, tickets, and other hospitality, control over the sale of media rights.

Both the sponsor and the sponsee have some obligations:
- *Sponsor* -> financing or payment of the agreed amount -> Provide financial or material support.
- *Sponsee* -> to be diligent (results are not required rather what is required is diligence) in performing the sponsored activity -> Promote the sponsor's image and reputation diligently.

Importantly, the obligation of the sponsored party is based on a "*best effort*" *standard* rather than guaranteed results. For example, a testimonial cannot be contractually required to win a competition or achieve specific outcomes but must avoid conduct that may damage the sponsor's reputation. Contracts often include *morality clauses* outlining unacceptable behaviours, such as involvement in scandals or drug use.
Generally, the main (written) clauses relate to the:
1. *Detailed description of the link to be realised between the sponsored product and the sponsee/testimonial*
2. *Behaviours that the sponsee cannot undertake and in connection with this … (also in his/her personal life)*
3. *Circumstances tat could either modify or interrupt the agreement*
4. *Amount of funds and other kinds of equipping*
5. *Duration* -> Typically short-term, often one year, with possibilities for renewal.
6. *Renewal*
7. *Exclusivity* -> Prevents the testimonial from representing competitors during and sometimes after the contract (cooling-off period).

Some examples of sponsorship in sports comprehend:
- *Luxury sports* (such as golf and sailing) are suitable for luxury products
- *Popular sports* (such as soccer and basketball) are suitable for commodities or base products
- At least at the beginning, *niche products have been associated to niche sport* (surfing)
- *Each sport can be associated with a particular producer or brand of the equipping of that sport*

WHAT CAN AFFECT THE AGREEMENT… LOOKING AT A REEBOK CONTRACT

«*Athlete acknowledges that Athlete's actions and behavior may affect the* ***value of the endorsement*** *(i.e. Athlete's name, any other intellectual property owned by or on behalf of Athlete; and all other identifiers or characteristics that identify Athlete in the mind of the public)* ***and agrees to use Athlete's best efforts to protect and maintain the value of the Endorsement***».

Best effort to mantain the value of the endorsement

«*During the Term, Athlete will* ***comply with the rules and regulations*** *of all governing bodies or other entities having jurisdiction over any sport or athletic activity in which Athlete participates and will behave in a sportsmanlike manner at all times. During the Term, Athlete* ***will not endorse, advertise or promote any weapons, alcoholic beverages or tobacco products***».

Reputational element - Atlete's obligation to have a good behavior - Not only acts, but also omissions

«*Reebok agrees that any Marketing Materials will present Athlete* ***in a positive manner and will not materially impair*** *the value of the Endorsement. Athlete shall have* ***the right to review and approve*** *all proposed Licensed Products as the same may utilize or incorporate the Endorsement or any part thereof*».

Reputational element - Sponsee's obligation to present the Atlete in a good way

21

For a sponsor, *exclusivity* is key. The value of an event sponsorship is often dependent on the scope of exclusivity. Generally, when a sponsor negotiate for exclusivity, it will ask for exclusive sponsorship in its product category. Defining such categories, however, is not always simple.
Sponsor -> the sponsor will want to define its category broadly, to exclude as many other sponsor as possible
Sponsee -> the sponsored entity, on the contrary, will want to define each sponsor's category as narrowly as possible, to avoid limiting itself with respect to other contracts.

Ambush marketing -> Ambush tactics are used when a *non-sponsor tries to associate itself with an event by using communication techniques that will lead consumers to believe the company acts as an official sponsor*. It is an effective weapon for companies seeking to associate themselves with international events, such as the Olympic games and the FIFA World Cups, without any official authorisations by event organisers, i.e. without paying any license or sponsorship fee. Thus, ambushers take *advantage of the media exposure* of events as well as of official sponsors' marketing efforts, but they sustain lower costs. In other words, ambush marketing offers a chance to capitalise on a global event's exposure without the big costs associated with extensive advertising -> Ambushers are basically free riders. This indirectly cause a prejudice to official sponsors, which finance the event or pay the relevant fees.

There are different types of ambush marketing:

1. **Insurgent ambush or ambush by intrusion** -> all those initiatives that are made by intrusion to a target event or near to it
2. **Saturation ambush** -> actions or initiatives that, without linking to the target event, are intended to prejudice its popularity or visibility, for example occupying in a significant manner

advertising spaces or arranging or sponsoring parallel or concurrent events so to distract the public attention from the target event

3. **Predatory ambush** -> intentional false claims to be the official sponsor or creation of an explicit link to a sign, trademark, logos or persons connected to the target event

Examples of insurgent ambush

- *1984 Los Angeles Olympic Games*, Kodak photo was the games' official sponsor. Fuji sponsored ABC network's broadcasting of the games. The huge majority of the US citizens watched the games on the ABC network. Kodak claimed that its monetary efforts were not as effective as they could have been.
- *1996 Atlanta Olympic Games*, one of the main sponsors of the competition, among sports companies, was Reebok who invested up to 60 million dollars mainly for wearing 3000 athletes, ad hoc campaigns emphasising the logo, and merchandising in stores spread all over the city. In particular, Reebok was the official sponsor of Linford Christie, Olympic gold medal sprinter. Linford Christie wear contact lenses with the Puma logo during the press conference for the athletes preceding the games. The stunt didn't sit too well with official sponsor Reebok, which had paid $40 million for the exclusive rights to the event
- *1992 Olympic Games* -> Sponsorship was used to fuel comparative advertising campaigns. For months, Visa International had been running TV spots advising American Express cardholders headed for the games at Albertville, France, to leave their cards home because "the Olympics don't take American Express", with images of ticket windows being slammed shut in the faces of American Express cardholders. Visa had paid $20 million for the rights to call itself an official exclusive sponsor and was, in fact, the only credit card accepted at the Games' on- site ticket window. Amex returned fire, launching a series of ambush marketing campaigns and responded pointing out in its own ad campaigns that "to visit Spain, you don't need a visa".

A key example cited is the 1984 Los Angeles Olympic Games, where Kodak, the official sponsor, faced an unexpected challenge from Fuji. Although Fuji was not an official sponsor, it secured *advertising slots on the ABC network*, which broadcast the Games. As a result, viewers associated Fuji with the event more strongly than Kodak, *undermining Kodak's investment*. This case illustrates the phenomenon known as "ambush marketing," where companies benefit from an event's visibility without formally sponsoring it. The lecture emphasises that while all involved contracts, between Kodak and the organisers, Fuji and ABC, were legal, there was a contractual loophole. This gap allowed Fuji to appear as a legitimate sponsor in the minds of consumers. The speaker suggests that Kodak could have *mitigated the issue by ensuring that the event organisers included clauses preventing broadcasters from accepting advertising from competitors*. The concept of *contractual incompleteness* is also discussed. It is impossible to anticipate and contractually prevent every potential form of ambush marketing. Various real-life examples are given, including a situation where an athlete, while under contract with one brand, wore visible contact lenses branded by a competitor, shifting public association to the latter. To address such

loopholes, Italy has introduced legal measures that *prohibit deceptive, misleading, or parasitic marketing practices in connection with large events*. These laws aim to protect the integrity of sponsorships by penalising entities that attempt to exploit event-related visibility without proper authorisation.

Looking at the Italian law on ambush marketing, there is a *lack of specific regulation until recently*. To avoid cases like the one just describes, on May 2020 the Italian Parliament enacted Law no.31/2020 which converted Law Decree no.16/2020. Urgent provisions for the organisation and holding of the Winter Olympic and Paralympic Games "Milano-Cortina 2026" and the ATP finals "Turin 2021-2025", as well as on the prohibition of ambush activities.

Prohibition of ambush marketing -> parasitic, fraudulent, deceptive or misleading advertising and marketing activities carried out in connection with the organisation of sporting events or trade fairs of national or international importance that are not authorised by the organisers and whose purpose is to gain an economic or competitive advantage are forbidden. There are 4 cases, all of which fall within the concept of "*parasitic advertising and marketing*":

1. The *creation of an even indirect connection between a trademark or other distinctive sign and one of the events* referred to in paragraph 1, which is capable of misleading the public as to the identity of the official sponsors
2. the *false representation or declaration in one's advertising that it is the official sponsor* of an event referred to in paragraph 1
3. the *promotion of one's own brand or other distinctive sign by means of any action, not authorised by the organiser*, which is suitable for attracting the attention of the public, carried out on the occasion of one of the events referred to in paragraph 1, and suitable for generating in the public the erroneous impression that the author of the conduct is the sponsor of the sporting or exhibition event in question
4. the *sale and advertising of products or services that are improperly marked, even only in part, with the logo of a sports or exhibition event* referred to in paragraph 1 or with other distinctive signs likely to mislead the public about the logo and to create the erroneous perception of any connection with the event or with its organiser or with the parties authorised by it.

