



ALLIURIS ACADEMY | SUMMER SCHOOL 2021

DIGITAL MARKETS & LAW

VIRTUAL, 19 - 23 JULY 2021

ORGANISED BY HERFURTH & PARTNER, HANOVER

Alliuris Summer School

19 – 23 July 2021

Digital Markets & Law

Digital business and policies, data protection and ownership, international intellectual property and trade mark protection

ALLIURIS ACADEMY
SUMMER SCHOOL 2021

Alliuris Academy Director:
Giuseppe Cattani, Avvocato,
FDL Law, Milan

Summer School Director and Moderator:
Prof. Dr. Christiane Trüe, Professor, University Bremen
Counsel to Herfurth & Partner, Hannover

Organisation & Conference Management:
Alisha Daley-Stehr, Alliuris Hannover / Brussels

Concept & Supervision:
Ulrich Herfurth, Rechtsanwalt,
Herfurth & Partner, Hannover/Brussels
Alliuris Chairman / CEO

Published by ALLIURIS A.S.B.L.
Avenue des Arts 56,
B-1000 Brussels / Belgium
Fon ++49 511 30756-0
Fax ++49 511 30756-10
Mail info@alliuris.org
Web www.alliuris.org

Editor: Ulrich Herfurth
Layout: Alliuris

The Alliuris Summer School

The Summer School 2021 took place from 19th to 23rd July. As the Covid-19 pandemic is still lasting, it was again not possible to organise a traditional Summer School for young lawyers. But Alliuris has picked up last year's success and organised a virtual conference which was hosted by Herfurth & Partner.

This year, Prof. Dr. Christiane Trüe, professor at the Bremen University of Applied Sciences, was the Director of the Summer School. She could welcome speakers from China, Italy, UK and Germany. Their presentations focused on IP & IT law and current legal developments around digitisation – thereby, not only practical know-how was shared by experienced lawyers, but also new developments were highlighted. The young lawyers got an update on data protection law with a focus on cookie consent, learned about trade mark protection in Europe and IP protection as well as legal proceedings in China. The topics Non-Fungible Tokens and data ownership were not only presented but the attendants had the chance to discuss them with the speakers afterwards.

Together with the Summer School, a new section of the website was launched for the first time this year where speakers and attendants could find all information around the Academy as well as the presentations and additional reading materials.

Although the personal contact and exchange cannot be replaced by a virtual meeting, Alliuris is aimed to still provide knowledge to its young lawyers in these difficult times. All subjects and materials are collected in a report again and published like it was already done for the Summer School 2020. We hope that this is another helpful stepstone for our young lawyers and helpful information for our member firms.

Many thanks to all who have contributed as speakers and organizers to the program and the online sessions and have helped to make the Alliuris Summer School again a success!

Hannover / Milan, July 2021

Ulrich Herfurth

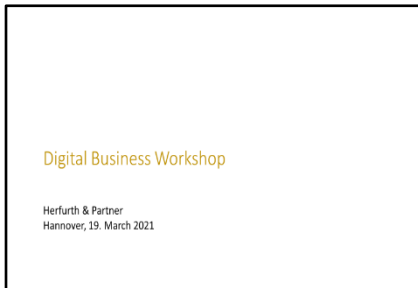
Chairman of the Board

*Giuseppe Cattani
Academy Director*

*Prof. Dr. Christiane Trüe
Director Summer School 2021*

Overview

Introduction to Digital Business



Ulrich Herfurth from Herfurth & Partner in Hanover started this year's Summer School by briefly introducing the participants to "Digital Business". First, he gave an overview of the main hard and soft resources involved in the business, such as microchips, cloud services, super-computers, open-source software, and artificial intelligence. Furthermore, he explained that the concept of digital business is not only relevant for trade and e-commerce, but also for different branches, i.e., finance, en-

ergy, and health. Due to the complexity and continuous innovation of digital business, its legal framework involves a variety of issues where legal advice is needed, such as IP legal protection, data ownership, fair trade and competition law and data protection and security.

European Digital Policies and US Digital Policies

Big tech companies have a lot of power in the digital markets. Google, for examples, retains a market share of about 87% worldwide and 95% in the USA for general search services. Ulrich Herfurth explained to the participants the issues imposed by the dominance of these companies, and how new regulations are necessary to ensure fair play in the digital markets. The speaker updated the young lawyers on the current proceedings of the European

Commission against GAFAM and the digital policies of the EU, such as the drafts of the Digital Markets Act, the Digital Services Act, and the Data Governance Act, while familiarizing the non-EU participants with the legal system of the Union. He then gave the word to Sara Nesler from Herfurth & Partner, who summarized the main antitrust proceedings against GAFAM in the USA and introduced the local legislative development. Afterwards, Ulrich Herfurth depicted the situation in Germany, where the Act against Restraints of Competition (GWB) was recently amended to include the concept of "paramount significance across the markets".



NFTs (Non-Fungible Tokens)



On the second day of the Summer School, Noor Kadhim from Armstrong Teasdale in London introduced the young lawyers to Non-Fungible Tokens. She described their nature by breaking down the concept and explaining the functioning of a blockchain and the characteristics of digital assets and nonfungible property. As certificates of ownership for a digital asset, NFTs can be sold and traded and can be used for a variety of purposes, i.e., tickets, gaming, fashion and collectibles, the latter being currently their primary use. Here, the value an NFT comes from the collectability of the asset, as well as its potential future sale value, which ranges from the triviality of Cryptokitties to multimillion-dollar digital art. While having much potential in the digital art market and possibly other fields, NFTs present some disadvantages, such as the high energy consumption of the blockchain technology. The use of NFTs also involves legal issues, especially concerning data storage and hosting, intellectual property, electronic theft, royalties, and data protection law.

Data Ownership



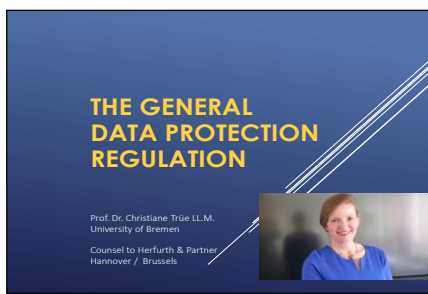
Prof. Dr. Christiane True from Herfurth & Partner introduced the concept of data ownership as a legal right over a single piece or set of data. She asked the participants to reflect on the concept of ownership, the difference between data ownership and protection, and who the owner of data should be. Prof. Dr. True also gave an overview on the applicable European and German law, on the contrasting interests that are involved and on the need for an update of the regulations. The young lawyers were then divided into groups and asked to compare the protection of databases in their home countries and to discuss the balancing of interests undertaken in EU Directive 96/9/EC on the legal protection of databases. During the breakout session, the participants also had a chance to virtually meet the colleagues from other countries.

Data Protection Update International – Understanding Cookies Consent

The third day of the summer school started with a guest speech on Cookies Consent by Constantin Herfurth from Eversheds Sutherland in Munich. After a brief introduction to the different types of cookies and the law applicable to cookies consent, Constantin Herfurth explained in depth the requirements, such as “agree” and “freely given” that a request for non-essential cookie needs to meet. Doing so, he took a practice-oriented approach, presenting the participants with real examples and explaining how, due to unclear regulations, legal advice on cookies often involves weighing out the risks of a non-or partial compliance.



Data Protection - National

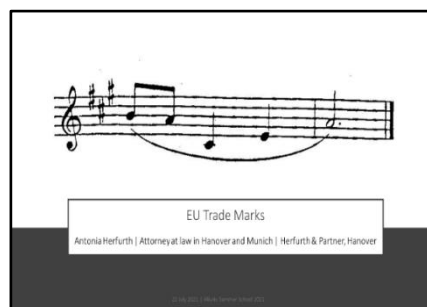


Prof. Dr. Christiane True offered the young lawyers an overview on the “General Data Protection Regulation” of the EU, emphasizing that in the current times, understanding data protection is like nailing a jelly to the wall. The GDPR finds direct application in the Member States, but being supplemented by State legislation, the legal framework is slightly different throughout the EU. After depicting the scope of application of the regulation, Prof. Dr. True defined the concepts of personal and sensitive

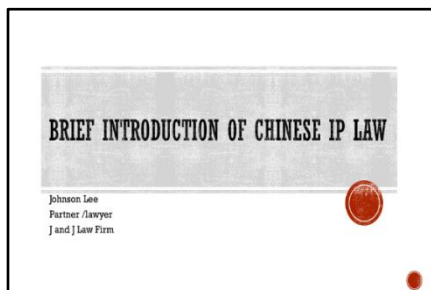
data and described the three principles of data protection embodied in art. 5 (1) GDPR. Particular attention was given to the conflicting basic rights/ human rights and the procedural and institutional protection of data. After the presentation, the participants were divided in groups for a breakout session. The discussion topics were: the balance of privacy and data protection against the rights to information and commercial activity and the adequacy of the existing laws on the matter, the procedural instrument for data protection, and how far the aims of the GDPR, such as better data access, more control for data subjects, and cross-border co-operation have been achieved.

IP & IT Information Websites, Trade Mark Protection in Europe

Antonia Herfurth from Herfurth & Partner in Hanover started her speech by providing the young lawyers with useful research sources on IP & IT law in the EU and worldwide. Thereafter, she introduced the participants to EU trade marks, which cover the entire territory of the EU and can only be registered when a sign is capable of being a trade mark in all Member States. After describing the requirements that a sign must meet to be registered as an EU trade mark, including e.g. distinctiveness and non-descriptiveness, the speaker focused on the opposition to a trade mark and its cancellation. Antonia Herfurth also offered the participants a practice-oriented overview of possible legal actions, from a mild warning letter to a civil action (preceded by a preliminary injunction, if provisional legal protection is needed) and up to an action before a criminal court in case of counterfeiting and piracy activities.



Legal Basis of Intellectual Property Protection in China



Johnson Lee from J & J Law Firm in Guangzhou introduced the participants to Chinese IP law, including aspects of Chinese Patent Law, Copyright Law, Trade Mark Law and Anti-unfair Competition Law. Beginning his speech, Johnson Lee empathized that international conventions, such as the TRIPS Agreement, had an important role in the amendment of Chinese IP law. This provided the country with a modern legal framework, whose main structures

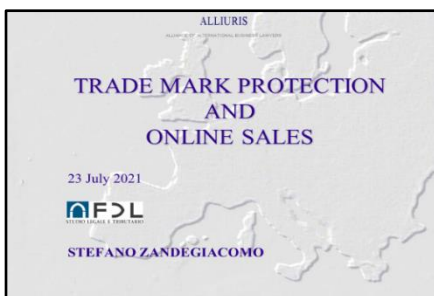
resulted familiar to the young lawyers and that ensure a strong degree of protection. For example, the right holder can be entitled to damages up to five times the actual loss suffered from an infringement of his IP rights. Furthermore, the speaker explained how additionally to civil and criminal law, the administrative authority plays an important role in the protection of intellectual property in China.

Dispute Resolution in China, Litigation and Arbitration

On the last day of the summer school, Roland Huang from J & J Law Firm in Guangzhou gave the participants an overview on the settlement of international trade disputes in China. He started by describing the pro and contra of the conciliation and mediation processes. Thereafter he described the Chinese court system, which is based on four levels, and the local arbitration systems. The speaker pointed out to the young lawyers the main advantages and disadvantages of both options, focusing on the Chinese peculiarities. A choice should be made based on a case specific approach: for big cases against a powerful company that would be likely to be heard in a small city in China's interior, Roland Huang advised to resort to arbitration. On the other hand, a Chinese court would be the better option if particular remedies are needed.



Trade Mark Protection and Online Sales



Stefano Zandegiacomo from FDL – Studio legale e tributario in Milan updated the young lawyers on the protection of trade mark rights against original products sourced from outside of the EU/EEA. This is based on the “trade mark territoriality” principle of EU trade marks and the “legitimate reasons” preventing the exhaustion of Trade Mark rights. He explained to the participants the role played by a selected distribution system in the protection of the image of luxury goods. He also described the requirements and restrictions that can be imposed on distributors who wish to sell a given product online, i.e., using solely their own online store. In the end of the presentation, he also presented other legitimate reasons preventing the exhaustion of TM rights, such as the manipulation of batch codes and products' identification codes.

Trade Mark Quiz and Virtual Toast



The Summer School ended with an interactive and fun trade mark quiz, in which Antonia Herfurth tested the participants' understanding of EU trade marks with well-known or peculiar examples, such as the Lindt bunny.

The participants also had the chance to get together for a virtual toast, hoping to be able to meet in person soon and enjoy once again the social component of the event.



ALLIURIS ACADEMY

SUMMER SCHOOL 2021
19 - 23 JULY 2021

ORGANISED BY
HERFURTH & PARTNER, HANNOVER





The speakers and organizers of the Summer School 2021

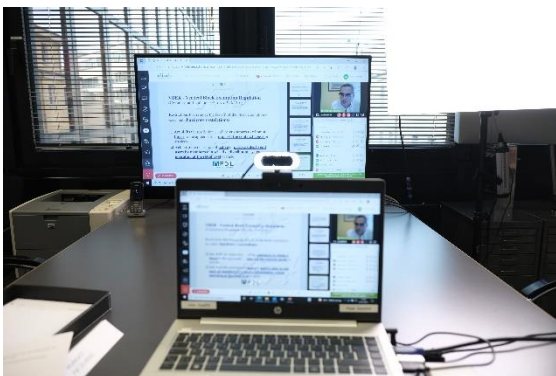
Herfurth and Partner in Hanover organized the conference

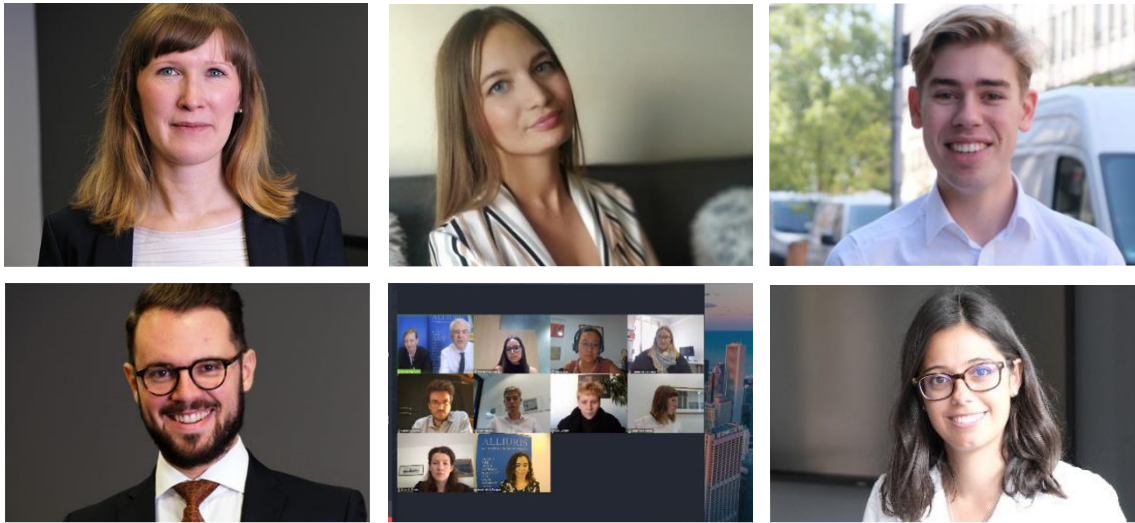




Behind the scenes of the Summer School

The direction





Young Lawyers from China, USA, Argentina, UK, Italy, Spain, Croatia, Iran, Germany, Mexico, Brazil, and the Netherlands attended the Summer School

Virtual Toast at the end of the Summer School



Report

Contents

I. Chapter One – Introduction to Digital Business

1. **Presentation**

(Ulrich Herfurth | Herfurth & Partner)

II. Chapter Two – European Digital Policies and US Digital Policies

1. **Presentation**

(Ulrich Herfurth | Herfurth & Partner)

2. **Q&A**

2.1. How has competition law in your country developed with respect to digital market practices?

2.2. Which legal instruments does the law provide in your country against misuse of market power?

3. **Materials**

3.1. The EU Digital Services Act

Compact, August 2021 *(Antonia Herfurth & Sara Nesler | Herfurth & Partner)*

3.2. The EU Digital Markets Act

Compact, December 2020 *(Ulrich Herfurth | Herfurth & Partner)*

3.3. Trading Platforms and Competition

Compact, April 2021 *(Sara Nesler | Herfurth & Partner)*

3.4. Overview of the current antitrust proceedings of the European Commission

July 2021 *(Sara Nesler | Herfurth & Partner)*

3.5. USA – Overview of the proposed Digital Market Antitrust Policies

July 2021 *(Sara Nesler | Herfurth & Partner)*

3.6. USA – Overview of current antitrust proceedings

July 2021 *(Sara Nesler | Herfurth & Partner)*

III. Chapter Three – NFTs (Non-Fungible Tokens)

1. Presentation

(Noor Kadhim | Armstrong Teasdale)

IV. Chapter Four – Data Ownership

1. Presentation

(Prof. Dr. Christiane Trüe | Herfurth & Partner)

2. Q&A

2.1 Are there discussions on data ownership in your country? Please give your opinion: arguments in favour and against.

3. Materials

Data rights and data use – Who shall own the data?
White Paper, Mai 2018 *(Ulrich Herfurth | Herfurth & Partner)*

V. Chapter Five – Data Protection Update International – Understanding Cookies Consent

1. Presentation

(Constantin Herfurth | Eversheds Sutherland)

2. Materials

2.1 The new EU law for data and services
Compact, September 2021 *(Jan Weber | Herfurth & Partner)*

VI. Chapter Six – Data Protection (National)

1. Presentation

(Prof. Dr. Christiane Trüe | Herfurth & Partner)

2. Q&A

- 2.1 Does a Data Protection Act or any other data protection law exist in your country?

VII. Chapter Seven – IP & IT Information Websites

1. Presentation

(Antonia Herfurth | Herfurth & Partner)

VIII. Chapter Eight – Trade Mark Protection in Europe

1. Presentation

(Antonia Herfurth | Herfurth & Partner)

2. Q&A

- 2.1. What kind of infringement of IP rights are most common and/or significant in your country?
- 2.2. What are the biggest challenges with regard to data protection in your country?

3. Materials

- 3.1. The European Copyright Reform
Compact, April 2019 *(Antonia Herfurth | Herfurth & Partner)*

IX. Chapter Nine – Legal Basis of Intellectual Property Protection in China

1. Presentation

(Johnson Lee | J & J Law Firm)

2. Materials

- 2.1. Data Protection in China
Compact, December 2021 *(Jennifer Feng | J & J Law Firm)*

X. Chapter Ten – Dispute Resolution in China, Litigation and Arbitration

1. Presentation

(Roland Huang | J & J Law Firm)

XI. Chapter Eleven – Trade Mark Protection and Online Sales

1. Presentation

(Antonia Herfurth | Herfurth & Partner)

2. Materials

2.1 International Trade Mark Protection

Compact, February 2021 *(Aline Kristin Pehle | Herfurth & Partner)*

XII. Chapter Twelve – Trade Mark Quiz

1. Presentation

(Antonia Herfurth | Herfurth & Partner)

Chapter One

Introduction to Digital Business

Digital Business Workshop

Herfurth & Partner
Hannover, 19. March 2021

1

Hard Resources

- Microchips
- cloud services
- Mobile devices, hardware
- Supercomputers
- Quantumcomputer
- Net 5G
- Net broad band, glas fibers
- chip design, services for production
- IT / data security
- Supply contracts
- Development projects
-
- Campus Nets
- Grid planning / establishment

2

Soft Resources

- Open Source Software
- Software as a Service
- Platform Business
- Artificial Intelligence
- Data Mining
- Licence contracts
- Services contracts
- Use /sharing contracts
- Development projects
- Orders

3

Digital Business

- Trade, e-Commerce
- Services
- Finance
- Information
- Mobility
- Energy
- Health
- Entertainment, Education
- Sales contracts
- Services contracts
- Finance transactions
- Use / Licence Contracts
- Sharing, Infoservices, Logistics
- Net management,
• diagnosys, treatment, medication
- Copyright, licenses

4

Legal Framework

- Compliance
- Regulatory
- Fair trade / competition
- IP legal protection
- Criminal law
- Sovereignty
- Data ownership
- Copyright in software
- Copyright in pictures, sound, text
- IP rights of data bases
- Patents
- Business secrets

5

Legal Framework

- Data Protection
- DP statements
- DP policy
- DP management
- DP disaster plan
- Data security
- Technical Norms & Standards
- Organisation
- People, social engineering
- Contractual protection

6

Chapter Two

European Digital Policies and US Digital Policies

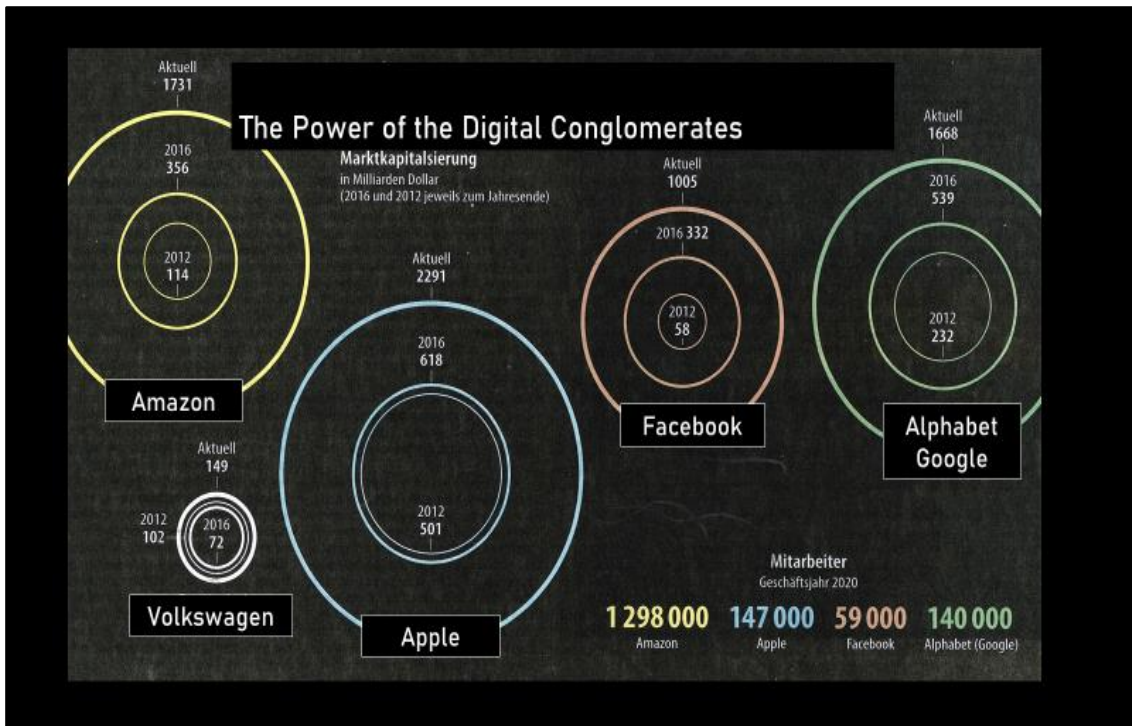
DIGITAL MARKETS

1

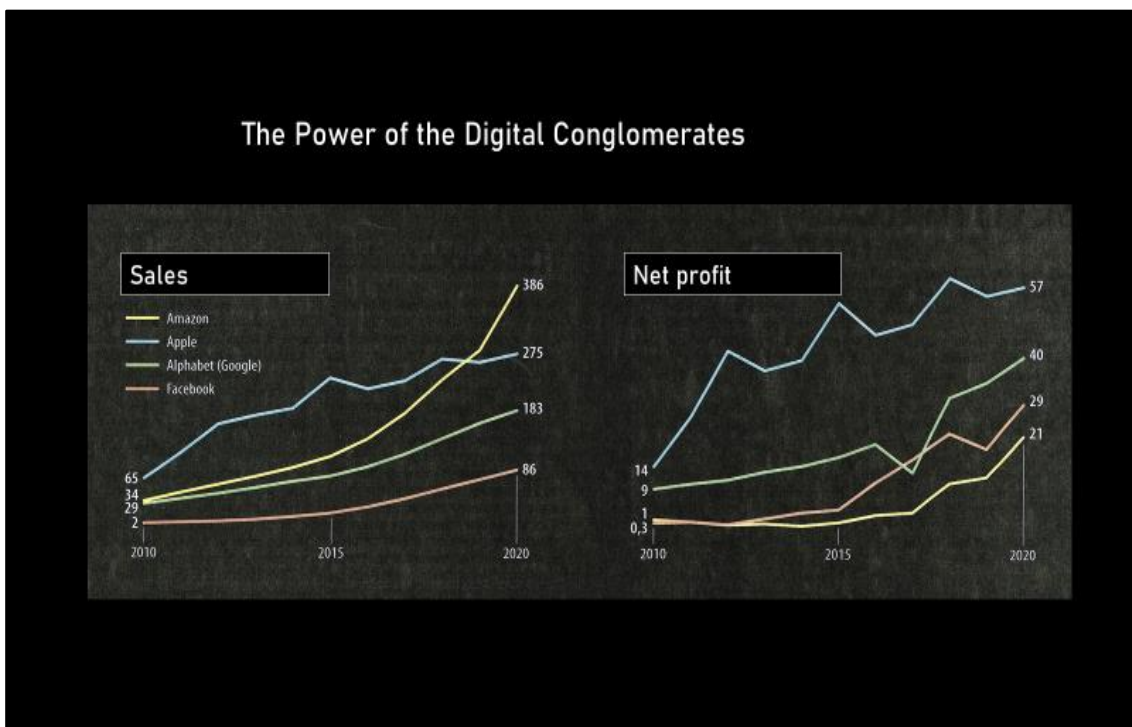
FAIR PLAY IN DIGITAL MARKETS

ALLIURIS ACADEMY | SUMMER SCHOOL 2021 | ONLINE

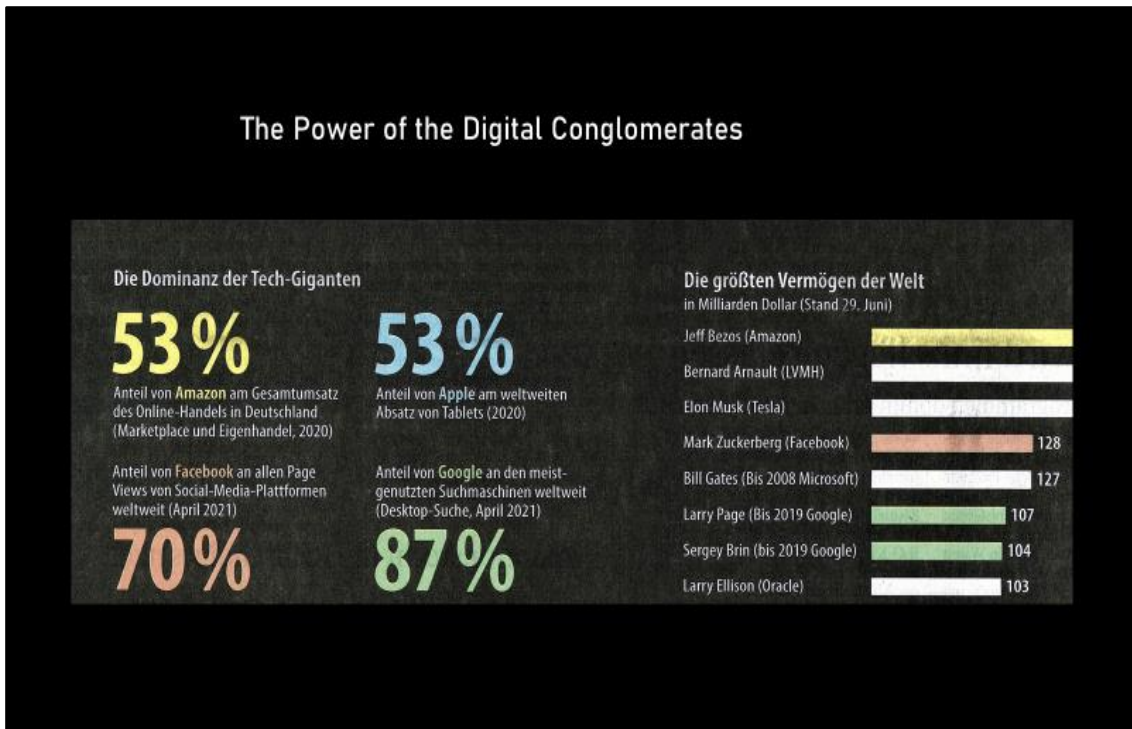
2



3



4



5



6

The Power of Law.

A photograph of Lisa Khan, a member of the US Federal Trade Commission, speaking at a podium. She is wearing a blue blazer and has her hands raised in a gesture. In the background, other people are visible, some wearing face masks. An 'AP' logo is in the bottom right corner of the photo.

Lisa Khan | US Federal Trade Commission

7

The Power of Law.

The flag of the European Union, featuring twelve gold stars arranged in a circle on a blue background.

- European Commission vs GAFAM
- Digital Market Policy of the EU

8



The Power of Law.

European Commission vs GAFAM

- Google, price comparison system
- Google, Android System
- Google, Adsense advertising
- Apple, music streaming
- Apple, E-Books, audiobooks
- Apple, Apple Pay
- Amazon, Buy Box
- Amazon, Market Place
- ...

9



The Power of Law.

The European legal system

- **Green Paper, White Paper:** policy, concept
- **Directive:** legal framework act, to be implemented by the member states in national law by national acts; if not implemented in due time, the EU directive might have direct effect in such member state
- **Regulation:** legal act of the EU, with direct effect in the member states, no room for national law in the same matter, except when opening clause in the Act allows so for specific details

10



The Power of Law.

Digital Market Policy of the EU

- General Data Protection Regulation | in force
- EU Copyright Directive | in force
- Digital Markets Act | draft act
- Digital Service Act | draft act
- Data Governance Act | draft act
- White Paper on AI
- AI Regulation | draft act
- Fairness & Transparency Regulation
- E-Commerce Regulation | in force
- E-Privacy Regulation | draft act
- Algorithms

11



The Power of Law.

Digital Market Policy of the EU

- **General Data Protection Regulation (GDPR)**
in force, was to be implemented until May 2019, market principle:
applicable to any data processor who is active in the EU territory,
processing of personal data prohibited except for specific reasons, inter
alia (Art. 6a GDPR):
 - fulfilment of legal / contractual obligations
 - Written consent of the individual
 - Specific interest of the processor, prevailing the interest of the individual

12



The Power of Law.

Digital Market Policy of the EU

EU Copyright Directive
in force and to be implemented until June 2021,
platforms are liable for avoidable IP infringements by the content published on the platform, obligation to control uploads (major platforms) >> upload filters ?

- Under German law non-essential copies are now allowed without compensation
 - 160 signs of a text
 - 15 sec of sound, video, movie
 - 125 kb of a picture / graphics

13



The Power of Law.

Digital Market Policy of the EU

Digital Markets Act
draft act of January 2021, intended to control market power in the digital markets: big platforms are gatekeepers to services and amounts of data, they cut off competitors from such resources.

- defined profile of gatekeepers specific obligations for gatekeepers regarding the data
- regulatory competence of the EU Commission (pro-active approach)
- somehow parallel instrument to competition law (re-active approach)

14



The Power of Law.

Digital Market Policy of the EU

Digital Service Act
draft act of November 2020, intended to control service providers

- the privilege of the providers (they are in principle not liable for content) shall be limited
- providers shall no longer be subject to their home jurisdiction but to the EU jurisdiction (market principle)
- member states may control/restrict the business of providers
- the services of big providers shall be interoperable with services of other providers

15



The Power of Law.


Digital Market Policy of the EU

Data Governance Act
draft act of January 2021, intended to open the access to big data,

- main idea is to introduce new organisations as data trustee, hosting big data in a kind of escrow, available to the public and not only to commercial (paying) users
- data trustees must not trade as data brokers or as other commercial entities

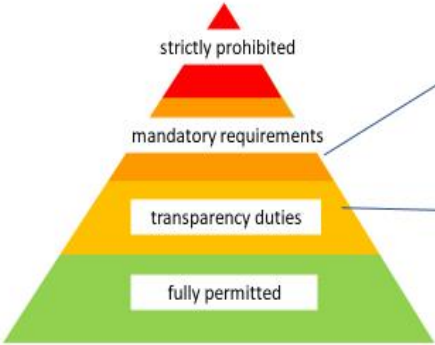
16

The Power of Law.



Digital Market Policy of the EU

Artificial Intelligence



strictly prohibited

mandatory requirements

transparency duties

fully permitted

AI-System: risk management system, quality of data, security, human control
Provider: quality management system, evaluation of conformity, documentation
User: designated use, supervision

Information or notice when interaction with AI-system is not visible

17

The Power of Law.



- Antitrust vs GAFAM
- Digital Market Policy of the USA

18




The Power of Law.

Antitrust vs GAFAM

- Antitrust Division vs Alphabet (Google)
- Federal Trade Commission and 48 States vs Facebook
- Epic Games vs Apple
- Epic Games vs Google
- District of Columbia vs Amazon

19



The Power of Law.


Antitrust vs GAFAM

Alphabet (Google)

The Antitrust Division filed a lawsuit against Google for the abuse of its monopoly power (95% of market shares for general search services on mobile devices in the USA). Through distribution and incentive agreements with the phone makers, Google ensures its status as the default search provider on most devices, preventing other developers from reaching a competitive scale. Similar dynamics are taking place in the development of the Internet of Things.

20

The Power of Law.



Antitrust vs GAFAM

Apple and Google
Epic Games sued Apple and Google for the removal of the game "Fortnite" from their app stores. Epic had intentionally violated the terms of its developer agreement by implementing a payment system that allowed players to bypass the app stores (and their 30% share). The company accuses Apple and Google of exploiting their market power and denying the consumers access to better prices and greater product choice and innovation. A decision is expected in July 2021.

21

The Power of Law.



Antitrust vs GAFAM

Apple and Google
Epic Games sued Apple and Google for the removal of the game "Fortnite" from their app stores. Epic had intentionally violated the terms of its developer agreement by implementing a payment system that allowed players to bypass the app stores (and their 30% share). The company accuses Apple and Google of exploiting their market power and denying the consumers access to better prices and greater product choice and innovation. A decision is expected in July 2021.

22

The Power of Law.



Antitrust vs GAFAM

Amazon

The District of Columbia has sued Amazon, for anticompetitive practices in its treatment of third-party sellers on the platform. Sellers are not allowed to offer their products at a lower price on other platforms or their own websites. Through this policy Amazon fixes the online retail prices, to the disadvantage of the consumers.

Traditional understanding of antitrust, based on consumers and prices.

23

The Power of Law.



Digital Market Policy of the USA

- Ending Platform Monopolies Act
- Platform Competition and Opportunity Act
- Merger Filing Fee Modernization Act
- American Choice and Innovation Online Act
- Augmenting Compatibility and Competition by Enabling Service Switching Act (ACCESS Act)

24

The Power of Law.



Digital Market Policy of the USA

Ending Platform Monopolies Act
Promote competition in digital markets by eliminating conflicts of interest arising from simultaneous ownership or control of platforms and other companies.

25

The Power of Law.



Digital Market Policy of the USA

Platform Competition and Opportunity Act
Aims to generally forbid the acquisition of shares or assets of persons engaged in or affecting commerce through platform operators. Exceptions are in place through section 7A(c) of the Clayton Act, or if the platform operator proves that the assets or shares are not in a competitive relationship with the platform and the acquisition does not improve or help maintain its market position.

26

The Power of Law.



Digital Market Policy of the USA

Merger Filing Fee Modernization Act
Promotes antitrust enforcement by adjusting the merger filing fees and increasing antitrust enforcement resources.

27

The Power of Law.



Digital Market Policy of the USA

American Choice and Innovation Online Act
Prevents discriminatory behavior by covered platforms among business users and promotes a fair relationship between platforms and business users.
The measures regard self-preferencing behaviors, the interoperability and interdependence of services, the usage of data, the preinstallation of applications, the communication among business-users and costumers and the pricing policies.

28

The Power of Law.



Digital Market Policy of the USA

Augmenting Compatibility and Competition by Enabling Service Switching Act (ACCESS Act)
Regulates the interportability and interoperability of the platform's data and their security, imposes information requirements and limits the collection and usability of data in order to promote competition and lower entry-barriers for consumers and online businesses.

29

The Power of Law.



- Federal Cartel Office vs GAFAM
- Digital Market Policy in Germany

30



The Power of Law.

Federal Cartel Office vs GAFAM

- Facebook: data protection under market dominance, Oculus
- Apple: extensive integration among market levels, App Store
- Amazon: price control, agreements with brand manufacturers, cross-market power
- Google: data usage, consumers choice

31



The Power of Law.

Federal Cartel Office vs GAFAM

Facebook

The Federal Cartel Office sues Facebook for misuse of market power: like no other social media platform Facebook collects the consent of its users to the processing of their personal data, just because the users in practice have no choice. The Higher State Court has refused the claim (arguing that this is a matter of data protection, not of competition law), the Federal Supreme Court has stated that it accepts the view of the Cartel Office.

32

The Power of Law.

Federal Cartel Office vs GAFAM

Procedures under section 19a GWB

The Federal Cartel Office has recently initiated two-step procedures against Facebook, Apple, Amazon and Google under the newly introduced regulations. The Office is i.e. examining the linkage between Facebook and Oculus (virtual reality products). The use of the company's latest virtual reality glasses requires registration using a facebook.com account.

33

The Power of Law.

Digital Market Policy in Germany

- Competition Act (Act against Restraints of Competition / GWB)
9th Amendment 2018
- Competition Act (Act against Restraints of Competition / GWB)
10th Amendment 2021
- Unfair Trade Law
- Civile Code
- Copyright Act
- Media State Convention

34



The Power of Law.

Digital Market Policy in Germany

**Competition Act (Act against Restraints of Competition / GWB)
9th Amendment 2018**

introduced inter alia a new concept for merger control, in order to avoid killer acquisitions of new technology start-ups by big players:

- while the classic element for the importance of an acquisition was the turnover of the target, now the purchase price for the target is also a reason for a review by the cartel office

35



The Power of Law.

Digital Market Policy in Germany

**Competition Act (Act against Restraints of Competition / GWB)
10th Amendment 2021**

introduced inter alia a new concept for the assessment of market dominance: the *cross-market importance* of a player (Art. 19a GWB) i.e. dominant position in market A may lead to a new dominance in market B.

- A player of *cross-market importance* is subject to similar control as a market dominating player with regard to a misuse of its dominant position

36

Thank you for listening to

FAIR PLAY IN DIGITAL MARKETS



Ulrich Herfurth
Attorney at law
Hannover / Brussels

With the support of
Sara Nesler

www.herfurth.de

ALLIURIS ACADEMY | SUMMER SCHOOL 2021 | ONLINE

37

Questions and Answers

Competition in the Digital Markets

1. How has competition law in your country developed with respect to digital market practices?

Cheril (China):

In the development process of the Anti-Unfair Competition Law, there is no clear legal provision on the relevant behaviors of the digital market. The Law is mainly a behavioral regulation law (regulating unfair competition behavior), not a power law (giving operators the right to be protected from unfair competition behavior infringement). Its main legislative purpose and function is to regulate unfair competition, so as to guide market competition subjects to compete fairly, and ultimately establish a fair and healthy market competition order. Most of the cases related to the digital market in China are handled through Article 2 of the Anti-Unfair Competition Law. Article 2 is a general clause of the Anti-Unfair Competition Law. The application of the general clause should meet the following three requirements: First, the law does not make special provisions for this type of competition. Second, the lawful rights and interests of other business operators have been actually damaged due to the competition, Third, This kind of competitive behavior is improper or liable because it violates the principle of good faith and recognized business ethics.