The prohibition *does not apply to the conduct carried out in execution of sponsorship contracts concluded with individual athletes, teams, artists or authorised participants in one of the events* referred to in paragraph 1. After all, also in ordinary cases of sport sponsorship contracts, many clauses are devoted to govern the relationship between the sponsors of events, teams, broadcasters, on the one hand, and the sponsors of single athletes, especially when the latter are very famous.

Requirements of ambush law:

1. *Registration* -> the prohibition is applicable only if the organisers of the event affected by the ambush marketing action (i.e. the parasitic activity) have registered a trademark in relation to the event
2. *Time limits* -> the prohibition last also for a period of 180 days after the termination of the event
3. *Type of events* -> at the moment, the prohibition does not apply to events other than sporting events or exhibitions of national or international exposure, as well as shows with artist of national or international reputation

The assessment of violation of art. 10 of Law Decree no. 16/2020 is delegated to the Italian Competition Authority (AGCM), which may impose administrative fines from *€100,000 to € 2,500,000* on “parasites”. In addition, the parties harmed by the unlawful parasitic activity are entitled to *initiate actions for damages*, for example by claiming the application of art. 2598 cod. civ., which prohibits acts of unfair competition, or by claiming the application of their IPRs.

To summarise, we discussed about:

- Promotion of a good and service through advertising, behavioural advertising, sponsorship and ambush marketing
- EU legal framework on advertising -> UCPD and M&CAD
- Misleading practises (and in particular misleading advertising) and differences between the UCPD and M&CAD legal framework -> B2B vs B2C transactions
- Aggressive advertising
- Comparative advertising
- Focus on influencer marketing

Placement

The European Union has many regulations governing the sale and distribution of products and services. To make sense of them, we can break them down into two scenarios:

- *Whether you use indipendent third-party companies*
- *Whether you sell your products and services directly, including through you own branches*

We are not going to cover every regulation, but we will focus on a few that specifically stress the importance of fair trade practises and undistorted competition. More, we will devote significant time to the regulations governing sales through platforms that provide intermediary services, as the importance of these platforms is paramount and continues to grow.

You operate via third parties

Numerous national laws govern these contracts, and the applicable rules depend on the type of relationship you wish to establish with the third party. This can range from a very loose

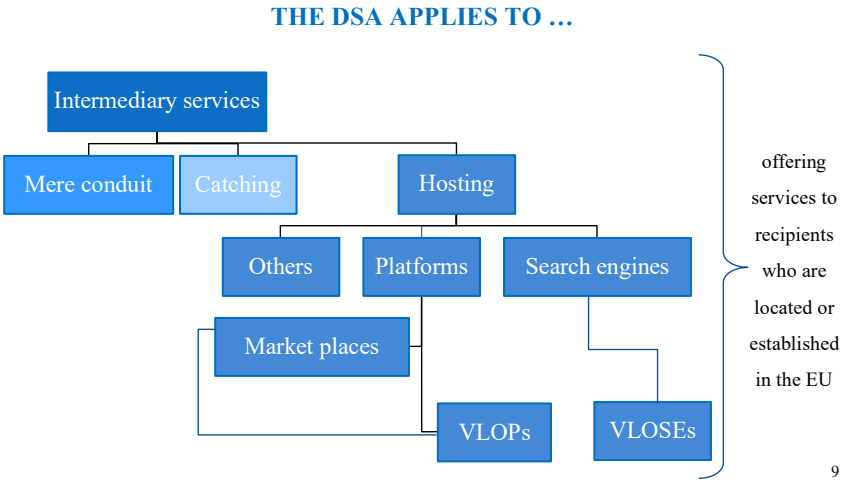
arrangement, such as a sales contract, to a highly integrated one, like a franchising contract. Regarding the main EU regulations governing B2B contracts, we will address the following:

- *Antitrust rules*, particularly those outlined in the *Regulation on Vertical Agreements (VBER)*
- The *Digital Service Act (DSA)*, which governs relationships with digital providers of intermediary service -> In the future, these rules could be crucial if you work for a digital company operating as an intermediary service provider or for any other company that interacts with it.

The starting point is *User Generated Content* that is stored and transmitted thanks to numerous and diverse services -> User-generated content (UGC) refers to any content created by users, rather than by the brand or company itself, and is often shared on social media or other digital platforms. This can include things like images, videos, reviews, testimonials, and even blog posts, all of which reflect real user experiences and opinions. The question is if there should be regulations for those services, the rationale is to fight disinformation and the spread of illegal or otherwise harmful content.

The DSA establishes harmonised rules for a *safe, predictable, and trusted online environment that fosters innovation while effectively safeguarding fundamental rights and consumer protection*. It applies to any content regardless whether it is user generated or not. Specifically, the DSA establishes:

- *A safe harbour form liability for providers of intermediary services*
- *Rules on due diligence obligations tailored to specific categories of providers of intermediary services*
- *Rules for the implementation and enforcement of the DSA itself*



The DSA imposes obligations on those providing *information society services*, that is those providing services normally for remuneration, at a distance, that offer and *intermediary service to recipients who are located or established in the EU*, regardless of whether that intermediary service provider is incorporated or located within the EU.

Do I offer an intermediary service?

- *I provide a mere conduit service* -> that is, I provide access to a communication network or I transmit information provided by the recipient in a communication network without altering the information itself. *Examples*: Direct messaging services and voice over IP (VoIP); Internet service providers; Virtual private networks (VPNs); Domain name registries
- *I provide a caching service* -> that is, my service involves the automatic, intermediate, and temporary storage of information for the sole purpose of efficient onward transfer of information provided by the recipient. *Examples*: Web and database caching, Reverse/ content adaption proxies; Content delivery networks
- *I provide a hosting service* –> that is, I store information provided by, and at the request of, a recipient. *Examples*: Cloud hosting; Shared hosting; Virtual private hosting

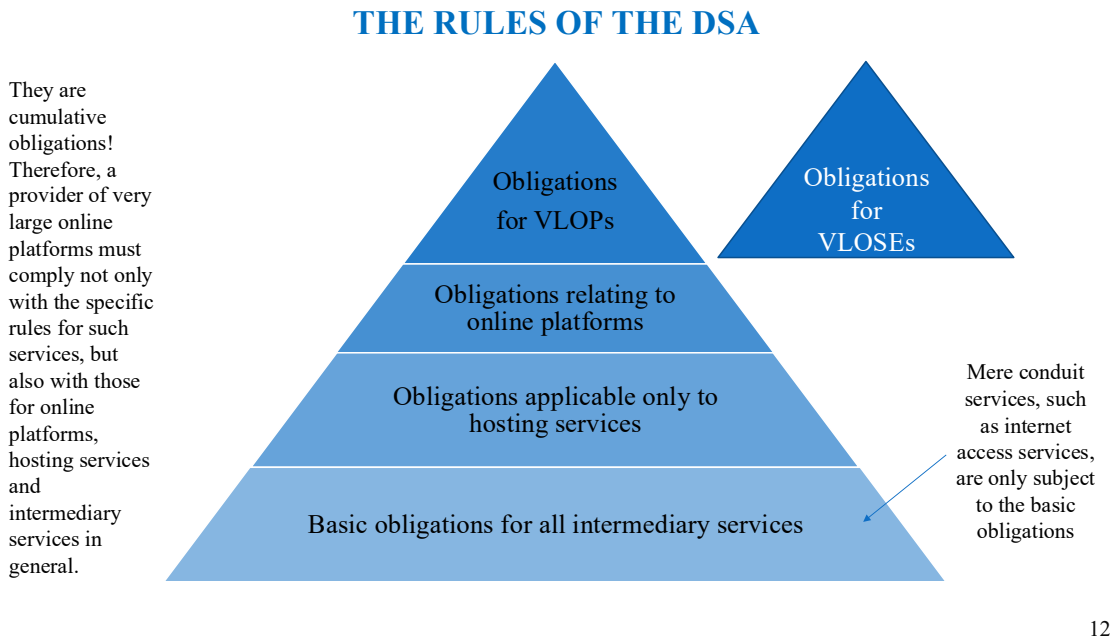
In addition, the DSA imposes further obligations on *online platforms* (which are not micro or small enterprises) and *search engines*, with even stricter requirements for marketplaces, *very large online platforms (VLOPs)* and *very large online search engines (VLOSEs)*.

What kind of hosting service do I offer?