Wenzhu Lan (China):

Firstly, I am so sorry so late to return you for i need to search. Secondly, since digital market have flourished over the past 20 years. In 2014, more company believe that as long as you occupy the digital market you can gain an advantage in the competition. From the concept of economics, "digital platforms" can be regard as intermediaries connecting two or more user groups, which benefit from each other' s direct or indirect network effect, And through a number of different but clearly identified user groups to form two-sided markets or multi-sided markets. In 2014, The Supreme People's court's case of Qihoo company v. Tencent company, it is the first time to have to confront the competition of digital market.

The court deployed on SSNDQ (Small but Significant Non-Transitory Decrease in Quality) and brought to a verdict that the relevant market in this case should be defined as the instant messaging service market in China, including personal computer instant messaging service and mobile instant messaging service not only integrated instant messaging services, but also non-integrated instant messaging services such as text, audio and video. There was "targeted and discriminatory differential treatment. It will make those merchants who have not entered into exclusive transactions with meituan, the dominant one, at a competitive disadvantage in terms of cost, forcing them to enter into exclusive transactions with meituan, and those merchants locked by exclusive cooperation cannot cooperate with other platforms because of restrictions. On the other hand, on March 3, 2021, the State Administration of market supervision and Administration (hereinafter referred to as the market supervision bureau) imposed administrative penalties on five community group buying enterprises for their improper pricing behavior. The State Council's anti monopoly Commission then issued the "anti monopoly guide on the field of platform economy" (hereinafter referred to as the "anti monopoly guide").

Ana Marija Đurić (Croatia):

Competition law in Croatia is regulated through the Act on Protection of Market Competition.

L. Tuncer (Netherlands):

The rise of digital market places does sometimes make the current methods of analyzing competition less useful. Network effects, artificial intelligence and other advantages increase the risk of winnertakes-all. Dominant players can transfer that advantage to other markets and it can lead to monopolies there. There is at European level talk about limiting the power of large social media companies whose influence is immense but not always visible.

Zoë Jardim (Brazil):

In Brazil we have what is called, "Lei Antitruste", it was created by Getúlio Vargas in the period known as Estado Novo (1937 - 1945) when Vargas ran for the Federal Senate of Brazil. This law was created to prohibit foreign capital from buying companies of the same order in Brazil, has the objective of repressing the exercise considered abusive of increasing market power.

2. Which legal instruments does the law provide in your country against misuse of market power?

Cheril (China):

China adopts administrative penalties to regulate the abuse of market dominance, Article 47 of Anti-Monopoly Law of the People's Republic of China stipulates that where the business operators abuse their dominant market position in violation of this Law, the Anti-monopoly Law Enforcement Agency shall order them to stop such violations, confiscate the illegal gains, and impose a fine of 1% up to 10% of the total sales volume made in the previous year.

Wenzhu Lan (China):

The price law, The provisions on prohibiting price fraud, The Interim Provisions on regulating sales promotion, Anti monopoly guide on the field of platform economy, Law of PRC Against Unfair Competition etc.

Ana Marija Đurić (Croatia):

In my country (Croatia) our legal instruments are Regulation (EU) no. 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (Regulation on market abuse) and repealing Directive 2003/6 / EC of the European Parliament and of the Council and Commission Directive 2003/124 / EC, 2003/125 / EC and 2004/72 / EC and delegated acts, implementing acts, regulatory technical standards, implementing technical standards and guidelines adopted in accordance with the Market Abuse Regulation.

L. Tuncer (Netherlands):

Article 102 of the TFEU prohibits one or more undertakings occupying a dominant position in the common market or a substantial part thereof from abusing that dominant position in so far as this abuse restricts competition and affects interstate trade. National cases are handled by the financial markets authority (AFM).

Zoë Jardim (Brazil):

By removing manual processes, adding automated tasks (such as chatbots, targeted advertising, etc.) and improving workflows (with artificial intelligence software), companies are looking to add value to their products and services and stand out in the market. The adoption of technological measures can represent a competitive advantage in the new digital market, with more productivity, less cost, and a better customer experience. In Brazil and most places in the world, data is the asset with the greatest competitive advantage. Because data processing is much faster today than it was 2 years ago, due to the ease of collecting and storing it, thanks to better internet functionality, it can be said that today data holding is the biggest competitive potential of a company.

3. Should unbundling become a legal instrument against monopolies and oligopolistic conglomerates in a dominant market position?

Cheril (China):

Yes, but I don't know much about this, at the end of this training, I hope that I will learn more.

Wenzhu Lan (China):

It could help in infrastructures to break open monopolies and enable competition. However, it is doubtful whether it will help strengthen competition in digital market practices.

Ana Marija Đurić (Croatia):

In Croatia, there are not many discussions over unbundling as a legal instrument against monopolies and oligopolistic conglomerates, since to this day there hasn't been many examples of oligopolistic conglomerates. Although German Competition Act provides for the possibility of ordering structural remedies, including divestitures (unbundling) of companies, in Croatia similar legal instruments do not exist.

L. Tuncer (Netherlands):

It could help in infrastructures to break open monopolies and enable competition. However, it is doubtful whether it will help strengthen competition in digital market practices.

Zoë Jardim (Brazil):

No, I do not believe so. Restrictions and regulations shall be made with monopolies and oligopolistic conglomerates, however, unbundling would be quite a radical decision to so. Free market is very important, but always with legal instruments to control it. I do not see unbundling monopolies as a solution, but maybe giving incentive for small business to grow could be one.

+ + +

Materials | Compact

The EU Digital Services Act

*Antonia Herfurth, attorney at law in Munich and Hanover
Sara Nesler, Mag. jur. (Torino), LL.M. (Münster)*

Hanover, August 2021

In November 2018, the European Commission presented its Digital Strategy for Europe. The aim of the strategy is to strengthen the digital single market and create fair competition, the latter especially vis-à-vis the US digital industry. Single Market Commissioner Thierry Breton made clear: "It's not us who need to adapt to today's platforms, it's the platforms that need to adapt to Europe."

The e-commerce directive from 2000 (RL 2000/31/EC) has so far provided the legal framework for digital services in the EU. It allowed the Internet to develop rapidly over the last 20 years and become what it is today. However, the directive is 20 years old. In 2000, the Big Five - Amazon, Apple, Facebook, Google and Microsoft - were already big, but today they dominate the global market. Furthermore, user behavior on the Internet has changed. Fake news and hate speech are commonplace. To counteract this development, the EU presented a proposal for a law on digital services, the Digital Services Act, as part of its digital law package on December 15, 2020.

Previous legal situation - e-Commerce Directive

The e-Commerce Directive has played a significant role in allowing the development of the internet. Key points of the directive are the formal validity of contracts concluded electronically, the provider privilege, the country-of-origin principle, information obligations for operators of digital services and the prohibition of a general monitoring duty.

Provider privilege

The provider privilege is a liability privilege for digital service providers. The privilege protects service providers from direct liability for content posted by users on platforms, Art. 12-14 e-Commerce Directive. If the provider forwards, transmits or temporarily stores content, only the user is liable, not the provider. The service provider only provides the infrastructure. The service provider is liable only if a user uploads illegal content and the provider does not delete it. This privilege has made it possible for the Internet to become a free communication space.

Country-of-origin principle

The country-of-origin principle regulates that service providers are subject to the law of the country in which they are based and not to the law of the country in which their services are offered, Art. 3 (1) e-Commerce Directive. The country-of-origin principle is a business-friendly regulation. Providers should be able to establish themselves freely within the EU, without barriers. Without the country-of-origin principle, service providers operating across borders would have to take 27 national regulations into account.

Prohibition of a general monitoring obligation

When the EU formulated the e-Commerce Directive, it deliberately decided against a general monitoring obligation, Art. 15 e-Commerce Directive. Service providers are not obliged to constantly and without cause monitor the content uploaded by their users or to actively search for illegal content. Of course, providers must sift through - allegedly - illegal content and delete it if necessary. However, the EU has intentionally not introduced permanent, complicated, time-consuming, and cost-intensive monitoring systems because, according to the EU, this not only inhibits development and is disproportionate, but also changes the character of platforms.

Conflict

Digital services have outgrown the e-commerce directive. Digitization has led to Amazon's market capitalization increasing by more than 1,400% since 2010, and Apple's by 600%. In addition, platforms are used intensively, hate speeches and illegal content are posted, and fake news are spread. So far, there are no European regulations in this regard. Member states are countering this by enacting national laws. In 2017, Germany enacted the Act to Improve Law Enforcement on Social Networks (*Netzdurchsetzungsgesetz*), France in 2020 enacted the Act against Hate Speech on the Net (so-called *Loie Avia*), which, however, was overturned by the French Constitutional Court in the summer of the same year, and in Austria the Communications Platforms Act has been in force since April 2021. The consequence of this is that there is no uniform European legal framework, and therefore no EU supervisory authority, but a patchwork of national regulations with different specifications. Not only are smaller European providers disadvantaged, but it is also more attractive for service providers entering the market to establish themselves in the USA or China.

Future legal situation – DSA

The Digital Services Act (DSA), together with the Digital Markets Act (DMA), is part of an EU legislative package that aims to unify the digital single market, create a control framework, and ensure fair competition. The changes envisaged by the DSA are discussed below. The DMA,

which seeks to combat unfair competition by platforms, is covered in the Compact "The EU Digital Markets Act," December 2020.

The aim of the DSA is to promote fairness, transparency, and accountability in relation to the moderation of digital content, and to ensure respect of fundamental rights and the independence of legal remedies. To this end, the regulations are aimed at providers of intermediary services - pure transit, caching, and hosting - regardless of their domicile. Only the user must be domiciled in the EU.

Provider privilege

Other than originally planned, the provider privilege for transit, caching and hosting will not be abolished. The European Parliament had also spoken out against the abolition. Instead, the provider privilege of the e-commerce directive will be adopted, supplemented by a Good Samaritan privilege for providers acting on their own initiative, Art. 3-5 of the DSA proposal. Service providers are allowed to conduct voluntary investigations but are not obliged to monitor the transmitted or stored information or to actively search for illegal activities, Art. 6 of the DSA proposal. However, there is a duty to cooperate with national authorities in combating illegal content as soon as they adopt a corresponding order.

This solution is a compromise. The lobby had objected that too strict controls and restrictions would inhibit the development of the Internet as in the last decade and restrict freedom of expression through upload filters and overblocking. Overblocking is the unwanted blocking or deletion of lawful content. On the other hand, it was argued that privatized law enforcement is a problem that would only be worsened by the lack of public control. Facebook, Amazon and others decide which content is illegal and which is not. Not only do the service providers apply different standards, but they are also acting as legislators and judges. This task must fall to a public, independent body.

Moderation

Content moderation is to become more transparent in the future. According to the new regulations, service providers must introduce reporting procedures, which should simplify the submission of sufficiently substantiated reports. Reports from trusted whistleblowers, so-called trusted flaggers, will be examined and decided upon as a matter of priority. Trusted flaggers are designated by the Member States based on their expertise, their independent representation of collective interests and the timeliness, diligence, and objectivity of their reports. Whistleblowers who frequently submit obviously unfounded reports are to be blocked for an appropriate period following a warning. This is intended to counteract overblocking.

Fairness and transparency

There should be more transparency regarding the consequences of illegal actions. Users who provide illegal content should be blocked for a reasonable period and the content deleted. The procedure should be clearly and specifically justified. The handling of cases of abuse, the criteria for a decision on such cases and the duration of a suspension must be clearly regulated in the GTCs. If there is suspicion of a criminal act, it must be reported to the competent authorities. To ensure that users can complain about the actions of digital platforms, providers should set up internal complaints management systems; this does not apply to online platforms that are small or micro-businesses. Users should also have the right to act against the platform before an authorized dispute resolution body. In the event of a decision in favor of the user, the platform must pay all fees and other reasonable costs.

Protection of fundamental rights

To promote the protection of fundamental rights, very large online platforms shall assess, at least annually, the systematic risks that exist in the operation and use of their platform. According to Art. 26 of the DSA proposal, special attention is to be paid to the dissemination of illegal content, the negative impact on fundamental rights and the intentional manipulation of services - especially regarding the consequences for public health, minors, civil discourse, election results and public safety. Platforms are required to take measures to mitigate risks. Accordingly, they must designate an internal compliance officer and provide access to data necessary to conduct external inspections of the online platform.

Enforcement

Enforcement of the DSA is to be carried out primarily by the member states. These appoint a so-called digital services coordinator, who is to have investigative and enforcement powers and can issue sanctions, such as fines of up to 6% of annual turnover in the previous fiscal year. However, enforcement of the GDPR has shown that member states often lack the resources to establish EU-style data protection authorities. Contrary to initial assumptions, however, the reform proposal does not include the creation of a Union-level supervisory authority. The new European Digital Services Authority to be established shall have only an advisory role. Instead, the possibility of cross-border cooperation and the involvement of the European Commission have been envisaged, the latter at the request of a Member State or ex officio in the case of very large platforms.

Outlook

The DSA proposal has yet to be discussed by the European Parliament and the member states as part of the ordinary legislative procedure and to be adopted. It will then be directly applicable throughout the EU. This will be the case in 2022 at the earliest.

+ + +

The EU Digital Markets Act

Ulrich Herfurth, attorney at law in Hanover and Brussels

Hanover, December 2020

The European Union's Digital Markets Act introduces rules for platforms that act as "gatekeepers" in the digital sector. These are platforms that have a significant impact on the European single market due to their size and reach. This market power sometimes manifests itself in the fact that corresponding platforms can unilaterally determine the "rules of the game" for their users. Google, Facebook, YouTube and Amazon come to mind. However, the regulation also covers those platforms whose gatekeeper function is only to be feared in the future. Such platforms are often a central interface for communication between companies and their customers.

The Digital Markets Act aims to prevent gatekeepers from imposing unfair conditions on businesses and consumers and to ensure the openness and transparency of important digital services. Examples of these unfair conditions include prohibiting companies from accessing their own data or situations where users are locked into a particular service and have limited options to switch to alternative services ("lock-in effect").

Applicability

The Digital Markets Act will only apply to large companies. The draft regulation that has now been adopted sets objective criteria for identifying "gatekeepers." They must control at least one so-called "core platform service" (such as search engines, social network services, certain messaging services, operating systems, and online intermediary services) and have a persistent, large user base in several EU countries. The Digital Markets Act can thus be seen as a response to the rampant market power of the Internet giants.

Specifically, there are three main cumulative criteria that bring a company within the scope of the Digital Markets Act:

(1) A size that affects the internal market: This is presumed if the company has an annual turnover in the European Economic Area (EEA) of at least €6.5 billion in the last three financial years, or if its average market capitalization or equivalent market value in the last financial year was at least €65 billion, and it provides a central platform service in at least three member states;

(2) The control of a major gateway for commercial users towards end users: this is presumed if the company operates a central platform service with more than 45 million monthly active end users based or located in the EU and more than 10,000 annually active commercial users based in the EU in the last fiscal year;

(3) A (presumably) consolidated and lasting position: this is presumed if the company has met the other two criteria in each of the last three financial years.

If all these quantitative thresholds are met, the company in question is presumed to be a gatekeeper, unless it can prove otherwise. However, a company may also be identified as a gatekeeper by the Commission if it does not (yet) meet all the requirements. Market investigations by the Commission are to take place for this purpose.

Legal consequences for platforms

In the future, gatekeepers will have to behave in a way that ensures an open and fair online environment for companies and consumers. To this end, they must comply with certain obligations set out in the draft legislation, i.e., proactively implement certain behaviors and refrain from unfair conducts.

If a company does not yet have an established and lasting market position, but it is foreseeable that this will be the case in the near future, it must already comply with a certain part of the obligations under the Digital Markets Act. This is to ensure that the gatekeeper in question does not use unfair means to achieve a consolidated and permanent market position in its field of activity.

Duties and prohibitions of gatekeepers

The Digital Markets Act sets forth a list of obligations that gatekeepers must implement in their daily operations to ensure fair and open digital markets. This list is to be continually developed and updated.

Some examples of the obligations include:

- Gatekeepers must provide businesses advertising on their platform with access to the gatekeeper's performance measurement tools and the information necessary to allow advertisers and publishers to conduct their own independent review of their advertising hosted by the gatekeeper;
- Gatekeepers must allow their business users to advertise their offers and enter into contracts with their customers outside of the gatekeeper's platform;

- Gatekeepers must allow their business users access to data generated by their activities on the Gatekeeper platform.

Some examples of prohibitions include:

- Gatekeepers may no longer prevent users from uninstalling pre-installed software or apps;
- Gatekeepers may not use data obtained from their business users to compete with those business users;
- Gatekeepers may not prevent their users from accessing services that they may have purchased outside of the Gatekeeper platform.

Implementation by the Commission

Once the Digital Markets Act is enacted, the Commission will consider whether companies engaged in core platform services qualify as gatekeepers under the regulation:

- (1) companies will have to verify for themselves whether they meet the quantitative thresholds set out in the regulation for identifying gatekeepers. They will then have to provide information on this to the Commission.
- (2) the Commission will then designate as gatekeepers those companies that meet the thresholds of the Regulation, based on the information provided by the companies (subject to possible substantiated rebuttal) and/or following a market investigation.
- (3) within six months after a company is identified as a gatekeeper, it must comply with the obligations and prohibitions set forth in the Regulation. For those gatekeepers who do not yet hold an established and permanent position, but who are expected to do so in the near future, only such obligations shall apply that are necessary and reasonable to ensure that the company does not use unfair means to achieve such an established and permanent position in its operations.

Legal consequences in the event of infringement

To ensure the effectiveness of the new rules, the possibility of sanctions for non-compliance with the prohibitions and obligations is provided for.

If a gatekeeper does not comply with the rules, the Commission can impose fines of up to 10% of the company's total annual worldwide turnover and periodic penalty payments of up to 5%

of the company's total annual worldwide turnover. Fines in the billions are thus theoretically possible. In the case of systematic violations, the Commission may impose additional measures. If necessary to achieve compliance and if no alternative, equally effective measures are available, these may include structural remedies, such as requiring a gatekeeper to sell a company or parts thereof (break-up).

Market investigations

To ensure that the new gatekeeper rules keep up with the rapid pace of digital markets, the Commission will have the power to conduct market investigations. The purpose of market investigations is threefold:

- Identify gatekeepers that are not covered by the quantitative thresholds provided in the Digital Markets Act, or that meet those thresholds but have made a reasonable request that rebuts the presumption based on those thresholds;
- Determine whether additional services within the digital sector should be added to the list of core platform services covered by the regulation or whether new practices are emerging that could have the same adverse effects as those already covered;
- Develop additional remedies if a gatekeeper has systematically violated the Digital Markets Act rules.

Enforcement of the Digital Markets Act

Given the cross-border nature of gatekeepers and the complementarity of the Digital Markets Regulation with the Digital Services Regulation and other internal market legislation, and in particular competition law, enforcement of the instrument will remain in the hands of the Commission. Member States may at any time request the Commission to launch a market investigation for the purpose of designating a new gatekeeper.

Damages

The Digital Markets Act is a regulation that imposes precise obligations and prohibitions on gatekeepers affected by its scope. Once adopted, the regulation is directly applicable in every member state of the EU. This facilitates damages claims by those harmed by the conduct of non-compliant gatekeepers.

Relationship to competition law

The Digital Markets Regulation complements competition law enforcement at the EU and national levels. The new rules are without prejudice to the enforcement of EU competition rules (Articles 101 and 102 TFEU) and national competition rules relating to unilateral conducts. With the Digital Markets Regulation, the Commission aims to be able to take faster and easier action against anti-competitive behavior. By constantly developing the obligations and prohibitions, it should be possible to flexibly stop new practices. Existing competition law is not always sufficiently suited to the fast-paced online world.

Further procedure

The regulation still has to be adopted by the EU Parliament and the member states before it comes into force.

+ + +

Trading Platforms and Competition

Sara Nesler, Mag. iur (Torino)

Hanover, April 2021

Those who want to sell their products online often cannot avoid working with one or more platforms. The relationship between merchants and operators is often problematic due to the market power of some platforms. New developments in legislation and case law put merchants in a better position.

In 2020, a total revenue of EUR 83.3 billion was generated in Germany from the sale of goods online. This represents a growth of 14.6% compared to the previous year. Many retailers rely on the services of platforms to reach potential customers. Their own online stores, if available, do not have good visibility.

Some of these platforms have large market shares in certain sectors or even across markets. For example, Zalando is the online market leader in fashion. According to a study by Handelsverband Deutschland e.V., Amazon achieved a total of 46% of German online retail market share in 2018 via Marketplace (25%) and direct sales (21%). With total German sales of approximately €17 billion, the company generates more than the other nine largest online retailers combined, including Otto and Zalando. By comparison, the eBay platform, which is classified as an online auction house, had global sales of around 10.75 billion.

The advantages for commercial users

The Online presence on certain platforms and the sales generated there are existential for many retailers. A collaboration not only offers the opportunity to increase the visibility of one's own products at low cost, but also other important benefits. For example, with programs such as *Fulfillment by Amazon* or *Zalando Fulfillment Solutions*, retailers have the option of outsourcing merchandise logistics. This means they don't have to worry about the demanding task of meeting specified shipping times. With the *Vendor Central* program, selected merchants are offered the opportunity to sell larger inventories directly to Amazon. This regularly leads to a significant increase in sales because customers show greater trust in products that are not only shipped but also sold by Amazon.

Dependence and loss of control

Nevertheless, caution is advised. If the presence on a particular platform is a central point of the business model, one is tied to the operator. The degree of dependency increases with the proportion of sales volume handled on a platform. The greater the number of services used, the more control over one's own products is lost. If, for example, shipping and returns are left to the platform, control over the packaging of one's own goods as well as customer contact is lost.

Any move that ties a business's success more closely to a particular platform needs to be carefully considered. Merchants invited into Amazon's *Vendor Central* or a similar program should not make the decision of a commitment lightly. The moment merchandise is sold to the platform operator, the operator has control over pricing, regardless of what the manufacturer or merchant thinks. On the one hand, specifications must be adhered to in order to remain in the program. These can be imposed by the strong contract partner even after the contract has been concluded. Voluntary exit from the program, on the other hand, is not readily permitted. In addition, anyone wishing to gain insight into the statistics of the goods sold to the operator must pay for this. The analysis tools included in the basic program are not provided here.

Merchants as customers and competitors of the platform

The situation for merchants is complicated by the fact that many platforms, including Amazon, eBay and Zalando, are vertically integrated, offering both their own goods and those of third-party merchants. This means that commercial users are both customers and potential competitors of the platform.

Based on the data collected, operators can closely monitor which products are particularly successful. Thus, they can decide to invite the retailer or manufacturer to a particular program and, if necessary, exert pressure to get them to accept the offer. However, there are also known cases in which successful retailers have been forced out of the market by price wars, with the platform operator selling identical products from the same source as its own offers.

The fear that the platform's algorithms will disadvantage the products of third-party retailers in favor of their own is therefore well-founded. Also justified is the fear of being excluded from a platform's marketplace or having one's business account blocked without good reason.

Positive developments for merchants

In recent years, this questionable market power attracted the attention of the German Federal Cartel Office, which, through its intervention, achieved, among other things, a change in Amazon's terms and conditions in favor of merchants.

A significant change in competition law has been brought about by the Tenth ARC Amendment (Amendment to the Act against Restraints of Competition), which came into force on 19. 01. 2021. The new Section 19a ARC introduces the criterion of a company's paramount significance for competition across markets. It thus covers spillover effects from one market into other markets, both horizontally and vertically.

The Federal Cartel Office can formally acknowledge the paramount significance for competition and prohibit the company from, among other things:

- favoring its own offers over the offers of its competitors when mediating access to supply and sales markets;

- providing other companies with insufficient information on the scope, quality or success of the service provided or commissioned or otherwise making it difficult for them to assess the value of this service;
- demanding benefits for handling the offers of another undertaking which are disproportionate to the reasons for the demand. In particular, to demand the transfer of data or rights that are not reasonably required for this purpose;
- making the quality in which these offers are presented conditional on the transfer of data or rights which are disproportionate to the reason for the demand.

Section 19a of the ARC does not completely eliminate the problems associated with the vertical integration of platforms. This would require a prohibition on acting simultaneously as a platform and as a merchant in a market, as in the provisions currently discussed in the USA. Nevertheless, it sets important limits for companies with cross-market significance that make it more difficult to exploit their position of power. At the present time, the Federal Cartel Office has started proceedings to investigate the cross-market significance of Facebook, Amazon, Google and Apple.

European and international level

Important measures against the platform's abuse of power are also being introduced at the European level. The EU Commission is conducting proceedings against Amazon for violating European antitrust regulations, especially for the misuse of data. The company faces fines in the billions (up to 10% of the annual global turnover, over EUR 230 billion in 2019). In December, the EU Commission presented a legislative package for the regulation of digital services and digital markets. If this is passed, platforms would be forced to grant commercial users a fairer business environment under threat of heavy fines.

Positive signals are also coming from the U.S.A.: antitrust proceedings for the misuse of third-party data have already been initiated, and five proposed bills addressing antitrust issues in the digital markets are currently in discussion.

These developments are welcome from the perspective of commercial platform users. However, while waiting for further action from the relevant authorities, merchants continue to face existential questions, especially if they are forced out of a market segment or the platform blocks their account.

Can platforms exclude products from certain merchants from the marketplace?

Every company is allowed to conduct its business activities in a way that it deems to be economically reasonable and correct. This means that basically, platform operators are also free to decide which merchant they want to have a business relationship with, and what types of goods can be offered on the platform.

However, this business 'freedom only exists within the limits of competition law. If the operator holds a dominant position in the relevant market, the exclusion of some merchants may constitute an unlawful restriction of competition.

For example, the German district Court of Frankfurt recognized an unfair hindrance of third-party sellers when Amazon became a direct seller of Apple products. As part of the agreement, Amazon deleted all product ads of the brand that did not originate from Apple-authorized resellers. As a result, only Amazon's own listings and those of two other authorized resellers remained on the platform. The illegality of the exclusion is here independent from the admissibility of the agreement, which is being investigated by the Federal Cartel Office.

If a similar constellation exists, it may be worthwhile to seek injunctive relief. Compensation for lost profits may also be considered.

When can the operator block or terminate a business account?

If there is a concrete indication that the merchant, by using the platform, violates the rights of a third party, the operator has the obligation to prevent further violations. An immediate blocking is also permissible without a prior hearing of the user and without an examination of the alleged infringement. However, the user must be informed about the specific reasons for the blocking.

A blocking is also permissible if the commercial user violates his contractual obligations towards the operator.

The operator has a duty to inform and give reasons to the merchant. A general reference to a potential violation, such as the manipulation of a product rating, is not sufficient. Rather, a concrete explanation of the offending conduct is required. The merchant should not have to puzzle over what he might have done wrong.

Surprising and incomprehensible blockings or terminations, on the other hand, are questionable. As a result of the Federal Cartel Office's investigations, Amazon has changed its contract terms. The company is no longer allowed to block or terminate merchants with immediate effect and without justification. The permissibility of similar terms and conditions is also doubtful for other platforms and is to be reviewed in the event of a dispute.

What can be done against an unlawful blocking or termination?

If a blocking or termination occurs without a valid reason, the motivation is insufficient or the accused breach of contract does not exist, it is recommended to first contact the platform operator. The existence of an error or the truthfulness of the allegations should be ruled out.

If the facts of the case cannot be clarified or the dragging out of the issue has negative consequences for the merchant, an interim injunction can be applied for. This can be used to obtain the removal of the blocking or termination and can be followed by a suit to seek damages for lost profits.

In January 2021, the German district court of Munich ruled for the first time in preliminary injunction proceedings that a blocking that is not sufficiently justified constitutes a restriction of competition. One of the interesting points for retailers here is that antitrust claims are to be qualified as tortious. This means that the court of the place in whose district the act was committed has jurisdiction under German law. If the German retail market is affected, the court in whose district the defendant has its general place of jurisdiction is competent. If this does not apply, any German court has local jurisdiction.

+ + +

Materials | Overviews

Overview of the current antitrust proceedings of the European Commission

Sara Nesler, Mag. jur. (Torino)

Hanover, July 2021

EU Commission v. Google, preferential treatment of own price comparison services

As of 25.05.2021

Fine of 2.4 billion euros imposed on 27.06.2017

Action pending before the European Court of Justice (ECJ), very likely to proceed to the European Court of Justice (ECJ)

Google was accused of discriminating against European price comparison portals by giving preference to its own price comparison portal through the search engine. In doing so, Google was acting in breach of European competition rules and exploiting a dominant position. Accordingly, the Commission initiated a proceeding against Google under Article 102 TFEU and Article 54 of the EEA Agreement AT.39741 and imposed a fine of EUR 2.4 billion.

Google claims that the order given to the search results merely serves to provide consumers with comprehensive and rapid information and does not favor its own price comparison services. In addition, Google's conduct would not have any anti-competitive effects. The commission did not prove that this specific order has favored its own price comparison service, and an investigation of actual market effects is lacking.

For the Commission, Google's arguments are not convincing. Actual consumer behavior, surveys, and eye-tracking analyses show that consumers generally click much more frequently on results that are displayed at or near the top of the first results page. By contrast, results displayed further down the first page or on subsequent pages, where competing price comparison services are usually found after a downgrade, are clicked on much less frequently. Even on desktop computers, the ten highest-ranked generic search results on page 1 account for a total of around 95% of all clicks (for the first search result, it is around 35% of all clicks). The first result on page 2 of the Google search accounts for only around 1% of all clicks. On mobile devices, this effect is even more pronounced because the display is smaller. Stronger visibility in Google search provides Google's price comparison service with more clicks, while competing services have suffered losses due to poorer rankings.

The argument of "no investigation of the actual market impact" was also adopted in Germany by the OLG Düsseldorf in a case against Facebook (concerning the implications of data for competition). It remains questionable to what extent an investigation of the "actual market impact" beyond behavioral studies is feasible at all. However, the advantage is quite obvious.

EU Commission v. Google, Android System

As of 25.05.2021

Fine in the amount of 4.3 billion euros imposed on 18.07.2018

No pending legal proceedings (yet)

Google demanded the pre-installation of Google Search and the Chrome browser on all devices as a condition for licensing Google's app store. In addition, the corporation has made payments to major manufacturers and mobile network operators who pre-installed Google search app on their devices. Google has also prevented the sale of competing operating systems that rely on the open Android source code.

Google argued that the restriction was necessary to prevent fragmentation of the Android system. The tying of the Google Search app and the Chrome browser had been necessary to generate revenue from the investment in Android. The payments served to convince smartphone producers to make devices for the Android ecosystem.

For the Commission, the approach served the purpose of securing the Group's market position against other service providers. The only other relevant mobile operating system is the iOS platform of Apple's iPhones.

EU Commission v. Google, AdSense (advertising)

As of 25/05/2021

Fine of 1, 49 billion Euros imposed on 03/20/2019

No court case pending, none expected

Google had a 70% market share in search engine advertising between 2006 and 2016. Competitors could not sell advertising space on the result pages of the (market dominant) Google search engine, so they ran advertising space on third-party sites (e.g. blogs).

The Group included exclusivity clauses in its contracts since 2006. Accordingly, publishers were not allowed to place advertisements from competitors on their search results pages. Later, the clauses were relaxed by a "premium placement" clause. After that, publishers were obliged to reserve the best spaces on their pages for Google's ads and to place a minimum number of Google ads. This prevented Google competitors from placing their search engine ads in the most visible and most clicked places.

From March 2009, Google also included clauses in the agreements that prevented partner publishers from changing the way the search engine ads of Google's competitors were displayed. This allowed Google to control how interesting competitors' ads were and how often they were clicked.

This way, competitors had no way of competing with Google on performance. Either they were directly prohibited from placing their ads on publisher sites, or Google reserved for its own ads the most promising spaces on those sites while controlling how competitors' ads could appear.

Google stopped the behavior in July 2016, after the EU Commission issued a complaint.

EU Commission v. Apple, music streaming **EU Commission v. Apple, e-books and audio books**

As of 025.05.2021

Antitrust investigation opened on 16.06.2020

Apple holds a dominant position in the distribution of music streaming apps through its App Store. For app developers, the App Store is the only gateway to consumers using Apple smart mobile devices running Apple's iOS operating system. Apple devices and system software form a "closed ecosystem" in which Apple controls all aspects of the user experience for iPhones and iPads.

The market dominance position is exploited:

- Music streaming app developers must use Apple's own system for in-app purchases. Apple charges app developers a 30% commission on all subscriptions obtained through in-app purchases.
- App developers are hindered from informing users about alternative purchase options outside the apps. The Commission is concerned that Apple device users will pay significantly higher fees for their music subscriptions as a result, or will not be able to purchase certain subscriptions directly in the app.

A parallel proceeding with a similar content was initiated against the distribution of e-books and audio books through the Apple Store.

EU Commission v. Apple, Apple Pay

As of 25.05.2021

Antitrust investigation opened on 16.06.2020

Apple Pay is Apple's proprietary solution for mobile payments on iPhones and iPads, both in apps and websites and in stores. The Commission is concerned that Apple's terms and conditions and its other actions to establish Apple Pay as a payment method could distort competition, reduce choice, and dampen innovation. In addition, Apple Pay is the only mobile payments solution that allows iOS mobile devices' "tap and go" NFC feature to be used for in-store payments. The Commission is also examining alleged restrictions on access to Apple Pay that exist for certain competing products on iOS/iPadOS mobile devices.

EU Commission v. Amazon, Buy Box

As of 25.05.2021

Antitrust investigation opened on 10.11.2020

There are concerns Regarding the criteria used to select which offer is displayed in the Buy Box and the conditions under which a supplier can distribute its goods in the "Prime" program. Amazon could be violating Art. 102 TFEU and Art. 54 EEA by favoring Amazon's own products or merchants that use the "Fulfilment by Amazon" program. (These merchants are very heavily dependent on Amazon).

EU Commission v. Amazon, Marketplace

As of 25.05.2021

Antitrust investigation opened on 17.07.2019

Amazon is both a platform operator and, through the same platform, a merchant. The company continuously collects data on the activity of other merchants on the platform. According to the Commission's initial findings, Amazon appears to misuse sensitive information about marketplace merchants, their products and the transactions made by merchants on the platform. The Commission intends to investigate whether and how the use of such data affects competition. It will also examine the role that competitively sensitive data play in the selection of merchants displayed in the "Buy Box."

Amazon Marketplace was also investigated by the German Federal Cartel Office. Consequently, the company changed its terms and conditions worldwide and the case was dropped as a result. However, this particular issue was not covered. The BKA's and the EU Commission's main concerns are likely to be covered for the most part by the Digital Markets Act.

+ + +

USA - Overview of the proposed Digital Market Anti-trust Policies

Sara Nesler, Mag. jur. (Torino)

Hanover, July 2021

Ending Platform Monopolies Act

Introduction:

11/06/2021 (House, D/R).

Target:

To promote competition in digital markets by eliminating conflicts of interest that arise from the simultaneous ownership or control of platforms and other companies.

Measures:

It shall be forbidden for operators of a covered online platform (comparable to the "very large platforms" in the EU drafts) to own, control or have an economic interest in another business that:

- Uses the covered platform to sell or provide products.
- Offers a product or service, the purchase or use of which is a condition of use of the Platform, of a preferred status, or of placement of a business user's products or services on the Platform. (This could be very problematic for the "Fulfillment by Amazon" model. The prime membership is one of the reasons businesses leave logistics to Amazon).
- Leads to a conflict of interest (incentive or opportunity to favor one's own products, services, or lines of business. Incentive or opportunity to exclude and disadvantage the products, services, or lines of business of a competing company or an emerging or potential competitor of the platform).

Personal incompatibility of directors, officers, partners, and employees.

Enforcement:

By the Federal Trade Commission and the Department of Justice pursuant to the Federal Trade Commission Act (15 U.S.C. 41 et seq.) and the Clayton Act (15 U.S.C. 12 et seq.). A violation of this Act also constitutes an unfair competition act under Section 5 of the Federal Trade Commission Act.

For violations of this Act, the Federal Trade Commission may bring a civil action on its own behalf against the platform operator to collect a civil penalty and seek other appropriate remedies in a United States district court.

Directors, officers, partners, and employees who fail to comply with any provision of this Act may be subject to civil penalties of up to 15% of the person's total average daily sales in the United States for the preceding calendar year, or up to 30% of the person's total average daily sales in a line of business affected or targeted by the unlawful conduct during the period of the unlawful conduct, in a civil action brought by the Commission.

Platform Competition and Opportunity Act

Introduction:

11/06/2021 (House, D/R).

Target:

To promote competition in digital markets by prohibiting certain acquisitions by dominant online platforms.

Measures:

It shall generally be prohibited for operators of covered platforms (designated by the Federal Trade Commission or the Justice Department) to acquire all or a portion of the shares or assets of another person if it engages in or affects commerce. An exception applies if the operator proves that:

- the acquisition is a transaction described in section 7A(c) of the Clayton Act; or
- that the shares or assets acquired are not, or potentially will be in the future, competitively related to the platform or operator for the sale or provision of products or services, and
- the market position of the platform or the operator with respect to the products and services offered by or directly related to the platform is not improved or increased through the acquisition and the maintenance of the market position is not facilitated.

It is assumed that competition for the sale or provision of products or services includes competition for the attention of users.

An acquisition that grants access to additional data may also readily improve, increase, or maintain market position.

Enforcement:

By the Federal Trade Commission and the Department of Justice pursuant to the Federal Trade Commission Act (15 U.S.C. 41 et seq.) and the Clayton Act (15 U.S.C. 12 et seq.). A violation of this Act also constitutes an unfair competition act under Section 5 of the Federal Trade Commission Act. For violations of this Act, the Federal Trade Commission may bring a civil action on its own behalf against the platform operator to collect a civil penalty and seek other appropriate relief in a United States District Court.

A civil action may be brought by the Commission on its own behalf or by the Attorney General of a State on behalf of itself and natural persons residing in that State in the appropriate district court.

Private individuals may sue for injunctive relief and damages plus interest and costs of suit if they have suffered injury because of a conduct that is unlawful under this Act. In the case of foreign states, compensation is limited to damages and legal costs.

Merger Filing Fee Modernization Act

Introduction:

11/06/2021 (Senate, D/R).

Target:

To promote antitrust enforcement and protect competition by adjusting the merger filing fees and increasing antitrust enforcement resources.

Measures:

Several minor adjustments to sec. 605 Public Law 101-162 to increase merger filing fees.

Provides \$252,000,000 each for the Antitrust Division of the Department of Justice and \$418,000,000 for the Federal Trade Commission for 2022.

American Choice and Innovation Online Act

Introduction:

06/11/2021 (House, D/R).

Target:

To prevent discriminatory conduct by covered platforms, fair relationship between platforms and business users.