- *I provide an online platform* -> that is, my hosting service stores and disseminates information to the public (at the request of the recipient)
    - In particular, I provide a marketplace – that is I provide an online platform that allows consumers to conclude distance contracts with traders
    - In particular, I provide a VLOPs – that is, I have at least 45 million active users in the EU per month on average and the Commission has designated my service as a VLOP. Marketplaces can be VLOP

- *I provide an online search engine* –> that is, my hosting service allows users to input queries in order to perform searches of all websites or all websites in a particular language on the basis of a query in the form of a keyword, voice request, phrase or other input and returns results in any format to which the requested content can be found
    - In particular, I provide a VLOSEs – that is, I have at least 45 million active users in the EU per month on average and the Commission has designated my service as a VLOSE

Overall, we focus on the regulatory framework governing *digital and spatial environments, particularly with regard to the distribution of goods and services through third-party arrangements*. A significant part of this framework involves vertical agreements (contracts between businesses and intermediaries enabling distribution) and the newly adopted Digital Services Act (DSA) of the European Union. The DSA addresses a range of *legal and regulatory issues related to intermediary digital services*. It emerged in response to challenges posed by user-generated content, such as intellectual property infringements, unauthorised use of trademarks, the spread of fake news, terrorism-related content, and explicit materials. The core question is whether digital platforms *should be held accountable for content uploaded by users and, if so, to what extent*. To manage



these concerns, the DSA aims to *harmonise rules across EU Member States*, ensuring uniform application regardless of where a service provider is based, as long as it targets users within the EU. The regulation categorises service providers into several types (mere conduit, caching, and hosting services) and imposes obligations accordingly. Notably, it introduces *more stringent requirements for very large platforms (VLOPs) and search engine*s, which are defined as those with at least 45 million active users in the EU per month. The DSA establishes a "*safe harbor*" provision for intermediary services, exempting them from liability for illegal content, provided they were *unaware of it and act promptly once notified*. However, this protection does not extend to marketplaces that actively facilitate the dissemination of unlawful content. Furthermore, the regulation *does not require proactive monitoring by platforms but mandates action upon discovering illegal material*, including removal and reporting obligations. The DSA adopts a *risk-based approach*, recognising that larger platforms pose a higher risk of societal harm due to the scale of user interaction. It imposes increasing levels of due diligence obligations proportional to the size and influence of the service provider. This approach aims to protect democratic values and fundamental rights while also fostering digital innovation and economic development within a consistent legal framework.

Rules applying to all intermediary service providers

1. What if the information/content available through or on an intermediary service provider is unlawful? Should the intermediary be liable for it? -> NO, under Articles 4-6, there exists a liability exemption, also named, **safe harbor**, for ISPs. Namely, ISPs are not liable for the information/ content hosted on their service so long as they *either do not know* the information/content is illegal or infringing, or *they promptly remove or block access to that information/ content once aware* that it is illegal or infringing. Under article 6(3), the safe harbor

does not apply to marketplaces in cases of liability under consumer protection law if the online platform presents specific information or facilitates an unlawful transaction in a way that would lead an average consumer to believe that the information, product, or service is provided either by the platform itself or by a service recipient acting under the platform's authority or control.

2. Should intermediary service providers monitor and control happens through and on them? -> NO, under Articles 7-8, the DSA clarifies that *intermediaries are not under any general obligation* to conduct own-initiative monitoring for illegal or infringing content or activity. Still, they can run such initiatives. Therefore, the DSA further clarifies that intermediaries will not lose the benefit of the safe harbor by virtue of any own-initiative monitoring they carry out on their platforms. *However, if a provider does identify illegal or infringing content via its own-initiative monitoring, it must promptly remove or block access to such content.*

3. *Publication of annual reports on content moderation*, which must include information relating to illegal content, use of automated tools, training measures, and complaints received under complaints-handling systems. For VLOPs and VLOSEs only, such reports must be published *every six months* and the report must specify the *human resources dedicated* to content moderation.

4. *Appointment of points of contact and legal representatives*

5. *Updates to terms and conditions (T&Cs)* -> all providers must ensure that their terms of service use clear, plain, intelligible, user-friendly, and unambiguous language. Further, they must be available in an easily accessible and machine-readable format

6. *Content moderation policies and takedown orders* -> All intermediary services providers should have due regard to the rights and legitimate interests of all parties. Furthermore, they must execute *takedown orders from regulators*

Rules applying to hosting service providers

1. *Notice and takedown moderation* -> providers of hosting services are required to implement mechanisms to *allow recipients of their services to notify* them of the presence of allegedly illegal content. These mechanisms must allow for sufficiently precise and detailed notices to be submitted. Providers of hosting services then have an obligation to provide a *statement* of reasons to the affected user, which must include the decision taken, the facts and circumstances relied on in taking such a decision, information on the use of automated means, reference to the legal or contractual ground relied on (where the decision concerns allegedly illegal content or a violation of T&Cs), and information on the redress available.

2. *Reporting criminal offences* -> providers of hosting services are obligated to inform the national law enforcement or judicial authorities of the relevant EU member state of any

information that gives rise to suspicions of criminal offences involving a threat to the life or safety of persons

Rules applying to online platforms

1. *Redress mechanism for users* -> The DSA requires providers of online platforms to maintain an internal complaints- system that enables the recipients of their services *to lodge complaints* against a decision to remove, disable, suspend, or terminate a user's access to information, services, or their account. Furthermore, providers of online platforms are obligated to inform complainants of their r*easoned decision* and the options available to them, including out of court settlement or other redress options.

2. *But still taking measurers against abusive notices and counter-notices* -> meaning against who frequently provide manifestly illegal content

3. *Prioritising trusted flaggers* -> providers of online platforms must prioritise trusted flagger notices. Trusted flaggers are experts at detecting certain types of illegal content online, such as hate speech or terrorist content, and notifying it to the online platforms. They are appointed by the new authorities created by the DSA

4. *Safety by design: Non-deceitful online interface* -> under the DSA, providers of online platforms are obligated to ensure that their interfaces meet certain design and accessibility standards. In particular, providers *must not design online platforms in a deceitful manner* that would impair recipients' ability to make free and informed decisions. This prohibition seeks to prevent manipulation, that is: platform interfaces from promoting certain user choices over others; repeated requests to the recipient to make a choice which has already been made; and termination of the service being ‚made more difficult than initial subscription or sign-up

5. *Protection for minors* -> more, if an online platform is accessible to minors, providers must implement appropriate and proportionate measures to ensure a high level of security, privacy, and safety for minors

6. *Transparency obligations: Advertising, user profiling and recommender systems* -> providers of online platforms must supply users with information relating to any online advertisements on its platform so that the recipients of the services can clearly identify that such information constitutes and advertisement. Providers of online platforms are prohibited from presenting targeted advertisements based on profiling using either the personal data of minors or special category data (as defined in the GDPR). The DSA also requires providers of online platforms that use recommendation system to set out in their T&Cs the main parameters they use for such systems, including any available options for recipients to modify or influence them. VLOPs and VLOSEs must provide at least one option (not based on profiling) for users to modify the parameters used. They are subject to additional transparency reporting obligations.

Rules applying to marketplaces

1. *Know your business customer (KYBC) checks and other obligations* -> providers of online marketplaces are required to conduct KYBC checks on new traders offering products or services to consumers in the EU, including vetting information provided through reliable services. For any existing traders, providers of online marketplaces are required to make best efforts to do the same. In addition, providers of online marketplaces must also ensure that their interfaces enable compliance with contractual law and product safety information applicable under EU law

Rules applying to VLOPs and VLOSEs

The designation decisions follow a review process conducted by the Commission after the publication of the monthly active user numbers by all platforms on 17 February 2023. Based on this exercise, the Commission issued preliminary findings to the potential VLOPs and VLOSEs with more than 45 million users in the EU. On 25 April 2023, the Commission officially designated 19 VLOPs and VLOSEs. These platforms had to comply by end of August 2023 with the obligations of the DSA. Within the VLOPs and VLOSEs, we can find Alibaba, Amazon store, Apple app Store, Booking, Google, Facebook and many others.