Measures:

(a) Preference and discrimination: operators of a platform shall be prohibited from engaging in any conduct in connection with the platform that favors the products or services of the platform over those of other providers or excludes or discriminates against the products or services of others. In connection with user interfaces, including search or ranking functions, offered by the covered platform, it shall be prohibited to treat one's own products, services, or lines of business more favorably than those of another business user. Discrimination between similarly situated business users shall also be prohibited.

b) Interoperability and dependency of services: it shall be illegal for operators of covered platforms to restrict or prevent interoperability between systems. It shall also be illegal to make access to the platform, a preferred status or placement on the platform form dependent on the purchase or use of other products or services offered by the platform operator. Business users or their customers or users may not be prevented from interacting or connecting with any product or service.

c) Use of data: non-public data obtained from or generated on the platform from business users or their customers' interactions with the products or services may not be used to offer or support the platform operator's own products or services. Access by business users to data generated in such a manner may not be restricted or impeded.

d) Pre-installed applications: the uninstallation of software applications that have been pre-installed on the covered platform and the modification of default settings that guide or direct the users of the platform to products or services of the operator may not be prevented.

e) Customer-business user communication: it is unlawful to prevent or restrict business users from communicating information or providing hyperlinks on the covered platform to their users to facilitate business transactions.

f) Pricing: platform operators may not influence or restrict the pricing of business users.

g) Whistleblower: retaliation against business users or platform users who raise concerns about actual or potential violations to a law enforcement agency shall be prohibited.

Such conducts are not unlawful if there is convincing evidence that:

- They do not harm competition by restricting and inhibiting legitimate activities of business users; or
- The conducts were necessary to prevent or comply with a violation of federal or state law; or to protect user privacy or other nonpublic data. The conducts must have been carefully considered (not pre-formulated) and the intended objective could not have been achieved by a less discriminatory means.

Enforcement:

By the Federal Trade Commission and the Department of Justice pursuant to the Federal Trade Commission Act (15 U.S.C. 41 et seq.) and the Clayton Act (15 U.S.C. 12 et seq.). A violation of this Act also constitutes an unfair competition act under Section 5 Federal Trade Commission Act.

Civil Actions: Operators of a covered platform that fails to comply may be subject to civil penalties of up to 15% of the total average daily sales in the United States for the preceding calendar year, or up to 30% of the total average daily sales in the United States in a line of business affected or targeted by the unlawful conduct during the period of the unlawful conduct, in a civil action brought by the Commission.

Additional Measures (Beyond those provided by state or federal law):

- The Deputy Attorney General of the Antitrust Division, the Federal Trade Commission, or the Attorney General of a state may seek in court restitution of losses, rescission or modification of contracts, refund of money, or restitution of property.
- The Assistant Attorney General for the Antitrust Division or the Federal Trade Commission may seek disgorgement of infringer profits obtained because of the infringement. They may also seek injunctions to prevent, restrain or prohibit infringement in court. If the violation stems from a conflict of interest related to the simultaneous operation of several lines of business, the court shall consider requiring the divestiture of the line or lines of business giving rise to such conflict.

Civil action by damaged persons: damaged persons may apply to the appropriate district court for injunctions and bring suit to recover treble damages plus interest and costs of suit.

Augmenting Compatibility and Competition by Enabling Service Switching Act (ACCESS Act)

Introduction:

11/06/2021 (House, D/R).

Target:

To promote competition, lower barriers to entry, and lower switching costs for consumers and businesses online.

Measures:

The Federal Trade Commission shall designate covered platforms and issue specific interoperability standards for them. There shall be a Technical Committee established by the Commission for each covered platform with advisory authority to implement specific standards. The requests should aim to:

- Limit or eliminate network effects that inhibit competition.
- Provide data security and privacy protections for data portability and interoperability.
- Prevent abusive activities.
- Establish reasonable thresholds and fees for access to data on covered platforms for competing or potentially competing companies.

Data Interportability and Interoperability: covered platforms shall maintain a set of transparent, third-party accessible interfaces (including application programming interfaces) to enable the secure transfer of data to a user or, with user consent, to a business user at the direction of a user in a structured, commonly used, and machine-readable format that complies with the established standards.

Transparent interfaces accessible to third parties shall also be held available to facilitate and maintain interoperability with competitors or potential competitors.

Data Security: Competitors or potential competitors that receive ported user data from a covered platform or access a covered platform's interoperability interface shall reasonably secure all user data it acquires, processes, or transfers and take reasonable steps to avoid introducing security risks to user data or the covered platform's information systems.

The Commission may require the covered platform to cease cooperating with a competing or potentially competing entity if, in the Commission's judgment, the entity has violated these requests or the enacted standard. Covered platforms shall set their own privacy and security standards for access by competing businesses or potential competing businesses to the extent reasonably necessary to address any threat to covered platform or user data and shall report to the Commission any suspected violations of such standards.

Business Users are not required to maintain standards established by the Commission unless they initiate the transfer of data from a covered platform; or access an interoperability interface.

Modification of Interoperability Interfaces: Commission consent is required to make changes that may affect the interoperability interfaces. This will be granted if the change does not have the purpose or effect of unreasonably denying access to competing entities or potential competing entities or undermining interoperability. A change affecting interoperability may exceptionally be made without the Commission's consent if the change is necessary to address a security vulnerability or other urgent circumstance that poses an imminent risk to the privacy or security of users, provided that the change is narrowly tailored to address the security vulnerability and does not have the purpose or effect of unreasonably denying access to competing entities or potential competing entities or undermining interoperability.

Information Requirements: Within 120 days of the Commission's determination of rules and standards, covered platforms shall provide competitors or potential competitors with complete and accurate documentation describing access to the interoperability interface. Changes shall be communicated in a timely manner, for example, through public notice.

Collection and use of data: A covered platform may not collect, use, or disclose user data obtained from a business user through the interoperability interface except to protect the privacy and security of such information or to maintain the interoperability of the services. Business user shall not collect, use or disclose a user's information on a Covered Platform except to protect the privacy and security of such information or to maintain the interoperability of Services.

Enforcement:

A violation of this Act also constitutes an unfair competition act under Section 5 of the Federal Trade Commission Act.

For violations of this Act, the Commission may bring a civil action in a district court to collect a civil penalty or seek injunctive or other appropriate reliefs. The civil penalty may be up to 15% of the total United States revenue of the person, partnership, or corporation for the previous calendar year, or up to 30% of the total United States revenue in a line of business affected or targeted by the unlawful conduct during the period of the unlawful conduct.

Beyond the remedies provided by state or federal law:

- The Deputy Attorney General of the Antitrust Division, the Federal Trade Commission, or the Attorney General of a State may seek in court restitution of losses, rescission or modification of contracts, refund of money, or restitution of property.
- The Assistant Attorney General for the Antitrust Division or the Federal Trade Commission may seek disgorgement of infringer profits obtained because of the infringement. They may also seek injunctions to prevent, restrain or prohibit infringement in court.
- If a platform is found to have systematically violated the Act, the court may order the executive to forfeit to the United States Treasury all compensation received from the platform in the 12 months prior to or after the filing of the lawsuit.

USA – Overview of current antitrust proceedings

Sara Nesler, Mag. jur. (Torino)

Hanover, July 2021

Proceeding of the Antitrust Division v. Alphabet (Google)

Complaint 10/20/20

Section 2 of the Sherman Act, 15 U.S.C. § 2

Parallel to EU Commission proceedings

As of: 22.06.2021

Target:

To prevent Google from unlawfully maintaining monopolies in the markets for general search services, search advertising, and general search text advertising in the United States through anticompetitive and exclusionary practices and to remedy the effects of such conduct.

Google's position in the U.S.:

The most effective means of distributing a general search engine is through pre-installation on mobile and computer search access points. Users can change the default setting, but they rarely do. This results in the default preset search engine enjoying de facto exclusivity, especially on mobile devices. For years, Google has entered into restrictive agreements, including tying agreements, to close off distribution channels and block competitors.

Google's exclusionary agreements cover nearly 60 percent of all general search queries. Nearly half of the remaining search queries are routed through Google-owned and -operated properties (e.g., Google's Chrome browser). With the exclusionary agreements and Google-owned and -operated properties, Google effectively owns or controls the search distribution channels that are responsible for approximately 80 % of general search queries in the United States. Largely thanks to Google's exclusionary agreements and anticompetitive behavior, Google accounted for nearly 90 % of all general search queries in the United States in recent years, and nearly 95 % of searches on mobile devices. Google has thus eliminated competition in Internet search. Competitors in the general search space are denied vital distribution, scale, and product awareness, so they have no real chance to challenge Google.

Google monetizes this search monopoly in the search advertising and general search text advertising markets, which Google has also monopolized for many years, with revenues of about \$40 billion annually. Google "shares" these monopoly revenues from search engine advertising with manufacturers and sellers in return for a commitment to favor Google's search engine. These enormous payments provide a strong incentive for them to switch. The payments also raise barriers to entry for competitors - especially small, innovative search companies that cannot afford to pay a billion-dollar entry fee. Google's influence over distribution also thwarts potential innovation.

Nearly 20 years ago, the D.C. Circuit recognized in *United States v. Microsoft* that anticompetitive agreements by a high-tech monopolist that foreclose effective distribution channels or competitors, such as by imposing a preset default status (as Google does) and making it impossible to delete software (as Google also does), are exclusionary and unlawful under Section 2 of the Sherman Act. At the time, Google claimed that Microsoft's practices were anti-competitive. Google learned from this to choose its words carefully to avoid antitrust scrutiny. Specifically, Google employees were instructed to avoid terms such as "bundle," "tie," "crush," "kill," "injure," or "block," and not to claim that Google has "market power" in any market.

Earlier this year, while the United States was investigating Google's anticompetitive conduct, Google entered into agreements with distributors that are even more exclusionary than the agreements they replaced. Google has also turned its attention to emerging search gateways, such as voice assistants, to ensure that they, too, are covered by the same anticompetitive scheme. Google is now positioning itself to dominate the search access points of next-generation search platforms: Internet-enabled devices such as smart speakers, home appliances, and automobiles (so-called Internet-of-Things or IoT devices).

As a result, countless advertisers must pay a toll on Google's monopoly on search advertising and general search text advertising; American consumers are forced to accept Google's policies, privacy practices, and use of personal data; and new companies with innovative business models cannot step out of Google's long shadow.

Violation of Section 2 Sherman Act:

1. Relevant market:

Both general search services and search advertising and search text advertising are relevant markets in the U.S. without adequate substitutes.

2. Monopoly position:

- General Search Services Market: there are only four providers in the US: Google, Bing, Yahoo!, and DuckDuckGo. Google dominates the market with an 88% share and 95 on mobile devices.

- Search advertising and search text advertising: Google has at least 70% of the market share in both, with competitors often offering only specialized advertising in specific areas.

3. Actions to preserve and maintain a monopoly position:

- Anti-forking agreements (Anti-Fragmentation Agreements and Compatibility Commitments): although Android is an open-source system, Google maintains control through anti-forking agreements that prohibit any actions that "cause or result in fragmentation of Android". Fragmentation is not defined and is interpreted broadly by Google. Android represents over 95 % of licensable mobile operating systems for smartphones and tablets in the United States. Most well-known manufacturers are bound by AFAs and ACCs.
- Pre-installation Agreements (Mobile Application Distribution Agreements): creators who want to pre-install a Google app (including Google Play, which installs 90% of apps on Android devices), or need access to GPS and the APIs to make their apps work properly, must sign pre-installation agreements. Any manufacturer installing Google Play or GPS must pre-install a full suite of apps including the search access points most used by consumers: Chrome, Google Search app, Google Search widget and Google Assistant. These apps are pre-installed in such a way that they cannot be deleted by the user. Most MADAs require Google to be pre-installed as the default search engine.
- Search Revenue Sharing Agreements (RSAs) and Mobile Incentive Agreements (MIAs) for Android: in return for being pre-installed as the only default search engine, Google offers a share of the search advertising revenue. For some agreements, this only applies if all Android devices from a manufacturer meet the exclusivity requirements. For others, the agreement applies by model. In the latest negotiations, RSAs have been replaced by MIAs. Under these, manufacturers are paid if they pre-install Google as the default search engine and meet a significant number of "incentive implementation requirements." Google has revenue sharing agreements (RSAs or MIAs) with all major U.S. operators and manufacturers of Android devices, as well as with several smaller operators and manufacturers.
- Search revenue sharing agreements (RSAs) with Apple and others: Google has also entered into revenue sharing agreements with competing browsers and other device manufacturers (esp. Apple, which accounts for 60% of mobile devices in the U.S.), further foreclosing access to search for competition. In 2005, Apple began using Google as the default general search engine for Apple's Safari browser. In return, Google gave Apple a significant percentage of Google's advertising revenue derived from searches on Apple devices. Two years later, Google extended this agreement to Apple's iPhones. In 2016, the agreement was further expanded to cover additional search access points - Siri and Spotlight - and made Google the default general search engine for both services. Today, the distribution agreement between Google and Apple gives Google the coveted default preset position on all major search access points for Apple computers and mobile devices. In addition, Google has RSAs with almost every major non-Google browser that is not distributed by Microsoft.

- The future and the Internet of Things: Through anti-forking agreements and increased leverage, Google can maintain control over next-generation devices (Internet of Things) and prevent the introduction of alternative search services on these devices. For example, Google partners with car manufacturers on the condition that they do not pre-install competing search-related apps. Google has similarly restrictive agreements with smartwatch manufacturers: its agreements to license Google's "free" smartwatch operating system (Wear OS) prohibit manufacturers from pre-installing third-party software, including competing search services. Google also refuses to license its Google Assistant to manufacturers of IoT devices that would simultaneously host another voice assistant - a feature commonly known as "concurrency." Concurrency could allow a competing voice assistant to gain popularity and challenge Google's control over how consumers generally access the Internet, even on more established devices such as mobile phones. Finally, Google is using its control over hardware products - including smart speakers and Google Nest smart home products - to protect its overall search monopoly.

Lawsuit of the Federal Trade Commission and 48 States v. Facebook

Filed 09.12.2020

Violations of: sec. 2 Sherman Act, 15 U.S.C. § 2, sec. 5(a) FTC Act, 15 U.S.C. § 45(a).

As of: 06/22/2021

Target:

Facebook is accused of buying up competitors, specifically WhatsApp and Instagram, to liquidate competition in the social media industry. The FTC's antitrust lawsuit aims to force Facebook to reverse these two major acquisitions.

Violation of antitrust laws:

1. Relevant market:

Provision of personal social networking services in the United States.

2. monopoly position:

Facebook has held a monopoly position (more than 60% of market share) in the provision of personal social networking services in the United States since at least 2011.

3. actions to maintain and retain a monopoly position:

- Acquisition of Instagram (2012): Instagram was Facebook's main competitor in sharing images to cell phones. Facebook recognized the company as a threat, neutralized it through an acquisition in 2012, and thereby also deliberately hindered potential opportunities for other companies to become popular through their image sharing applications
- Acquisition of WhatsApp (2013): Facebook recognized the risk that WhatsApp, which offers mobile messaging services, could have entered the personal social networking market, and become a threat to its own business model. Instead of investing and innovating to remain competitive, WhatsApp was acquired.
- For many years, Facebook enforced anti-competitive terms of access to its platform connections, such as application programming interfaces ("APIs"). To communicate with Facebook (i.e., send data to or retrieve data from Facebook), third-party apps must use Facebook APIs. Until recently, Facebook made key APIs available to third-party apps only on the condition that they not provide the same core functionality that Facebook provides (including through Facebook Blue and Facebook Messenger), and not connect to or promote other social networks. This behavior - motivated by a desire to weaken and hinder potential competitive threats - harms competition and helps maintain Facebook's monopoly.

In this way, Facebook deprives users of personal social networks in the United States of the benefits of competition, including greater choice, quality, and innovation. Facebook cannot justify this significant harm to competition with claimed efficiencies, pro-competitive benefits, or business justifications that could not be achieved through other means.

Personal social networking providers are typically funded by the sale of advertising (approximately \$70 billion in 2019 for Facebook and Instagram), so more competition in the personal social networking space likely means more competition in the provision of advertising. By monopolizing personal social networks, Facebook also deprives advertisers of the benefits of competition, such as lower advertising prices and greater choice, quality, and innovation related to advertising.

Lawsuit Epic Games v. Apple (and Epic Games v. Google)

District Court: California, Northern District

Lawsuit filed on 13.08.2021. Judgment expected in July 2021.

A parallel lawsuit is pending against Google, for the same reasons.

As of: 22/06/2021

Facts of the case:

The game "Fortnite" was removed from Apple's and Google's app stores on Aug. 13, 2020, after Epic intentionally breached the terms of its developer agreement by implementing a payment system in the game that allowed players to bypass the app store. In this way, Epic circumvented

paying Apple's and Google's share of goods sold through their digital storefronts: 30%, an industry standard for digital platform owners such as Apple, Google, Microsoft, Sony, Nintendo and others. Epic immediately initiated lawsuits against Apple and Google. On August 17, 2020, Apple informed Epic that it would end access to developer accounts and tools for the App Store and iOS and macOS on Aug. 28, 2020.

Requests:

Epic accuses Apple and Google of operating a monopoly through the Apple Store and Google Store and exploiting their market power. The terms imposed by Apple and Google deny consumers access to lower prices, greater product choice and business model innovation.

Epic has sued for injunctive relief against the anti-competitive conduct and injunctions against the removal of "Fortnite" from the store and the blocking of developer accounts -and tools. Epic has not sought damages.

Apple has initiated a counterclaim and is seeking damages for breach of contract.

Current state:

The preliminary injunction to allow "Fortnite" in its current state (with Epic's storefront) was not granted.

Apple is prevented by a preliminary injunction from terminating Epic's developer accounts so that it can continue to maintain Unreal Engine for iOS and macOS systems.

A decision on the merits is expected in July 2021.

Complaint District of Columbia v. Amazon

Complaint 05/24/2021

Violations of D.C. CODE § 28-4503.

As of: 22/06/2021

Target:

Stopping Amazon's anticompetitive pricing policies.

Facts of the case:

According to the DC attorney general, Amazon fixes prices for online commerce through contract provisions and policies applied to third-party sellers on its platform. These provisions and policies prevent third-party sellers from offering their products at lower prices or better terms on other online platforms, including their own websites. These agreements effectively force third-party sellers to include Amazon's fees (up to 40% of the total product price) not only in the

price charged to customers on the Amazon platform, but also on any other online retail platform. As a result, these agreements enforce an artificially high price floor across the online retail market and allow Amazon to establish and maintain monopoly power, in violation of the District of Columbia Antitrust Act.

In 2019, Amazon claimed to have repealed its price parity policy, which explicitly prohibited third-party sellers from offering their products at a lower price elsewhere. In fact, however, Amazon replaced the Price Parity Policy with a virtually identical replacement: the Fair Pricing Policy. Under the Fair Pricing Policy, third-party sellers can be sanctioned or removed entirely from Amazon if they offer their products at lower prices or better terms on a competing online platform.

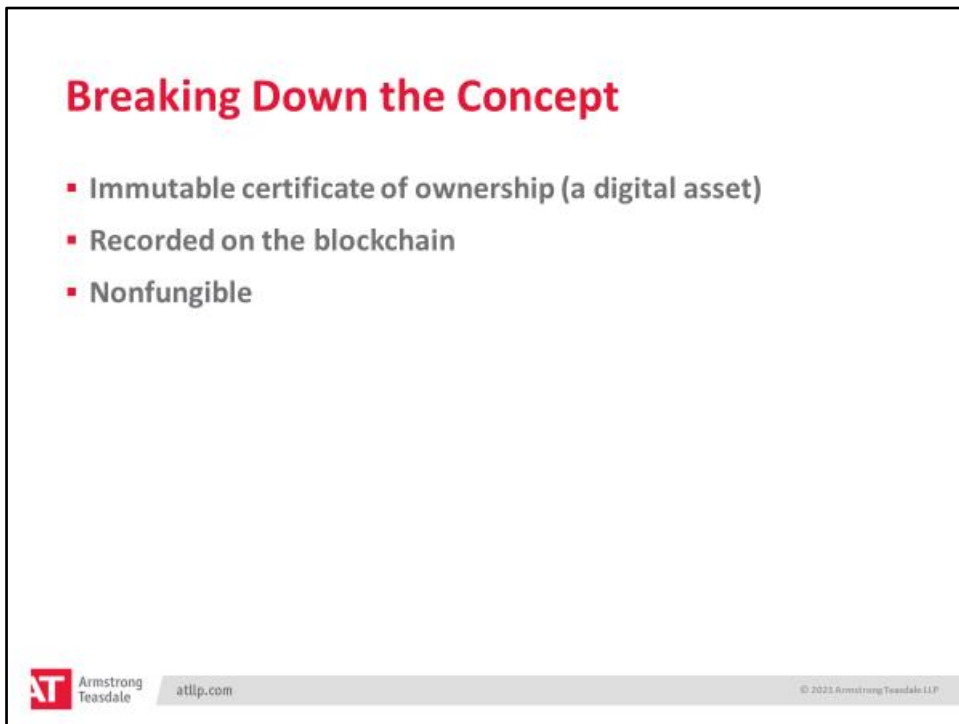
+ + +

Chapter Three

NFTs (Non-Fungible Tokens)



1



2

Blockchain (Re)explained...