1. *Conducting risk assessments and establishing a compliance function* -> VLOPs and VLOSEs are required to conduct an annual assessment on any systemic risks stemming from the functioning and use of their services and mitigate risks identified in such risk assessment by implementing tailored, reasonable, proportionate and effective mitigation measurer. Such assessments will cover:
   - Dissemination of illegal content
   - Any negative effects for the exercise of the fundamental rights for private and family life, freedom of expression and information, the prohibition of discrimination, and the rights of the child
   - Intentional manipulation of their service with actual or foreseeable negative effects on the protection of public health, minors, civic discourse, or related to electoral processes and public security

2. *Crisis response* -> VLOPs and VLOSEs may be required to take one or more of the following actions in case of a crisis:
   - Assess whether the functioning and use of their service contribute to a serious threat
   - Identify specific, effective and proportionate measurers to eliminate such contribution
   - Report to the commission on these assessments
3. *Compliance function* -> VLOPs and VLOSEs must also establish a compliance function that is independent form operational functions and comprises one or more compliance officers including the head of the compliance function

4. *External and independent auditing* -> VLOPs and VLOSEs must submit annual independent audits to confirm their compliance with various obligations under the DSA. If the opinion of the auditor is not positive, the report must also provide operational recommendations on specific measurers to achieve compliance. Within on month of receiving such recommendations, the platform must adopt an audit implementation report setting out the remedial measures to be implemented. If those measures were not implemented, it should provide justifications for not doing so and any alternative measures taken to address the non-compliance.

5. *Content moderation* -> VLOPs and VLOSEs are required to include in their transparency reports the human resources dedicated to content moderation, the qualifications and linguistic expertise of the persons carrying out the activities, and the indicators of accuracy and related information referred to in such reports

6. *Compile a publicly available database on advertisements* -> VLOPs and VLOSEs that present advertisements on their online interfaces have an additional obligation to make publicly available a repository of information relating to these practices, including information concerning:
   - the period and content of the advertisement, including the name of the product, service
   - brand and the subject matter
   - the person on whose behalf the advertisement is presented and who paid for it (if different)
   - whether the advertisement was intended to be presented to a particular group
   - commercial communications published
   - the number of recipients reached.

No personal data should be included in the repository, and for each advertisement, information about such advertisement should be displayed for the entire period during which the provider presents the advertisement and for one year after the last time the advertisement was displayed.

7. *Data sharing with authorities* -> VLOPs and VLOSEs must provide access to data necessary to monitor their compliance with the DSA where requested by the relevant Digital Service Coordinator

Sanctions -> each EU Member State is permitted to determine the penalties applicable to infringements of the DSA by providers of intermediary services under their competence, with the maximum penalty for failure to comply with the DSA to not exceed 6% of that intermediary service provider's total annual worldwide turnover. The Commission is empowered to issue binding orders and fines directly against VLOPs and VLOSEs, with fines to not exceed 6% of the provider's total annual worldwide turnover, or, in the case of periodic penalty payments, 5% of the average daily income or annual worldwide turnover per day. Furthermore, the DSA affords recipients of services the right to seek compensation from providers in respect of damage or loss suffered due to an infringement by the providers to comply with the DSA.

To summarise, the Digital Services Act (DSA) introduces a *harmonised regulatory framework across the European Union*, aiming to increase accountability, transparency, and user protection in the digital space. It imposes *layered obligations* on intermediaries, particularly hosting services and online platforms, with increased responsibilities for very large online platforms (VLOPs) and search engines.

1. *Governance and Designated Personnel* -> Organisations must appoint responsible personnel for DSA compliance. A designated officer should oversee adherence to the DSA within the organisation, ensuring internal processes align with legal expectations.
2. *Transparency and Terms of Use* -> Platforms are required to clearly communicate terms and conditions to users in an accessible and comprehensible manner. Transparency must be maintained not only in terms of content rules but also in how users are informed of platform decisions.
3. *Takedown Orders and Content Moderation* -> If notified, especially by regulators, of unlawful content, platforms must act promptly to remove it. These takedown orders are binding, and platforms cannot contest them. Failure to act may result in liability. Users must also be informed of the rationale for content removal or retention, along with available redress mechanisms.
4. *User Notification and Redress* -> Platforms must implement accessible procedures through which users can report illegal content. Upon receiving such a notice, platforms must respond, provide justification for actions taken (or not taken), and guide users on further steps, including appeals. These mechanisms aim to balance the prevention of unlawful content with safeguards against opportunistic or mistaken takedowns.
5. *Duty to Report Criminal Offences* -> Where platforms become aware of content that may indicate criminal conduct, particularly threats to life or safety, they are legally obliged to report such matters to law enforcement authorities. This obligation supersedes privacy considerations in such cases.
6. *Interface Design and Anti-Manipulation Requirements* -> Platforms must avoid manipulative interface design (e.g., dark patterns) that mislead users into undesired actions. Special protections apply to minors, including restrictions on profiling and algorithm-based content recommendations.
7. *Transparency in Advertising and Recommendations* -> Platforms must disclose the parameters behind advertisement targeting and recommendation systems. Users should be offered alternatives that are not based on profiling—particularly minors.
8. *Marketplace Obligations (Know Your Business Customer)* -> Online marketplaces must vet traders before allowing them to operate on their platforms, ensuring consumer protection and the legitimacy of business partners. Interfaces must enable compliance with contractual and consumer protection requirements under EU law.
9. *Obligations for Very Large Online Platforms (VLOPs) and Search Engines* -> Designated VLOPs (e.g., Google, Amazon, Meta platforms) face enhanced obligations:

- Risk Assessments: Evaluate risks to fundamental rights, dissemination of illegal content, and systemic manipulation.
- Mitigation Measures: Implement proportional and effective strategies to mitigate identified risks.
- Crisis Management: Establish contingency plans for rapid response in case of significant breaches.
- External Auditing: Undergo independent audits to verify DSA compliance.
- Human Oversight: Employ human moderators to review content and evaluate algorithm performance.

Some critics argue the DSA may *disproportionately affect non-EU digital service providers*, particularly U.S. and Chinese companies, raising concerns about its role in global trade tensions.

Overall, in the the indirect model, businesses rely on *intermediaries or distributors to manage the placement of their goods and services*. In contrast, direct distribution involves the *company itself reaching out to consumers* without third-party involvement. Each approach brings its own set of legal implications, particularly under current European regulatory frameworks. The legal landscape surrounding indirect distribution has been significantly shaped by the *Digital Services Act (DSA)*, a recent regulatory initiative from the European Commission aimed at harmonising the governance of digital intermediaries. The principal objective of the DSA is to create a *uniform framework* for addressing the circulation of unlawful content and products across online platforms. To achieve this, the Commission established a threefold mechanism. Firstly, the DSA preserves the *safe harbor principle*, which stipulates that intermediary service providers are not liable for the content they host, provided they have *no actual knowledge of its illegality*. However, once notified of unlawful content, intermediaries are legally obliged to *act swiftly to remove or disable access to it*. Notably, there is *no general obligation to monitor user activity*. The regulation also includes a *"Good Samaritan" clause*, which ensures that platforms engaging in voluntary monitoring are not penalised if they fail to act perfectly, thereby incentivising responsible oversight without imposing strict liability. Secondly, the enforcement framework introduced by the DSA is *multilevel*. Oversight responsibilities are divided between the European Commission and national authorities. The Commission directly supervises major platforms and search engines, while national regulators handle the rest. This structure aims to *balance efficiency and coordination across the EU*. The third and most innovative feature of the DSA is its *asymmetric regulation model*. This approach tailors regulatory obligations to the *size and influence of the platform*. Obligations increase progressively from basic intermediaries to hosting services, to online platforms, to marketplaces, and finally to the largest entities (vlops and vloses). Larger platforms, due to their broader impact, are subject to *stricter transparency and accountability requirements*. The rationale is that the more extensive a platform's reach, the more information it must disclose about its operations, particularly regarding how it moderates content and manages its algorithms. The overarching aim is not to punish intermediaries but to *transform opaque systems into transparent ones*, enabling

consumers and businesses to understand and challenge platform practices. *Transparency* is viewed as a prerequisite for the effective exercise of consumer rights and the prevention of unfair competition. In essence, the DSA does not impose harsher sanctions on platforms but rather imposes *costs associated with compliance*, particularly in terms of transparency obligations. These costs have been met with resistance from industry players, but the regulation argues that such transparency is essential to allow users, be they consumers or small businesses, to understand and challenge the behavior of digital platforms.

Antitrust rules and the regulation on vertical agreements

We then transitions to talk about *EU competition law*, often referred to as "uncontrolled rules," which regulates *commercial relationships between independent economic actors*, especially in distribution arrangements. The foundational objective of this legal framework is to preserve and promote competition within the internal market. This body of law draws heavily from *antitrust principles*, originally developed in the United States during the late 19th century as a response to monopolistic abuses. At its core, antitrust law seeks to ensure that *markets remain open, competitive, and efficient*. A fundamental economic principle underlying antitrust law is the concept of *market equilibrium under conditions of perfect competition*. In such a market, prices align with marginal costs, thereby maximising both output and consumer welfare. When firms deviate from this equilibrium, either through collusion or the unilateral exercise of market power, the result is a decline in output and an increase in prices. This leads to *allocative inefficiency*, typically illustrated by the concept of *deadweight loss*. Despite the availability of production inputs and the prevailing state of technology, fewer consumer needs are satisfied, which is economically suboptimal. Moreover, such deviations often result in a *redistribution of surplus*, whereby wealth is transferred from consumers to producers.