AT Armstrong Teasdale
atllp.com

© 2021 Armstrong Teasdale LLP

3

What are they?



AT Armstrong Teasdale
atllp.com

© 2021 Armstrong Teasdale LLP

4

Common Digital Assets

The diagram lists the following digital assets:

- Cloud storage
- Digital media
- Graphics
- Word documents
- PDF documents
- Presentations
- Website domains
- Directories

AT Armstrong Teasdale atllp.com © 2021 Armstrong Teasdale LLP

5

Fungible Property v. Nonfungible

Blockchain Simplified

Examples of Fungible & Non-Fungible Tokens

Fungible	Non-Fungible
Dollar 	Cryptokitties 
Bitcoin 	Art 
Ethereum 	House/Property 


AT Armstrong Teasdale atllp.com © 2021 Armstrong Teasdale LLP

6

NFTs v. Cryptocurrency

- Cryptocurrency is fungible.
- NFTs are not.
- Damian Hirst: 'NFT currency'

Forces buyers to choose between owning a digital token or a work on paper.



AT Armstrong Teasdale atllp.com © 2021 Armstrong Teasdale LLP

7

Value of Use of NFTs?



A nonfungible token, being a certificate of ownership for a digital asset, has value that comes from the collectability of that asset, as well as its potential future sale value. NFTs can be sold and traded.

Uses:

- Tickets
- Fashion
- Collectibles
- Gaming

AT Armstrong Teasdale atllp.com © 2021 Armstrong Teasdale LLP

8

Examples of (Other) NFT Sales



A screenshot of a tweet from the user 'jack' (@jack) dated March 21, 2006. The tweet text reads 'just setting up my twttr'. It has 8.6K replies, 130.2K retweets, and 150.8K likes. Below the tweet are two images: on the left, a photograph of a baby crying; on the right, the 'Nyan Cat' meme featuring a pink cat with a rainbow trail.

AT Armstrong Teasdale atllp.com © 2023 Armstrong Teasdale LLP

9

Pros and Cons of NFTs



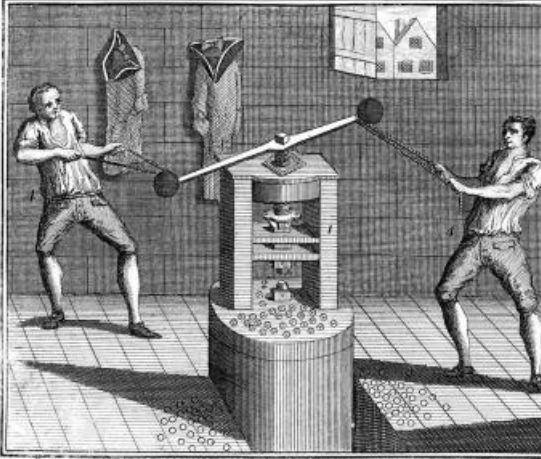
A close-up photograph of a gold-colored metal stamp. The stamp has a scalloped edge and the letters 'NFT' are embossed in a stylized, blocky font in the center.

AT Armstrong Teasdale atllp.com © 2023 Armstrong Teasdale LLP

10

Some Legal Issues

The ART of COINING.




- Data storage and hosting
- Intellectual property
- Electronic theft
- Royalties
- Data protection laws

Engraved for the Universal Magazine 1730 for J. Kinton at the Kings Arms.

AT Armstrong Teasdale | atlp.com | © 2023 Armstrong Teasdale LLP

11



Noor Kadhim
0207 539 7099 / nkadhim@atlp.co.uk
Full bio [here](#).

AT Armstrong Teasdale | atlp.com | © 2023 Armstrong Teasdale LLP

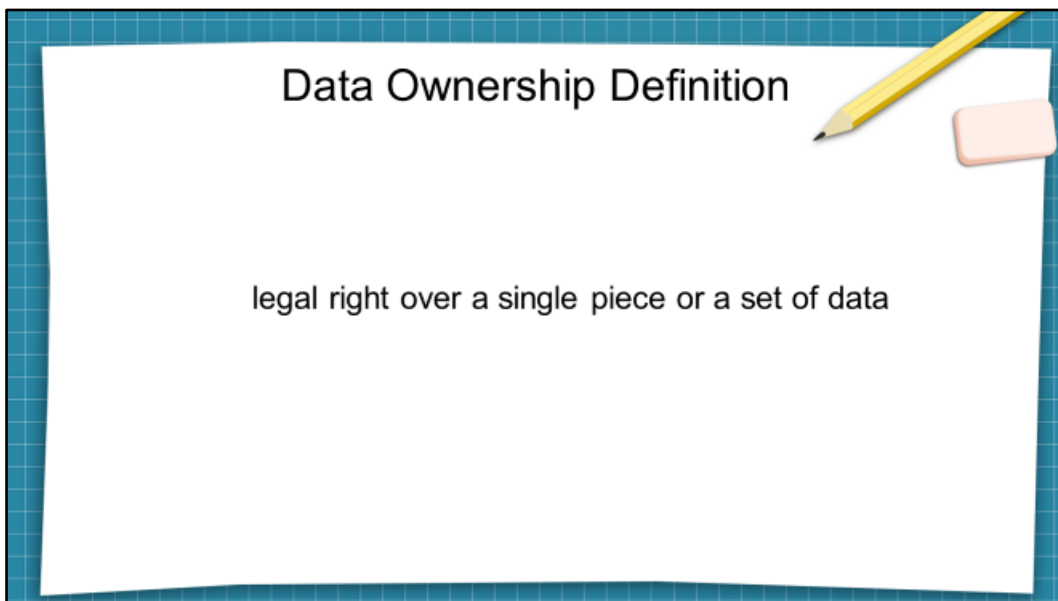
13

Chapter Four

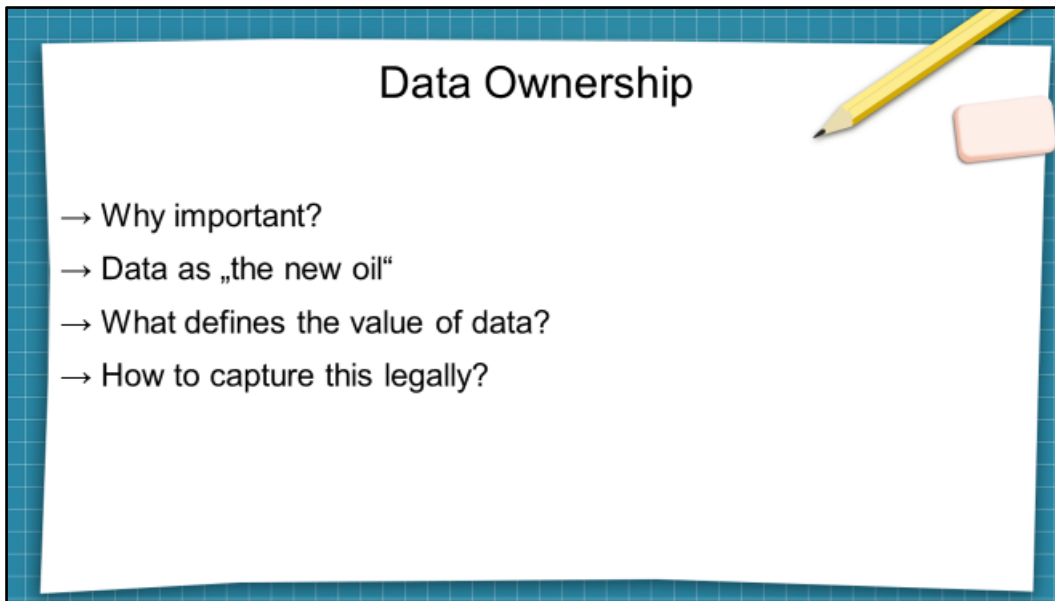
Data Ownership



1



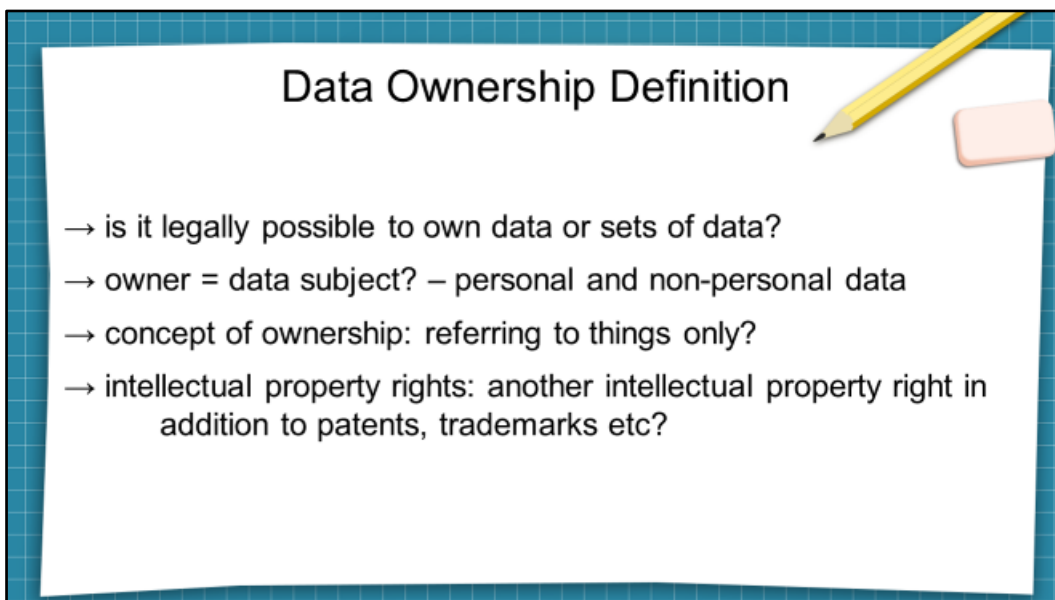
2



Data Ownership

- Why important?
- Data as „the new oil“
- What defines the value of data?
- How to capture this legally?

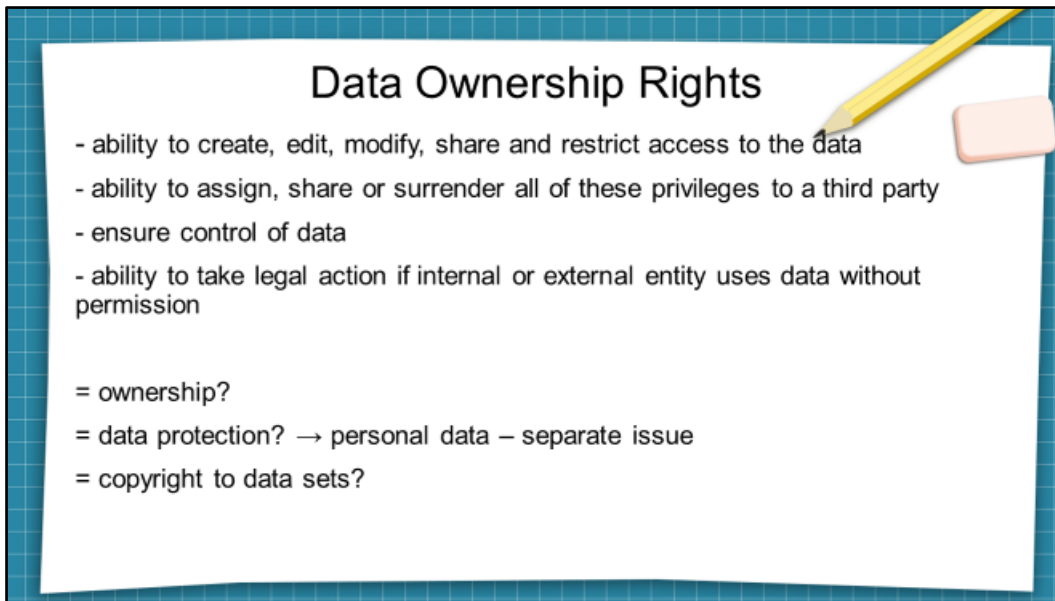
3



Data Ownership Definition

- is it legally possible to own data or sets of data?
- owner = data subject? – personal and non-personal data
- concept of ownership: referring to things only?
- intellectual property rights: another intellectual property right in addition to patents, trademarks etc?

4

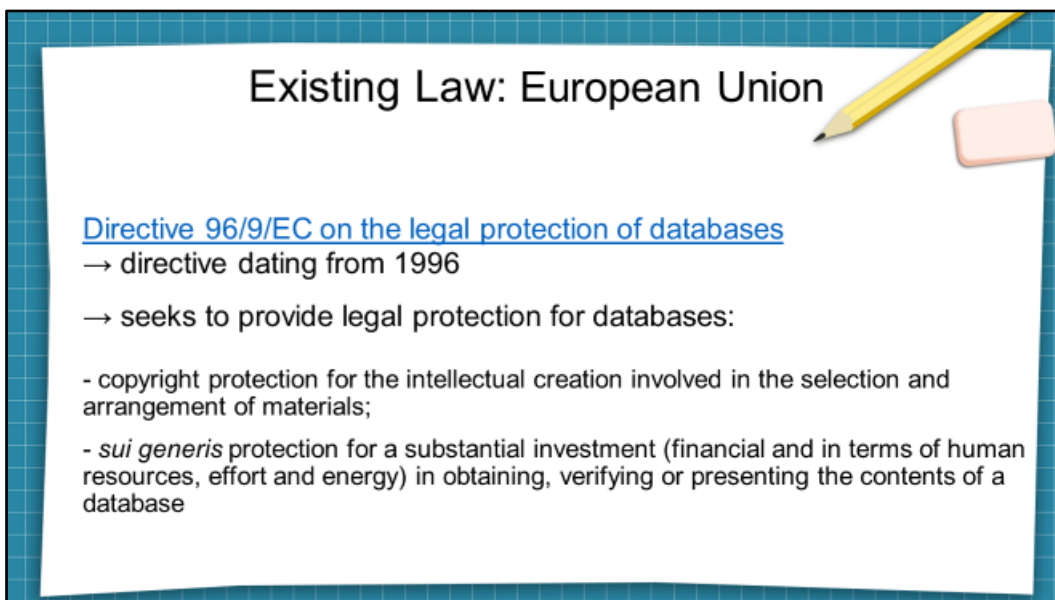


Data Ownership Rights

- ability to create, edit, modify, share and restrict access to the data
- ability to assign, share or surrender all of these privileges to a third party
- ensure control of data
- ability to take legal action if internal or external entity uses data without permission

= ownership?
= data protection? → personal data – separate issue
= copyright to data sets?

5



Existing Law: European Union

[Directive 96/9/EC on the legal protection of databases](#)
→ directive dating from 1996
→ seeks to provide legal protection for databases:

- copyright protection for the intellectual creation involved in the selection and arrangement of materials;
- *sui generis* protection for a substantial investment (financial and in terms of human resources, effort and energy) in obtaining, verifying or presenting the contents of a database

6

Existing Law: European Union

Directive 96/9/EC on the legal protection of databases

→ Copyright for 15 years (from creation completion)

- database protected by copyright if the selection or arrangement of its contents constitute the creator's own intellectual creation
- creator's exclusive rights, e.g. reproduction, alteration, distribution, etc.
- legitimate user's rights

7

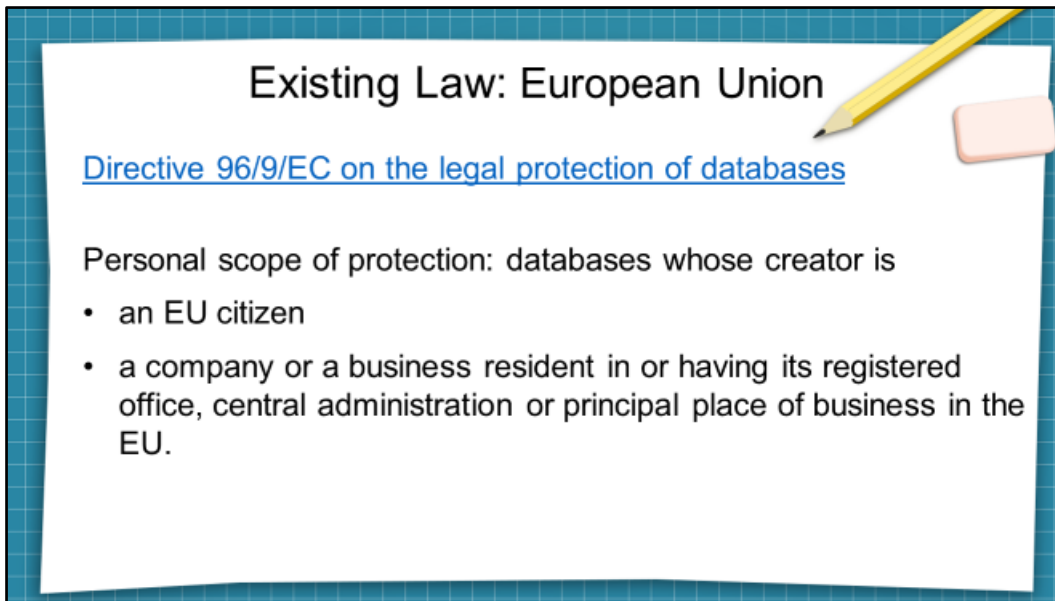
Existing Law: European Union

Directive 96/9/EC on the legal protection of databases

Permitted activities for lawful users without authorisation:

- extract and reuse non-substantial parts of the contents of a database
- not carry out acts that unreasonably harm the legitimate interests of the creator of the database or of a person providing the works or services it contains
- Free use for illustration for teaching or scientific research

8



Existing Law: European Union

[Directive 96/9/EC on the legal protection of databases](#)

Personal scope of protection: databases whose creator is

- an EU citizen
- a company or a business resident in or having its registered office, central administration or principal place of business in the EU.

9



Existing Law: German Act on Copyright and Related Rights

Implementation of the Directive in Germany in Copyright Act

[Division 6](#)
[Protection of makers of database](#)

[Section 87a](#) Definitions

[Section 87b](#) Rights of makers of database

[Section 87c](#) Limitations on rights of makers of database

[Section 87d](#) Duration of rights

[Section 87e](#) Contracts dealing with use of database

10

A slide with a blue grid background and a white paper-like center. The title is "Existing Law: German Act on Copyright and Related Rights". Below it is "Implementation of the Directive in Germany in Copyright Act". The section is "Section 87a Definitions". The text reads: "(1) A database within the meaning of this Act is a collection of works, data or other independent elements arranged in a systematic or methodical way and individually accessible by electronic or other means and whose obtaining, verification or presentation requires a substantial qualitative or quantitative investment. ...". There is a yellow pencil and a pink eraser in the top right corner.

Existing Law: German Act on Copyright and Related Rights

Implementation of the Directive in Germany in Copyright Act

Section 87a
Definitions

(1) A database within the meaning of this Act is a collection of works, data or other independent elements arranged in a systematic or methodical way and individually accessible by electronic or other means and whose obtaining, verification or presentation requires a substantial qualitative or quantitative investment. ...

11

A slide with a blue grid background and a white paper-like center. The title is "Existing Law: German Act on Copyright and Related Rights". Below it is "Implementation of the Directive in Germany in Copyright Act". The section is "Section 87b Rights of makers of database". The text reads: "(1) The producer of the database has the exclusive right to reproduce and distribute the database as a whole or a qualitatively or quantitatively substantial part of the database and to make this available to the public. The reproduction, distribution or communication to the public of a qualitatively or quantitatively substantial part of the database shall be equivalent to the repeated and systematic reproduction, distribution or communication to the public of qualitatively or quantitatively insubstantial parts of the database insofar as these actions run contrary to a normal utilisation of the database or unreasonably impair the legitimate interests of the producer of the database. ...". There is a yellow pencil and a pink eraser in the top right corner.

Existing Law: German Act on Copyright and Related Rights

Implementation of the Directive in Germany in Copyright Act

Section 87b
Rights of makers of database

(1) The producer of the database has the exclusive right to reproduce and distribute the database as a whole or a qualitatively or quantitatively substantial part of the database and to make this available to the public. The reproduction, distribution or communication to the public of a qualitatively or quantitatively substantial part of the database shall be equivalent to the repeated and systematic reproduction, distribution or communication to the public of qualitatively or quantitatively insubstantial parts of the database insofar as these actions run contrary to a normal utilisation of the database or unreasonably impair the legitimate interests of the producer of the database. ...

12

Existing Law: German Act on Copyright and Related Rights

Implementation of the Directive in Germany in Copyright Act

Section 87c
Limitations on rights of makers of database

(1) The reproduction of a qualitatively or quantitatively substantial part of a database shall be permissible

1. for private use; this shall not apply to a database whose elements are accessible individually by electronic means,
2. for the purposes of scientific research pursuant to sections 60c and 60d,
3. for the purpose of illustration in teaching in educational establishments pursuant to sections 60a and 60b.

In the cases referred to in nos. 2 and 3, the source shall be clearly indicated and section 60g (1) shall apply accordingly.

...

13

Existing Law: German Act on Copyright and Related Rights

Implementation of the Directive in Germany in Copyright Act

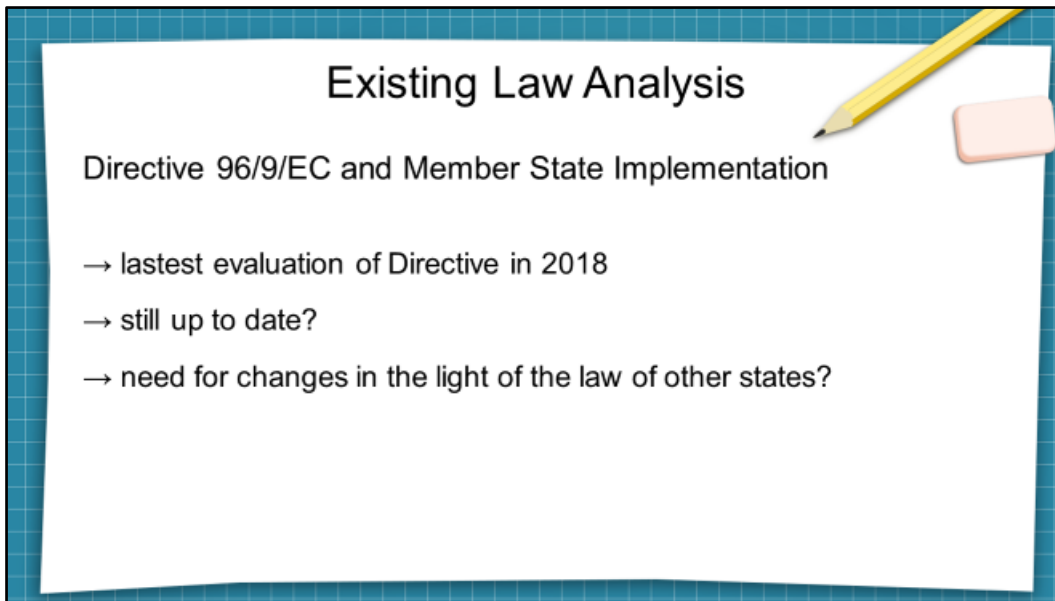
Section 87c
Limitations on rights of makers of database

...

(2) The reproduction, distribution and communication to the public of a qualitatively or quantitatively substantial part of a database shall be permissible for use in proceedings before a court, an arbitration tribunal or authority, as well as for the purposes of public safety.

...

14

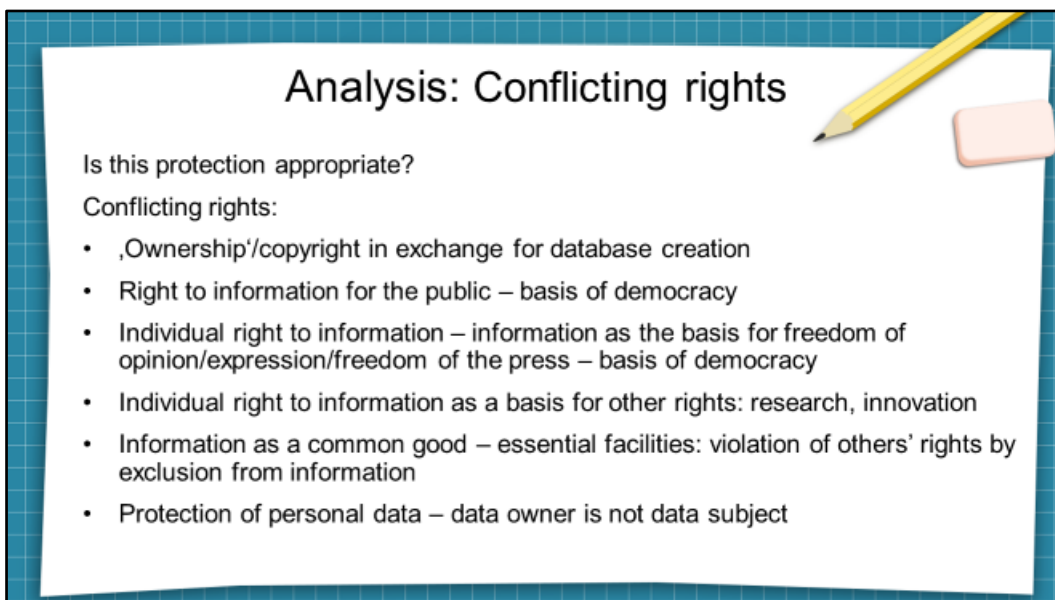


Existing Law Analysis

Directive 96/9/EC and Member State Implementation

- latest evaluation of Directive in 2018
- still up to date?
- need for changes in the light of the law of other states?

15



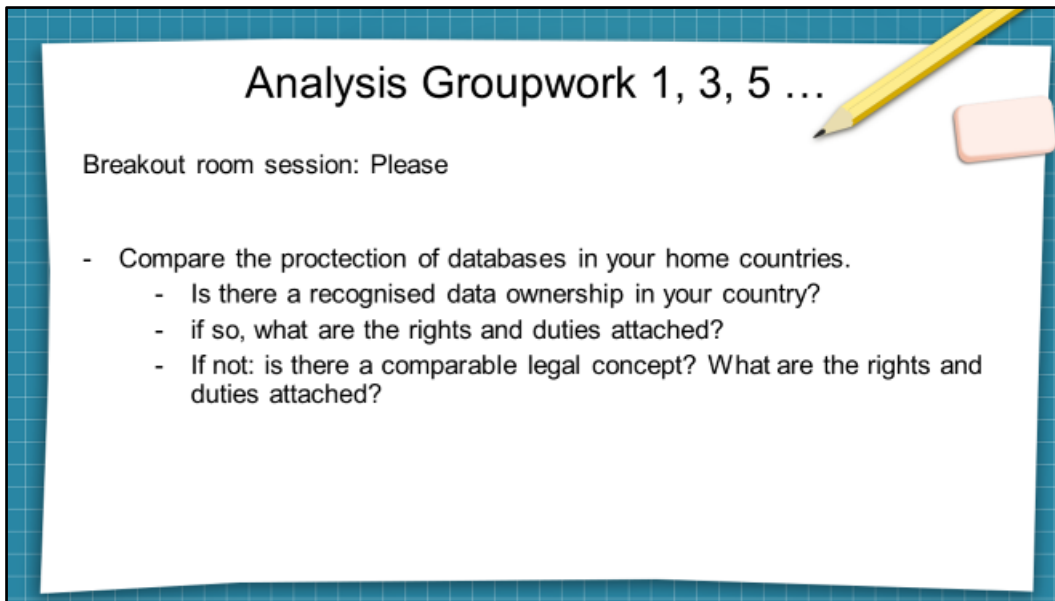
Analysis: Conflicting rights

Is this protection appropriate?

Conflicting rights:

- ,Ownership'/copyright in exchange for database creation
- Right to information for the public – basis of democracy
- Individual right to information – information as the basis for freedom of opinion/expression/freedom of the press – basis of democracy
- Individual right to information as a basis for other rights: research, innovation
- Information as a common good – essential facilities: violation of others' rights by exclusion from information
- Protection of personal data – data owner is not data subject

16

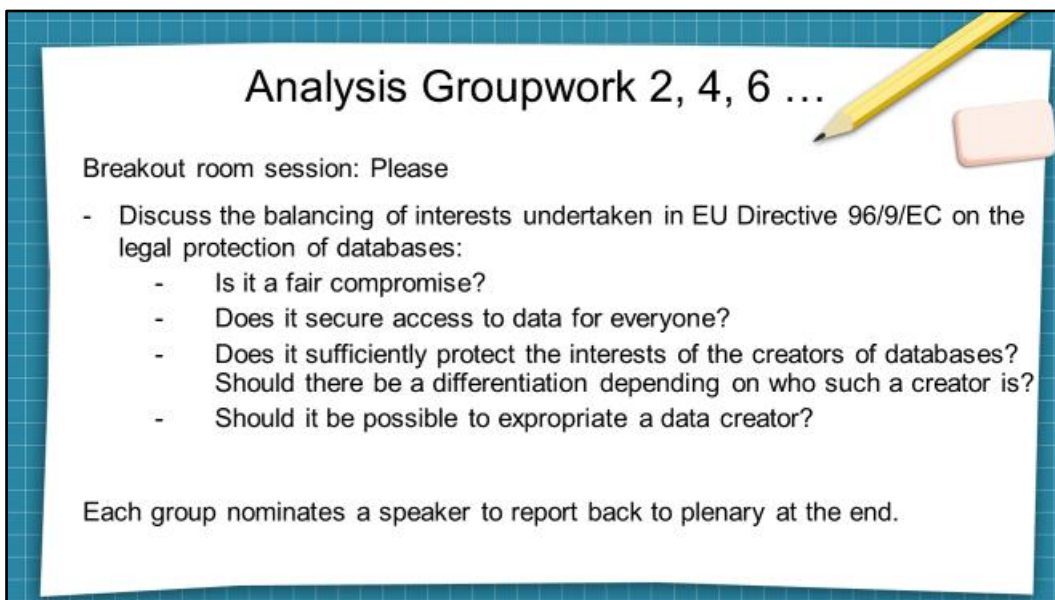


Analysis Groupwork 1, 3, 5 ...

Breakout room session: Please

- Compare the protection of databases in your home countries.
 - Is there a recognised data ownership in your country?
 - if so, what are the rights and duties attached?
 - If not: is there a comparable legal concept? What are the rights and duties attached?

17



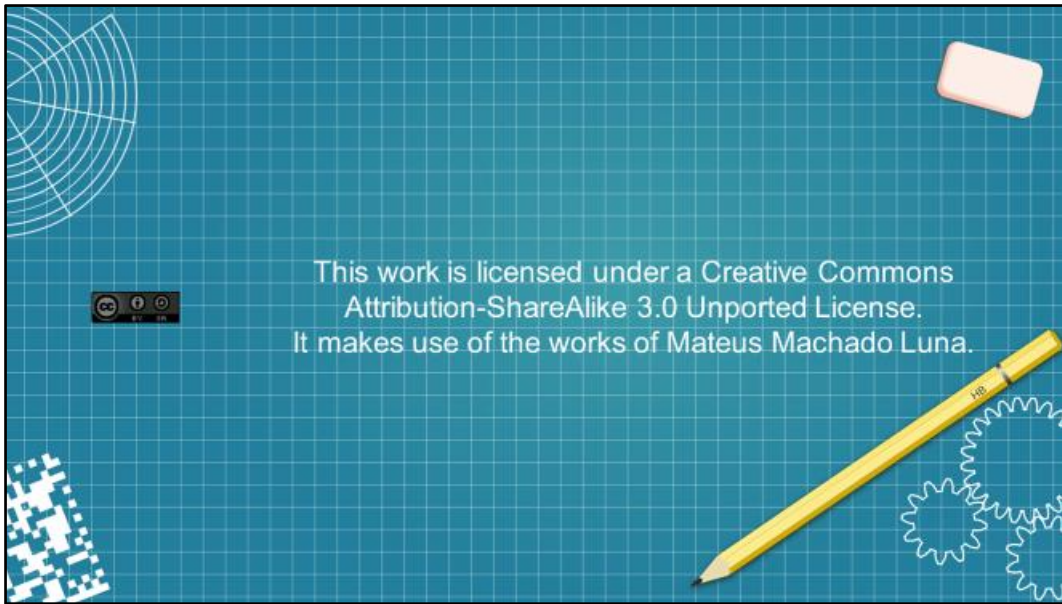
Analysis Groupwork 2, 4, 6 ...

Breakout room session: Please

- Discuss the balancing of interests undertaken in EU Directive 96/9/EC on the legal protection of databases:
 - Is it a fair compromise?
 - Does it secure access to data for everyone?
 - Does it sufficiently protect the interests of the creators of databases? Should there be a differentiation depending on who such a creator is?
 - Should it be possible to expropriate a data creator?

Each group nominates a speaker to report back to plenary at the end.

18



Questions and Answers

Data Ownership

Are there discussions on data ownership in your country? Please give your opinion: arguments in favor and against.

Cheril (China):

Yes, I think China should establish data rights in the form of legislation, for the following reason: Big data has had an unprecedented impact on all aspects of social life, and has also triggered many new issues worthy of study in various legal departments. Among them, the most important issue is the rights of personal data. On the one hand, the increasing digitization of social life and the continuous reduction of the cost of collecting and storing data have resulted in the collection, storage and utilization of massive amounts of personal data. It is extremely easy for data users to accurately capture the specific individuals' past activities through these data and predict the choice of its future behavior. If the rights of personal data cannot be fully protected, it is very easy to illegally collect, sell and use personal data and infringe on personal rights and property rights. On the other hand, massive personal data contains huge economic and strategic value. Without the collection, storage, sorting and utilization of personal data, data technology cannot be developed, as well as the data products. Personal data rights are also related to the development of the data industry. For data companies that collect and use a large number of personal data, whether they have rights to such personal data and what rights they have are critical to the development of data protection. The arrangement of rights on personal data directly determines the flow and sharing of data and the development of the data industry. In the future, the legislation of data rights protection in China should adopt a positive definition method to clarify the ownership rights and interests of enterprises in data products and non personal data, such as possession, use, income, disposal, etc.; for the part of enterprise data involving personal data, the legislative design of data controller should be used for reference to construct the scope of authority and obligation content of enterprises in personal data.

Wenzhu Lan (China):

I am in favour of the data ownership. because we are producers of data, the data should belong to the users themselves, only that the users host it in the servers of various companies. Internet companies should at least not sell users' data without permission. When using users' data, they should at least follow the two basic points of the consumer protection law. One is the right to know. You have to tell users what you will do with the data. The second is the right of choice. If the user refuses to use his data to do these things, you should delete the user's data.

Ana Marija Đurić (Croatia):

There are not many discussions on data ownership in Croatia. Although, I am familiar with discussions in other countries over data ownership where it is stated that the problem of data ownership has been reported, and the Commission has increased coverage of data ownership in its Communications. Some support the introduction of an ownership right for data while others distinguish between an exclusive and non-exclusive right to data property.

I would say that I oppose the implementation of data ownership laws because identifying the original owner of the data would be incredibly difficult, and regulation might lead to untenable scenarios. Also I believe that data ownership could be dealt with successfully through contracts.

L. Tuncer (Netherlands):

There are discussions about whether data, which is not something you can hold in your hand (or as required in the Dutch civil code "material") could be owned by someone. In my opinion, there are pros and cons to whether data should be subject to 'ownership'. It could solve problems with the forwarding of potential harmful pictures, sounds, on the internet. However most of these cases could already be subject to copyright protection or solved with portrait rights. The biggest problem with data that most of the time it is not exclusive, unless used with blockchain technology. It might offer a solution for the seizure of data, but we are simply not sure if it is 100% safe and effective yet.

Zoë Jardim (Brazil):

Yes, there is yes. They even created a law about that data protection called "Lei Geral da Proteção de Dados", that it's only applied on data from Brazil. I find it a very important topic that should definitely be discussed. This is an issue that everyday becomes more and more present in our reality, such as hackers stealing personal data or using our data for targeted marketing, etc. Every country should have a law like this. Unfortunately we are very vulnerable to the internet, and we depend on it for most of the things. Of course they need to have our data, for their interest and control. However, it is fundamental to have a certain protection for such data, for any case.

Materials | White paper

Data rights and data use – Who should own the data?

Ulrich Herfurth, attorney at law in Hanover and Brussels

Hanover, Mai 2018

IT systems are at the heart of integrated manufacturing, maintaining, and monitoring its functionality. Data that is generated and used in the (connected) machines is of great importance. On the one hand, it contains the business knowledge about the product, but also about the necessary processes; on the other hand, integrated manufacturing only runs smoothly if the data can be transmitted and used without obstacles.

Therefore, data from operations and business that are generated in the networked machines are becoming increasingly important as a raw material for a company. And the more digitally a company is set up, the more diverse legal questions arise about data security, data protection, compliance, but also about who has control over the data generated by the machines. This applies to all companies, whether in production or in services. For example, a car repair shop receives analysis data from the vehicle. Rights to this could be held by the repair shop - but also by the vehicle owner, the vehicle holder, the driver, the car manufacturer, the service system provider, a platform operator, the insurers, and authorities?

What is data?

Before we can clarify who owns data, the first question is: What is data?

When a computer scientist talks about "data" or "data protection", he usually means data in the technical sense, i.e., electronically readable information that is either stored on a data carrier or transmitted on a signal carrier. In other words: ones and zeros. "Data" in the legal sense, however, is actually information. Only these also have an economic value. In the digital world, both definitions usually coincide, but not always.

Is there such a thing as data ownership?

So what is data in the legal sense? Who owns the data that a machine generates? Is there a property right in the legal sense to the data generated?

Data are recognisable elements of information that are stored in a specific form that can be changed at any time and are fed to data processing systems for automatic processing or are sent by them.

Ownership is the comprehensive (absolute, real) right of dominion over movable and immovable objects in the sense of § 90 BGB. Ownership is therefore also an absolute right, i.e. it is effective towards everyone; whereas rights from contracts are in principle only valid between the contracting parties who have chosen each other and entered into the contract with each other, ownership and the rights arising from it are automatically valid towards any third party.

However, while things are physical objects, this is not the case with data. Therefore, there is no ownership of data in the classical, legal sense: a thing only exists once, but data can be reproduced in any number of identical ways.

Data therefore legally "belong" to no one. So far, the law does not provide for ownership of data. Yet there is much debate among experts as to whether such data ownership should be introduced by law. The arguments for and against it are either dogmatic or pragmatic: one clearly audible opinion considers data ownership to be anti-innovation because it hinders the exchange of knowledge. On the other hand, the information originates in the sphere of a particular company and can make up part of its value.