One major form of anti-competitive behavior is the formation of *cartels*. A cartel is a *collusive agreement among competitors*, typically aimed at fixing prices, restricting output, or dividing markets. These agreements enable firms to *charge prices above marginal cost, thereby securing economic profits that would not be possible under competitive conditions*. However, cartels are not only *illegal under antitrust law*; they are also inherently *unstable*. Each participant has a rational incentive to defect from the agreement to gain a larger share of the market, making *sustained collusion difficult without additional mechanisms for monitoring and enforcement*. For that reason, is the imperative to maintain strict confidentiality around commercially sensitive information. This includes data related to pricing strategies, cost structures, production volumes, and discount policies. The exchange of such information with competitors can constitute a *concerted practice*, which, while less formal than a cartel, is nonetheless prohibited under EU

competition law. Professionals must *avoid any action that could be interpreted as an attempt to coordinate market behavior*, even if there is no explicit agreement.
In addition to cartels, the chapter addresses *mergers* as another avenue through which firms may seek to influence market structure and dynamics. Unlike cartels, which are prosecuted ex post (after they occur), mergers are generally subject to ex ante review by competition authorities. This preventative approach aims to block mergers that would create or strengthen a dominant position likely to impede effective competition within the market.
Finally, we underscore the importance of vigilance in professional and industry settings, such as trade associations and standard-setting bodies. Professionals must be alert to any discussions that may imply *informal coordination*, such as suggestions to increase prices or reduce output. In such cases, it is not only advisable but legally necessary to *disengage from the conversation* and formally document one's dissent. This ensures transparency and helps avoid regulatory scrutiny or potential liability.
In sum, while the possession of market power is not unlawful in itself, *the abuse of that power*, whether through collusion, improper information sharing, or strategic mergers, is strictly regulated. The overarching aim of competition law is to protect consumer welfare, ensure efficient market outcomes, and preserve the integrity of competitive processes.

Antitrust law is designed to protect the proper functioning of the market from firms that use their market power to undermine the interaction between supply and demand. In particular, firms may attempt to limit competition among themselves to:

- *Increase market prices*
- *Restrict market output*
- *Reduce the quality, variety and pace of innovation in their offerings*

Firms can limit competition by:

- *Abusing their market power when they hold a dominant position*
- *Merging to change the structure of the market*
- *Making agreements* -> any form of cooperation among firms, whether they are horizontal rivals (horizontal agreements) or firms operating at different levels of the production-distribution chain (vertical agreements), is prohibited when the object or effect is to: increase market prices, reduce market output, limit the quality, variety or innovation of firms' offerings

In competition law, firms are not penalised for achieving a dominant market position through merit-based competition. Much like an athlete winning a race through superior performance, a firm that earns dominance by being *more efficient or innovative is not subject to sanctions*.
Instead, regulatory scrutiny arises when a dominant firm *employs anti-competitive practices* to maintain or strengthen its position, thereby impeding market contestability.
The core issue lies not in the existence of dominance per se, but in the *means used to preserve it*. When dominant firms use strategies that prevent competitors from entering or expanding in the

market, these may be considered *exclusionary or foreclosing practices*. One key area where such conduct can occur is in the use of *vertical agreements*, particularly *exclusivity contracts* between producers and distributors.

In EU, there is a regulation which governs vertical agreements -> the *Vertical Block Exemption Regulation (VBER)*. Under the VBER, vertical restraints are presumed to be legal in the absence of market power. The VBER uses a *market share threshold of 30%* as a proxy for the existence of market power. Therefore: below this threshold (the so-called safe harbor), vertical agreements are deemed lawful, *unless they include the so-called hard core restrictions*.
When talking about relevant market, we refer to:

- For suppliers, the relevant market is that on which it sells the goods or services in question
- For buyers, the relevant market is that on which it purchases the contract goods or services. It will often be of much broader geographic scope than the downstream market on which it resells the relevant goods or services.

An exclusivity clause in a distribution agreement may stipulate that a *distributor may only sell the products of one producer*, often accompanied by penalties for breach. When such contracts are executed by a dominant firm, particularly one controlling a significant share of the market, they may result in the *foreclosure of rivals*. For example, if a dominant producer secures exclusivity contracts with 80% of the market's distributors, rival producers are *deprived of critical market access*. Over time, this limits their ability to compete, leading to a reduction in output and an increase in prices -> hallmarks of anti-competitive harm. These effects are illustrated in economic models through the concept of *deadweight loss*, reflecting inefficiencies where consumer demand is unmet despite the availability of inputs and technology. Thus, the primary test of anti-competitive behavior remains whether a practice reduces output and increases prices, either in the short term (e.g., price-fixing cartels) or the long term (e.g., exclusionary distribution strategies). Not all exclusivity agreements are harmful. When *market shares are low, such agreements may serve efficiency-driven purposes, such as creating stable, cooperative relationships between producers and distributors*. This stability can enhance training, post-sale services, and consumer experience. yielding *pro-competitive effects*. In such cases, exclusivity may reduce transaction and coordination costs, contributing positively to consumer welfare. For example, a producer may choose to contract exclusively with a small distributor (e.g., one holding 5% of the market) to ensure service quality and brand consistency. In the *absence of significant market power, these arrangements are generally not considered to raise competition concerns*.

There is no presumption of illegality above the 30% threshold, but the block exemption will not apply and companies must make their own assessment to determine whether the agreement is restrictive of competition. The legality of exclusivity agreements under EU law depends on a *contextual analysis* of market share, contract duration, and actual or potential foreclosure effects. While such agreements can be beneficial in enhancing efficiency and service quality, they must

not be used by dominant firms to entrench their market position in ways that harm competition and consumer welfare. Ultimately, the guiding principle remains that a practice is considered anti-competitive when it *raises prices and reduces output*, thereby diminishing overall consumer welfare, whether this outcome is achieved through collusive conduct or exclusionary strategies. In antitrust law, a firm's conduct is deemed anti-competitive not only when it reduces output and increases prices but also when it diminishes product quality, variety, and innovation, thus harming consumer welfare. Once anti-competitive behavior is identified, it is important to analyse the specific conduct enabling such market power. These include abuse of dominance, mergers, and agreements. Particular attention is given to agreements, especially vertical agreements such as distribution contracts. Unlike horizontal agreements, which are often anti-competitive by object (e.g., price-fixing cartels), vertical agreements may have both pro-competitive and anti-competitive effects. Consequently, they must be assessed individually, based on their market impact and specific contract clauses.

The VBER contained a "blacklist" of vertical restraints, which are called hard core restrictions. The VBER does not cover a vertical agreement which includes one of these hard core restrictions, even if the market share threshold is not exceeded. In addition, hard core restriction are seriously anticompetitive. Therefore, it is very likely that agreements that include them are deemed unlawful by object. The hard core restrictions are:

- *Resale price maintenance (RPM)*
- *Restrictions of passive sales (including sales over the internet) in exclusive distribution agreements*
- *Restrictions of cross-suppliers between members of a selective distribution arrangement as well as restrictions of sales to end-users by buyers operating at the retail level of trade.*

Fixing minimum resale prices is *unlawful*. This can occur through explicit contractural provisions requiring to charge a specific price or indirectly through practices like *minimum advertised prices* (MAPs). MAPs prohibit distributors from advertising prices below a supplier-set level. While distributors can technically sell at lower prices, MAPs discourage this by *limiting their ability to inform customers of discounts, undermining price competition*. MAPs may be justified in cases where a distributor consistently resell products below wholesale price, provided it can be shown that the MAP prevent such losses.
RPM can also arise from measures to identify price-cutting distributors, such as *price monitoring systems, most favoured customer clauses, or requiring retailers to report deviations from standard price*s. At the same time, the practise of recommending a resale price or requiring a retailer to respect a maximum resale price is exempted by the VBER.

Guess case -> as well known, Guess specialises in the design, marketing and distribution of apparel and accessories. Guess distributes its products in the EU through a selective distribution network of authorised retailers. The commission initiated a proceeding against Guess in Jun 2017,

following the e-commerce sector inquiry. It found that: Point 11 of the General Sales Terms used for Guess' multi-brand retailers stated as follows: "For each sample range GUESS EUROPE shall fix a minimum price for sale to the public of its own products, by means of a «recommended price-list» inclusive of VAT, for the purpose of making the *product image uniform on the market*. The Purchaser undertakes to sell the goods purchased at prices that comply with those indicated on the aforementioned price-list. Failure to observe this obligation by the Purchaser shall give rise to the obligation to *reimburse the damages incurred* and shall entitle GUESS EUROPE to discontinue all future supplies."
The commission found that this clause was unlawful. Its object was to have uniform retail prices un specific markets in order to make the product image uniform on the market. Thus, Guess Europe monitored pricing of third-party retailers and tried to influence them to correct resale prices "misaligned" with Guess Europe's "recommended" resale prices.

Exclusive distribution -> In an exclusive distribution system, the supplier allocates a territory or a group of customers exclusively to one or a limited number of buyers (up to 5), while restricting all its other buyers within the Union from actively selling into the exclusive territory or to the exclusive customer group (80).
Pro-competitive effects: Suppliers often use exclusive distribution systems to incentivise distributors to make the financial and non-financial investments needed to develop the supplier's brand in a territory where the brand is not well known, or to sell a new product in a particular territory or to a particular customer group, or to incentivise distributors to focus their selling and promotional activities on a particular product. For the distributors, the protection provided by exclusivity may enable them to secure a certain volume of business and a margin that justifies their investment efforts.
Anticompetitive effects: The main possible competition risks are market partitioning, which may facilitate price discrimination, and reduced intra-brand competition. Furthermore, when most or all of the strongest suppliers active in a market operate an exclusive distribution system, this may also soften inter-brand competition and/or facilitate collusion, at both the supplier and the distributor levels. Lastly, exclusive distribution may lead to the foreclosure of other distributors and thereby reduce both inter-brand and intra-brand competition at the distributor level.
Passive sales restrictions on the other hand are a hard-core restriction under EU competition law. Thus, they cannot be imposed on the appointed exclusive distributor(s).

Selective distribution -> in a selective distribution system, the supplier undertakes to sell the contract goods or services, either directly or indirectly, only to distributors selected qualitative and/or quantitative criteria. Those distributors undertake not to sell such goods or services to unauthorised distributors within the territory reserved by the supplier to operate the system. Therefore, selective distribution systems are comparable to exclusive distribution systems in that they restrict the number of authorised distributors and the possibilities of resale. The main difference between the two types of distribution system lies in the nature of the protection granted

to the distributor. In an exclusive distribution system, the distributor is protected against active selling from outside its exclusive territory, whereas in a selective distribution system, the distributor is protected against active and passive sales by unauthorised distributors. The possible competition risks of selective distribution systems include a reduction in intra-brand competition and, especially in the case of a cumulative effect, the foreclosure of certain types of distributors, as well as the softening of competition and the facilitation of collusion between supplier or between buyers, due to the limitation of the number of buyers. In a selective distribution system, the following ones are hardcore restrictions:

- *Restrictions of cross-suppliers* between the members of the selective distribution system operating at the same or different levels of trade
- *Restrictions of active or passive sales to end users* by members of the selective distribution system operating at the retail level of trade

Online distribution -> a supplier cannot prevent its distributors from going online. A producer can prevent it distributors from selling its products through some websites, online marketplace. A producer can prevent its distributions from opening a website in a language different from that of the distributors's territory and from registering domain names corresponding to territories other than those of the distributors themselves

Following the DSA, we turned to *antitrust law*, whose goal is to *safeguard market functionality by preventing companies from leveraging market power to distort competition*. Market power may arise either from a company's dominant position or through collusive agreements with other firms. Not all agreements are prohibited. Those deemed *"restrictions by object"*, such as price-fixing cartels—are automatically unlawful due to their inherently anti-competitive purpose. However, many agreements fall into a more ambiguous. We discussed the principles of European Union competition law, particularly in the context of vertical agreements, passive and active sales, territorial restrictions, and the legal implications surrounding these commercial practices. Advertising in different countries within the EU, such as China and Italy, can be carried out, as long as it *does not interfere with the active sales territory of authorised distributors*. A hypothetical scenario is presented in which a German consumer travels to Italy to purchase a Mercedes vehicle at a lower price due to more favourable local pricing strategies. This is permissible because the European Union guarantees the *free movement of goods and services across its internal borders*. Consequently, Italian distributors cannot be prohibited from selling to German customers, even if such cross-border purchases result from price disparities. We shift to the concept of *passive sales*, particularly in online commerce, where practices such as *geo-blocking* previously allowed companies to restrict sales based on a customer's location or payment method. The EU's geo-blocking regulation now prohibits such restrictions, even when applied by vertically integrated platforms like Amazon, thereby reinforcing the internal market's non-discriminatory access principle.

A producer or distributor with a market share below 30% is generally safe from scrutiny, while those above 40% may be considered dominant and subject to more rigorous legal analysis. Between 30% and 40%, cases must be evaluated individually. If a producer with more than 40% market share and a distributor with more than 30% enter into exclusive agreements or similar arrangements, there is a high likelihood of competitive harm due to potential foreclosure effects. The *relevant market must be clearly defined based on the type of product and its method of distribution*, such as retail distribution on highways versus standard urban outlets. A monopolistic position can occur when a firm introduces a new technology with no substitutes, although dominance is more commonly established over time rather than instantly, due to existing alternative solutions that meet similar consumer needs. Further analysis is provided on contractual clauses that *restrict cross-supply among members of a selective distribution network or limit sales to end users*, which are considered "hardcore restrictions." The inclusion of such clauses removes the protection offered by the EU's "safe harbor" rules and exposes the agreements to antitrust scrutiny, potentially rendering them null and void.

Exercises

Scenario question 1

A multinational company, “TechVision S.p.A.”, manufacturers high-end televisions. To distribute its products in Italy, it enters into an agreement with a selected network of specialised retailers, including the chain “AudioLux”, imposing specific clauses in the contract. Comment on the following statements:

- Minimum resale price : Retailers are not allowed to sell TechVision television below a certain price set by the company
- Territorial exclusivity: each retailer is allowed to sell only within a specific geographical area, avoiding internal competition within the network
- Ban on unauthorised online sales: AudioLux and other retailers are allowed to sell the products only in physical stores and not through online platforms, unless expressly authorised by TechVision

The case of Tech Vision SBA is introduced as an illustrative example. This company restricts the sale of its products to physical stores only, barring online sales unless explicitly authorised. This practice must be evaluated to determine whether it *unjustly restricts passive sales or is a justified commercial policy under selective distribution rules*. The discussion then turns to territorial exclusivity, noting that while granting exclusive geographical areas to distributors can enhance efficiency and service quality, it must not inhibit passive sales. Whether the exclusivity applies to individual stores or entire retail chains does not affect the legal assessment; the key question is whether the practice *restricts active or passive sales*. Excessively narrow territories may be *commercially unviable for distributors*, while excessively broad ones may harm competition within the brand (intra-brand competition). The analysis of such practices requires *knowledge of market shares and the competitive structure of the relevant market*, although the course material assumes that students are not yet equipped to conduct full antitrust evaluations. Ultimately, the emphasis

lies on recognising when *vertical agreements cross into anti-competitive behavior and understanding the regulatory frameworks designed to preserve market integration, consumer access, and fair competition* within the EU's internal market. The goal is to identify and apply core legal rules, rather than engage in complex market analysis or consumer behavior assessments. We focus on the legal treatment of various vertical restraints under EU competition law, particularly in the context of online sales, passive sales, and the application of exclusive distribution agreements. It explains the implications of certain contractual clauses and commercial practices that restrict how products are distributed and sold within the internal market, highlighting which are lawful and which constitute hardcore restrictions. One of the key points concerns the **ban on minimum resale prices**, which is classified as a hardcore restriction under EU competition rules. A supplier *cannot impose fixed or minimum prices at which distributors resell products*; such vertical price-fixing is per se unlawful, as it restricts competition by eliminating price autonomy at the distribution level. Another central issue is the **prohibition on unauthorised online sales**, which is also largely considered unlawful when imposed broadly. A supplier cannot universally ban its distributors from engaging in online sales. The European Court of Justice has established that an outright prohibition of online sales constitutes a restriction of passive sales, which is not permitted under the Vertical Block Exemption Regulation (VBER). However, a supplier may still impose *qualitative criteria* to ensure a certain standard for online sales platforms, such as the use of specific website layouts, branding, or exclusion from third-party marketplaces like Amazon or eBay, provided these standards are non-discriminatory and proportionate. Nonetheless, these criteria must not serve as a disguised method to indirectly ban online sales, which would be unlawful. We also discuss *language and domain restrictions*. For example, a distributor granted territorial exclusivity in Italy cannot launch a website in German or register a domain ending in ".de", as this would constitute active sales into the German distributor's territory. However, *passive sales must remain allowed*, meaning a German customer can access the Italian distributor's website and purchase goods without any active solicitation. This reflects the broader principle in EU competition law that distinguishes between active sales (targeted marketing or direct approaches to customers in another distributor's territory) and passive sales (responding to unsolicited requests).

Scenario question 2

The company "Medilux AB", based in Sweden, manufacturers high-tech medial devices used in hospitals. Medilux operates a selective distribution network across the EU and signs exclusive distribution agreements for each country. In Italy, the exclusive distributor is "Sanitaria 3D S.r.l." In its contracts with distributors, Medilux includes a clause prohibiting them from responding to purchase requests from customers located outside their designated territory, even if the requests come directly from foreign hospitals. At the same time, Medilux implements a commercial policy involving the systematic refusal to supply distributors who have sold products in territories not assigned to them, especially when such sales were not actively promoted.
Comment this.

The case study of Medilux AB, a Swedish company with a selective distribution system, illustrates this principle further. Medilux's contractual clause prohibiting distributors from responding to unsolicited requests from customers in other EU territories is deemed **unlawful**, as it explicitly restricts passive sales. Additionally, Medilux's practice of systematically cutting off supplies to distributors who made such sales, without actively promoting them, is also unlawful if the distributors are already within the company's distribution network. However, if Medilux merely chooses not to initiate business relations with third parties known for engaging in passive sales, that decision, in itself, is **lawful**, since it involves no contractual obligation or punishment but rather a selective commercial policy. The distinction between these two scenarios, penalising an existing distributor versus choosing not to engage with a new one, is legally significant. The former can constitute a restriction of passive sales and thus be considered anticompetitive, while the latter falls within the supplier's discretion to choose its trading partners. In sum, the key legal takeaways concern the illegality of minimum resale price maintenance, the inadmissibility of blanket bans on online sales, the requirement to allow passive sales even within exclusive distribution systems, and the nuanced treatment of commercial decisions that affect intra-EU trade. These principles reinforce the European Union's commitment to ensuring the free movement of goods and services within the single market and upholding competitive market structures.

You operate as a sole proprietor

You sign B2C contracts -> the EU rules governing B2C contracts are many, such as:

- *Consumer rights directive* -> rules on consumer information, right of withdrawal and other contractual issues
- *Consumer sales and guarantees* -> rules on consumer remedies and guarantees in the sale of goods and the supply of digital content and digital services
- *Directive on repair of goods* -> promoting repair improves the sustainable consumption of good by consumers
- *Unfair contract terms directive* -> details of an EU law related to the language of consumer contracts that aims to prevent imbalances in the rights consumers and sellers/suppliers
- *Price indication directive* -> rules on the indication of the selling price, the price per unit and price reductions of consumer goods
- *Misleading and comparative advertising directive* -> EU law to protect traders (B2B and B2C) against misleading advertising
- *Unfair commercial practices directive* -> EU rules to protect consumers from unfair practices before, during and after a commercial transaction

The unfair contract terms directive -> the directive applies to all kinds of contracts on the purchase of goods and services, for instance online or off-line-purchases of consumer goods, gym subscriptions or contracts on financial services, such as loans. At present, these rules

already matter because we are consumers. For the future, they could be crucial, if we worked for a company that could impose unfair standard contract terms on its consumers.
The Unfair contract terms directive (93/13/EEC) aims to harmonise the rules that member states apply to protect consumers against unfair standard contract terms (unfair SCT) imposed by traders. In doing so, it ensurers a set of common principles and rules that guarantee the same minimum level of protection across the entire EU.
Some contracts may include terms that have not been individually negotiated. In other words, some contracts may be drafted in advance: they can be pre-formulated. Think about contracts in telecommunication, real estate, retail (products warranties, return policies, and customer loyalty programs), utilities, travel and hospitality, construction, banking, insurance or finance. In summary, SCTs facilitate commercial transactions and can be useful in setting out the rights and obligations of the parties under a given contract once and for all. Still consumers cannot influence the substance of these terms. Therefore, sellers and suppliers possess a considerable advantage over them, an advantage that they can abuse via one-sided standard contracts or by depriving consumers of their essential rights.
Contract terms are unfair if, contrary to the requirements of good faith, they cause significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer. When deciding if a contract term is unfair, we need to consider:

- The type of goods or services involved
- All the details and conditions existing at the time the contract was made, including any other related contracts

Importantly, the fairness check does not apply to the main purpose of the contract or whether the price is reasonable compared to what you are getting, as long as these terms are clearly and simply written. Such terms will not bind the consumer, and the contract will continue to bind the parties if it is capable of continuing in existence without the unfair provisions.

Examples

1. Eliza joined her local gym. When she had a closer look at her membership contract, she was surprised to read that the gym doesn't accept responsibility for any harm or injury caused by the use of the facilities and equipment, even when they are worn out or damaged -> this is unfair -> *a contract can't limit or exclude the seller's or supplier's responsibility if their actions (or omissions) cause a consumer's death or personal injury*
2. Sam ordered his weeding dress from a fashion designer. Two weeks before the wedding, he was supposed to meet the designer for a final fitting. When he called her to make an appointment, she told him she'd ended their contract without providing any real justification. Sam checked with a lawyer friend whether the designer could just cancel the contract like that. His friend explained it wad clearly and unfair term -> *A seller or supplier can't cancel the contract at their discretion without giving the consumer the same right*
3. Mark has a 1 year mobile phone contract which he took out 10 months ago. His wife recently switched to a new mobile phone company offering very attractive bundle packs and free calls

within the network. Mark decided to switch to this new operator as soon as his contract expired. He checked his contract and found out that, if he wanted to end it, he should have given 6 months' notice. As he hadn't done that, his contract had been automatically extended for another year. Mark was disappointed and decided to contract his national consumer organisation. They informed him it was unfair, because *a contract can't automatically renew unless the consumer has a fair and reasonable time to say they don't want it renewed* -> a six-month notice period is excessive for a one-year contract -> case by case analysis

Rights imbalance:

- A contract cannot limit the consumer's rights if the seller or supplier fails to meet their obligations
- A contract cannot block the consumer's legal actions, restrict evidence, or unfairly shift the burden of proof
- A seller or supplier cannot transfer their rights or obligations in a way that weakens consumer protections without consent
- A seller or supplier cannot have sole authority to judge contract compliance or interpret the terms

Money imbalance:

- A seller can't keep the consumer's payment after cancellation unless the consumer gets equal compensation if the seller cancels
- Consumers can't be charged and unfairly high penalty for not meeting their obligations
- The price can't be set at delivery or increased significantly without allowing the consumer to cancel

One-sided changes:

- A seller or supplier can't change the terms of the contract on their own without a valid reason clearly stated in the contract
- A seller or supplier can't change the product or service's key features without a valid reason
- A seller or supplier can't end an open-ended contract without reasonable notice unless there's a serious reason for it

Duty imbalance:

- A seller or supplier can't have the exclusive right to decide if the goods or services meet the contract terms or interpret the contract
- A consumer shouldn't be forced to meet all their obligations if the seller or supplier isn't doing their part
- A contract can't force the consumer to go through with the agreement if the seller's or supplier's obligation depends only on their own decision

Exercises

Example 1

A company that offers consumers personalised recommendations on events to attend launches a new online platform. During registration, users are asked to provide personal data (such as age, location, and consumer preferences) and to accept a generic privacy notice regarding data processing. After a few months, some users receive offers specifically targeted at the LGBTQ+ community. Several users complain, claiming they never consented to such targeted and potentially intrusive use of their personal information.
Comment.

This scenario raises several significant concerns under the General Data Protection Regulation (GDPR), particularly in relation to the *principles of valid consent, transparency, data minimisation, and the processing of special categories of personal data*. First, under Article 6(1)(a) of the GDPR, personal data may be processed based on the consent of the data subject. However, this consent must meet *strict requirements*: it must be freely given, specific, informed, and unambiguous. In the present case, users were asked to accept a generic privacy notice during registration. If that notice did not clearly explain the scope of data processing, particularly that personal data would be used to infer sensitive characteristics such as sexual orientation for the purpose of targeted recommendations, then the consent obtained *cannot be considered valid*. A general acceptance of terms without any detailed explanation of profiling and targeting does not satisfy the requirement for specificity or informed consent. Moreover, the use of user data to send offers targeted at the LGBTQ+ community raises concerns under Article 9 of the GDPR, which *prohibits the processing of special categories of personal data*, including data revealing sexual orientation, unless one of the exceptions applies. The most relevant exception here would be the explicit consent of the data subject. However, there is *no indication that users explicitly consented to this type of processing*. If the platform inferred or assumed sexual orientation based on user behaviour or preferences, and then used that inference for targeting, it would amount to unlawful processing of sensitive personal data in the absence of explicit consent.
Another issue concerns Article 22 of the GDPR, which *limits decisions based solely on automated processing*, including profiling, that produce legal effects or similarly significant impacts on individuals. If the platform used automated profiling to identify users as potentially belonging to the LGBTQ+ community and then targeted them with specific offers, that activity may fall within the scope of Article 22. Unless the user has given explicit consent, or the profiling is necessary for the performance of a contract, such processing would also be *unlawful*. The situation further raises questions under the GDPR's core principles of transparency and data minimisation, as set out in Articles 5 and 13. Users must be *clearly informed about what data is collected, for what purposes, and how it will be used*. If the privacy notice lacked clarity on the fact that personal data would be analysed to generate targeted offers based on potentially sensitive traits, then the platform failed to meet the transparency requirement. Similarly, if the data collected and the inferences made go beyond what is necessary for the service provided, it would breach the

principle of data minimisation. In conclusion, the platform appears to have violated the GDPR in several respects. The consent obtained from users was *neither sufficiently specific nor informed* to justify the type of targeted profiling that occurred. The inferred targeting based on sexual orientation constitutes processing of special category data without explicit consent, which is strictly prohibited. The *lack of transparency* in the privacy notice and the likely overreach in the use of personal data further exacerbate the compliance issues. The company should immediately reassess its data processing practices, revise its privacy notice to clearly explain profiling activities, and ensure that explicit consent is obtained before any sensitive personal data is used. A *Data Protection Impact Assessment* (DPIA) would also be appropriate, given the potentially high risks to individual rights and freedoms.

Example 2

BurgerBlast opts for a bold strategy, presenting a head-to-head comparison between their burgers and those of TastyBites. Their TV and online campaigns showcase the two offerings side by side, with a persuasive voiceover touting BurgerBlast's advantages: "Spot the difference! Our burger is bigger, juicier, and more affordable than TastyBites'. Plus, we pride ourselves on using only the freshest meats and top-notch ingredients for maximum flavour!" Comment

The marketing strategy adopted by BurgerBlast raises important legal considerations under the framework of *comparative advertising*, which is regulated in the EU by Directive 2006/114/EC concerning misleading and comparative advertising, as well as by national laws implementing it. While comparative advertising is permitted, it must adhere strictly to certain conditions in order to be lawful. Firstly, under Article 4 of the Directive, comparative advertising is allowed o*nly if it is not misleading, compares goods or services meeting the same needs or intended for the same purpose, and objectively compares one or more material, relevant, verifiable, and representative features of those goods or services*. In this case, BurgerBlast is comparing its burger directly to that of TastyBites, focusing on size, taste (juiciness), price, and ingredient quality. These are all material and potentially relevant features in the eyes of the average consumer.

However, several legal concerns may arise. The claim that BurgerBlast's burger is "bigger, juicier, and more affordable" must be factually *accurate and objectively verifiable*. If these claims are based on subjective impressions or internal tests that are not made available or independently substantiated, they may be considered misleading under both the comparative advertising directive and the Unfair Commercial Practices Directive (2005/29/EC). Similarly, the assertion that BurgerBlast uses "only the freshest meats and top-notch ingredients" implies a qualitative superiority that must be *backed by verifiable standards and evidence*. If TastyBites also uses high-quality ingredients and the difference is negligible or non-existent, the statement could unfairly denigrate a competitor. Furthermore, comparative advertising must *not discredit or denigrate the trademarks, trade names, or other distinguishing marks of a competitor*. While BurgerBlast's campaign does not appear to include explicit derogatory language, the tone and presentation may arguably border on disparagement if the comparison is found to exaggerate differences or

portray TastyBites' product in a negative, mocking light. For instance, the phrase “Spot the difference!” combined with the implication that TastyBites' burger is inferior could be perceived as creating an unfair impression that goes beyond fair competition. There is also a *reputational element* at stake: if TastyBites can demonstrate that the campaign unjustly harms its brand or misleads consumers, it may have grounds to bring a legal challenge based on unfair competition or defamation under national law.
In conclusion, while BurgerBlast’s comparative advertising campaign *may be permissible in principle, it is lawful only if the comparisons are accurate, substantiated, and presented fairly*. To mitigate legal risks, BurgerBlast should ensure that all claims made are supported by objective data, that the comparison does not mislead consumers, and that the tone of the advertisement does not unfairly undermine TastyBites’ reputation. If any of these conditions are not met, the campaign could be *subject to enforcement action, injunctions, or damages claims*.

Example 3

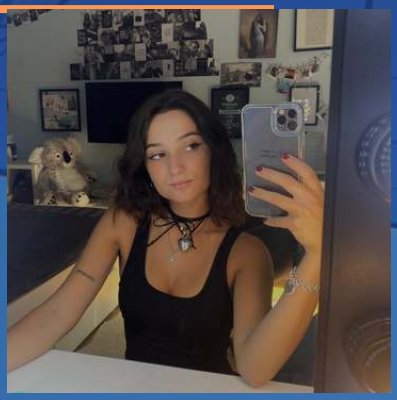
Alfa is a well-known sports footwear brand that signed a sponsorship agreement with the football player AUA for 2023 and 2024. The contract stipulates that AUA must always wear Alfa shoes in public and that, during 2023, he is to participate in three events of the “Alfa Sport Tour," in addition to a series of promotional activities on both Alfa's and AUA's social media channels.
In October 2023, Alfa's CEO becomes aware of the following:

- some photographs published in a gossip magazine showing AUA at a private party at his home wearing Beta shoes;
- the fact that AUA failed to attend the September 2023 "Alfa Sport Tour" event, while on the same day posting a livestream on his social media as he strolled through downtown Milan
- the fact that AUA tested positive in an anti-doping test conducted in August 2023.

The scenario involving Alfa and the football player AUA raises multiple legal and contractual concerns, primarily related to breach of contract, reputational risk, and potential termination for cause. Firstly, the incident in which AUA is photographed wearing Beta shoes at a private party may constitute a breach of the exclusivity clause in the sponsorship agreement. The contract requires AUA to "always wear Alfa shoes in public," and although the party occurred in a private setting, the subsequent publication of photographs in a gossip magazine arguably rendered the situation public. Courts or arbitrators may interpret “public” as including any context where the athlete's image becomes accessible to the public, especially if media coverage is foreseeable. In this sense, the act may undermine Alfa’s brand visibility and exclusivity expectations, constituting at least a minor breach of contract. Secondly, AUA’s failure to attend a scheduled event of the “Alfa Sport Tour,” combined with a social media livestream on the same day, is a more significant breach. His absence not only violates a specific obligation (participation in a required promotional event) but also publicly signals a lack of engagement with Alfa’s campaign, potentially harming the brand’s image and diminishing the value of the sponsorship. This failure may be considered a material breach, particularly given the deliberate choice to engage in an unrelated public activity

at the same time. The most serious issue is the revelation that AUA tested positive in an anti-doping test in August 2023. Although the sponsorship contract’s specific moral or conduct clauses are not detailed, most endorsement agreements of this nature include provisions allowing for termination in cases of conduct that could damage the sponsor's reputation. A positive doping test significantly tarnishes an athlete’s public image and may, by association, harm Alfa’s brand. This incident, especially when combined with prior breaches, could serve as a valid basis for immediate termination of the agreement for cause. It also opens the door for Alfa to seek damages, particularly if the company's brand image or promotional campaigns have been measurably impacted. In conclusion, AUA's actions appear to involve multiple breaches of the sponsorship agreement, ranging from potentially minor to materially serious. Alfa would be justified in initiating formal action, which may include demanding specific performance, seeking damages, or unilaterally terminating the contract based on a material breach or moral clause violation. The cumulative nature of the breaches strengthens Alfa’s legal position and highlights the importance of including clear, enforceable clauses in sponsorship agreements related to exclusivity, public conduct, and reputational harm.

FOR DOUBTS OR SUGGESTIONS ON THE HANDOUTS



CAMILLA BASTIA

camilla.bastia@studbocconi.it

@camiibastia

+39 3457148300

FOR INFO ON THE TEACHING DIVISION

VITTORIA NASONTE

vittoria.nasonte@studbocconi.it

@_vittorian_

+39 3274441476

ELENA CACIOLI

elena.cacioli@studbocconi.it

@elenacaciolii_

+39 3928931605

TEACHING DIVISION

OUR PARTNERS

Wall Street English®

TEGAMINO'S

ETHAN
SUSTAINABILITY

700+
CLUB

DELIVERY VALLEY
NO GENDER KITCHEN

LA PIADINERIA

LA PIADINERIA
dal 1994