Data as Intellectual Property

It is now conceivable that data can be protected as so-called intellectual property. Whether data can be the subject of such rights at all, and if so, which data, has only been clarified selectively so far. First and foremost, patent protection, copyright and database protection come to mind.

A patent protects technical "products", in the case of process patents, also the direct products of the protected process. Inventions are eligible for protection if they are new, can be used commercially and, above all, have a certain level of inventiveness, i.e. are the result of a special intellectual achievement. Data arising from the operation of machines or data collected in any other way are not covered as such.

Software as such cannot be protected by patents; computer programs, as personal intellectual creations, are covered by copyright. Again, machine-generated data as such is not a human creation, but the result of a machine process. It is true that there will also be data protected by copyright in companies under Industry 4.0, such as software or designs and construction sketches that are used in digital form as CAM data. However, the starting point for this data remains the human being, and the rules for the rights to this data are no different than they have always been.

The Copyright Act contains a special regulation for the protection of databases. However, this does not protect a personal intellectual creation, but only the financial investment. A database in the information technology sense is not sufficient; only a substantial investment in the acquisition, verification or presentation of data is protected. The mere recording of primary data, which accumulates in industrial production anyway or can be measured with simple means, does not fulfil these requirements. On the other hand, targeted, elaborately meas-

ured data as well as secondary data of complex big data analyses are eligible for protection.

Use of data as unfair competition

In certain cases, competition law can also provide protection, namely in the case of unfair imitation of a product or service. Whether this can apply to data has not yet been clarified. Overall, competition law offers at best weak legal protection of data, limited to certain constellations and fraught with legal ambiguities.

Data as trade secrets

Furthermore, one could think of data as trade and business secrets - these enjoy legal protection under competition law and criminal law. Trade and business secrets are facts, circumstances or processes that are not public knowledge and are only accessible to a limited circle; in addition, the company must have a justified interest in keeping them secret. Whether data from machine operation are secrets is, however, very questionable in many cases. In future, secrets will only be protected according to European law if they are specially secured against unauthorised access. In most cases, therefore, protection as a trade secret is ruled out. All in all, there is currently no law that absolutely protects data as such against access by third parties.

Value of data

However, data resources will increasingly become a decisive basis for customer benefit, market success and the earning power of a company. In addition, they are also a critical variable for the pure functionality of machines, plants, and systems, if only through them machines can be used efficiently.

At the latest when a company's business model is based on the fact that the data generated by the machines form the actual basis of the product, the question of the value of the data arises.

For example, if a company outsources production and sends the necessary data for production to a 3D printer, where the product is created, this control data is important.

If a machine manufacturer has a maintenance contract with his customer, he now uses online access to monitor the function of the machine and the wear of parts and even to predict the next maintenance (predictive maintenance). So the question arises as to who is or should be entitled to use this machine operating data: the company, the machine manufacturer or an external maintenance company? Who is allowed to evaluate the data, for example to compare the efficiency of operations with other companies?

If a company now also offers an app with additional benefits - for example, for planning or calculating components or projects - the provider learns a lot about the user: which products he is interested in, how often, when and in which region. From this, insights can be gained not

only about product interests, but also about market developments in different regions.

Companies regularly exchange data in the production process and in the supply chain: it is passed on from company to company, from machine to machine and via components, platforms, and servers - in both directions: from the customer to the smallest upstream supplier and from supplier to supplier up to the manufacturer. Who actually has data sovereignty will be more complicated to answer when this data is mixed in the supply chain.

Here, for example, the manufacturer could use the data of his suppliers not only to support his own production process, but also to compare the data with other suppliers and play them off against his competitors. He could also resell his insights to third parties in the market, thus creating new revenue streams from his suppliers' data.

Data use contracts

As soon as the data represent the company's entrepreneurial knowledge, they must be adequately protected. But because there is no legal right to machine data, this can only be regulated by so-called data use agreements. Data use agreements are contracts in which the companies involved agree who may use the data and how, how the data may be changed, what payment is to be made for the use of the data, etc. This basically applies to all conceivable forms of data use. This basically applies to all conceivable constellations, both for integrated Industry 4.0 processes and for Big Data and outsourced data processing or analysis.

If necessary, it should be precisely regulated who has to transmit which data to whom, who has to retain it, when it has to be deleted and whether this has to be proven. Contractual regulations on the acquisition of secondary knowledge and other processing of the data, on exclusivity as well as questions of technical data security (and the liability for this) also make sense.

As a supplier and maintenance company, a machine manufacturer could therefore agree with its user that the latter will only receive test data for the performance of contractual tasks and may only use it extensively for this purpose. The customer is then allowed to use the manufacturer's data, which serves to control and monitor the machine and its system. But the manufacturer would also use the data from the machines and systems for the operation, maintenance and control of the machine and system. More far-reaching are regulations according to which the manufacturer may process the data received from the customer and mix it with other data, evaluate and analyse it separately and across the board. Whether the manufacturer must make such findings available to its customer, is also a matter for the agreement then.

However, a data use agreement should not only include regulations on the use of the data, but also on its treatment. When a company gives its data to another company, it is important that the recipient handles the data with care, in particular that it is kept safe. The data must be protected against external damaging events, at least if only the recipient still has the originally transferred data or data generated from it later.

After all, long series of data - for example on operational processes or machine operation - can contain important findings. In addition, these data can be used as evidence to support legal positions in legal disputes.

Protection against access by third parties is particularly important. Whether the recipient is allowed to pass on the received data to other companies must therefore be clarified. Certainly, the transferor of data does not want competitors to gain access to such data, for example in the course of company comparisons. For the same reason, the recipient should also be obliged to protect the data received against access by unauthorised third parties. For this purpose, appropriate security measures should be taken, such as access controls, access security systems, monitoring systems and others.

Since there is no absolute right to data that is effective towards everyone yet, as is the case with intellectual property, only contractual protection between the parties involved remains. But this protection does not go any further, because only the contracting parties can bind each other, not third parties. Once the data has left the sphere of the transferor or recipient, it no longer enjoys protection.

The transferor should therefore attach the greatest importance to the recipient's handling of his data and safeguard compliance with these duties of care - as is customary in a declaration of confidentiality - with a contractual penalty.

The enforcement of such contractual terms of use for data naturally depends on the negotiating power of the respective contractual partner. A car manufacturer will hardly let a car repair shop dictate the conditions, but rather wants to enforce its own. Whether these are effective, then, is often to be measured against the standard of the law on general terms and conditions.

All in all, companies must be aware that data are playing an increasingly important strategic role and therefore deserve special legal attention.

For a first analysis these questions could be asked:

- What kind of data is collected in your company?
- How is this data currently used?
- Is the data processing necessary?
- What is the current and future purpose of the collection and processing?
- Is your company authorised to use the collected data for the intended purpose?
- Does your company have access to the relevant data at all?

+ + +

Chapter Five

Data Protection Update International

—

Understanding Cookies Consent

**EVERSHEDS
SUTHERLAND**

Understanding Cookie Consent
Alliuris Summer School

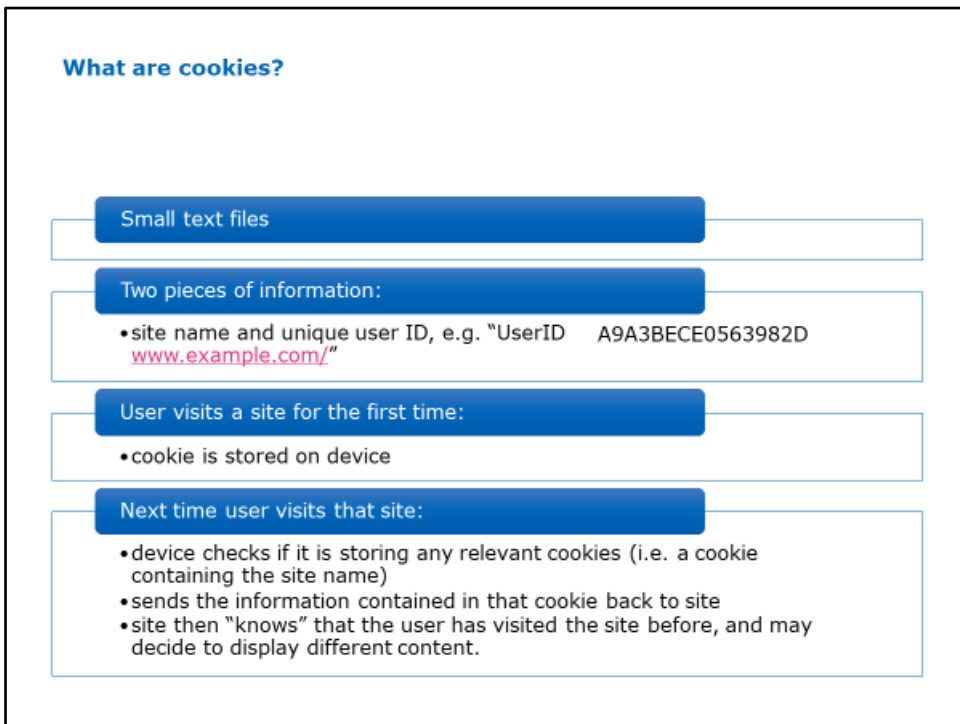
14.07.2021
Constantin Herfurth
Associate Data Protection & Cybersecurity



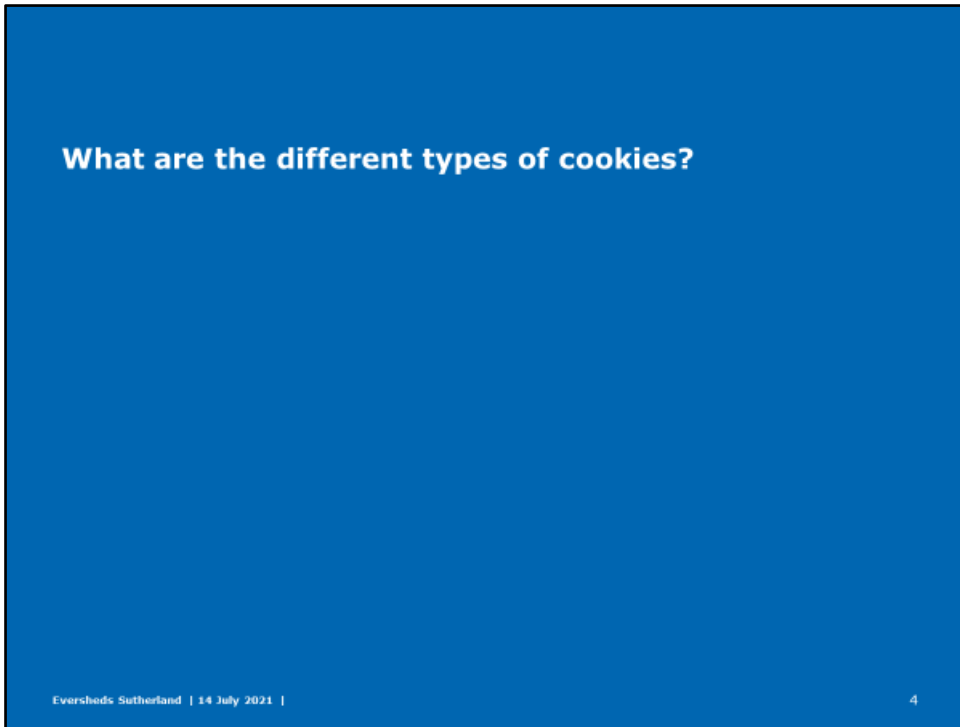
1



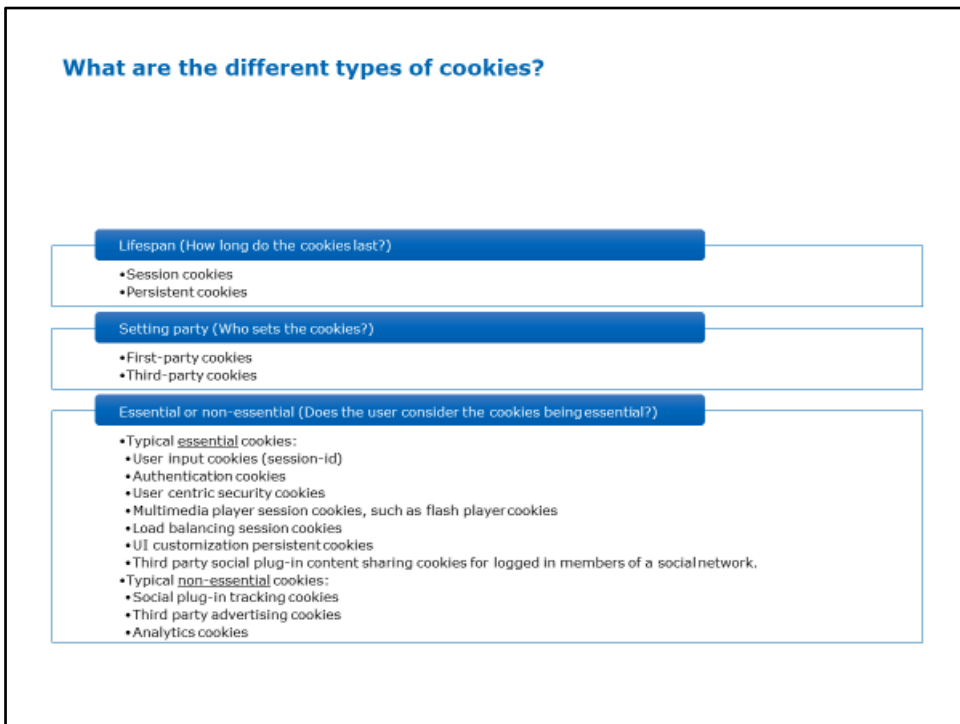
2



3



4



5

What laws regulate the use of cookies in the EU?

Eversheds Sutherland | 14 July 2021 |

6

6

What laws regulate the use of cookies in the EU?

- ePrivacy Directive: "Do we need to ask for consent before setting cookies?"
- General Data Protection Regulation: "How do we need to ask for consent before setting cookies?"
- future ePrivacy Regulation shall replace the ePrivacy Directive and may contain further or different requirements for the use of cookies.

7

Do we always need to ask the user for consent before setting any cookies?

Eversheds Sutherland | 14 July 2021 |

8

8

Do we always need to ask the user for consent before setting any cookies?

- No, depends on type of cookies
- Essential cookies: No consent needed
- Non-essential cookies: Consent needed

9

Which requirements do we have to meet when asking for consent with regard to non-essential cookies?

Eversheds Sutherland | 14 July 2021 |

10

10

Which requirements do we have to meet when asking for consent with regard to non-essential cookies?

- When asking for consent, we have to ensure that the user's consent is:
 - given prior;
 - freely given;
 - specific;
 - informed;
 - indicated unambiguously;
 - revocable at any time.

11

What does "given prior" mean?

given prior;

freely given;

specific;

informed;

indicated unambiguously;

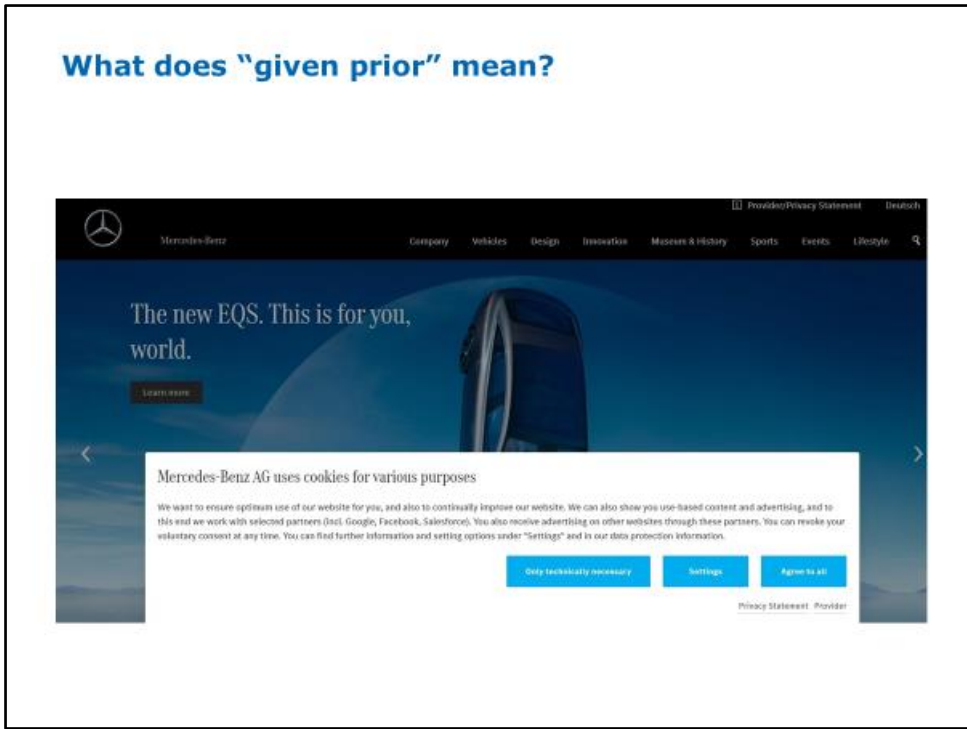
revocable at any time.

12

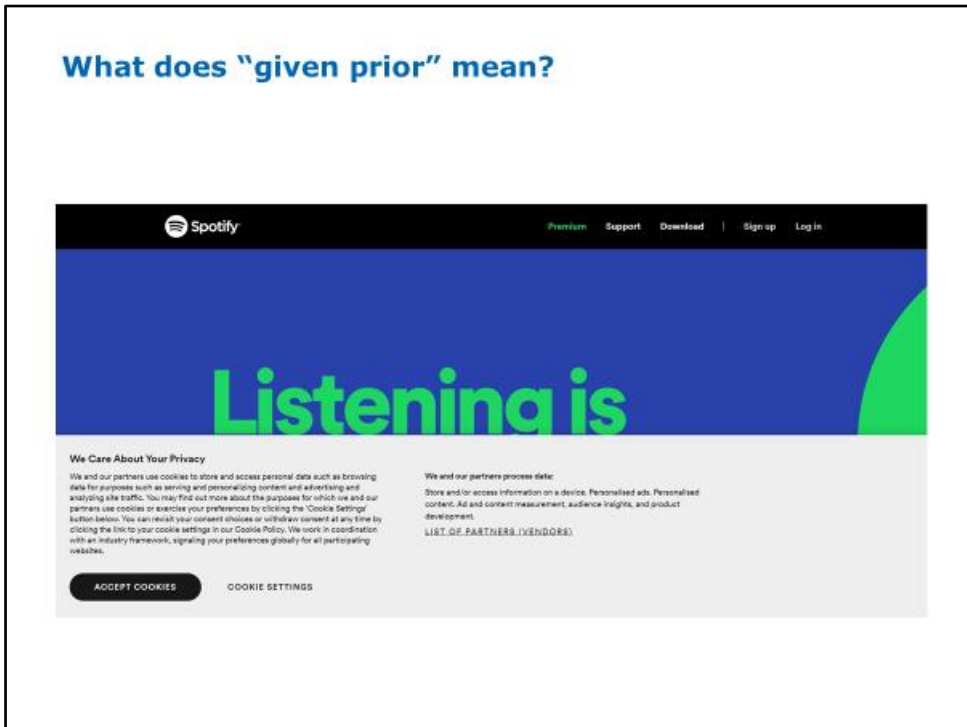
What does "given prior" mean?

- User must give consent (e.g. by clicking "Accept") before we set cookies on his device
- If user does not give consent (e.g. by clicking "Reject" or by not clicking on any the options available and going straight through to another part of our site), we cannot set cookies

13



14



15

What does "freely given" mean?

given prior;

freely given;

specific;

informed;

indicated unambiguously;

revocable at any time.

Eversheds Sutherland | 14 July 2021 |

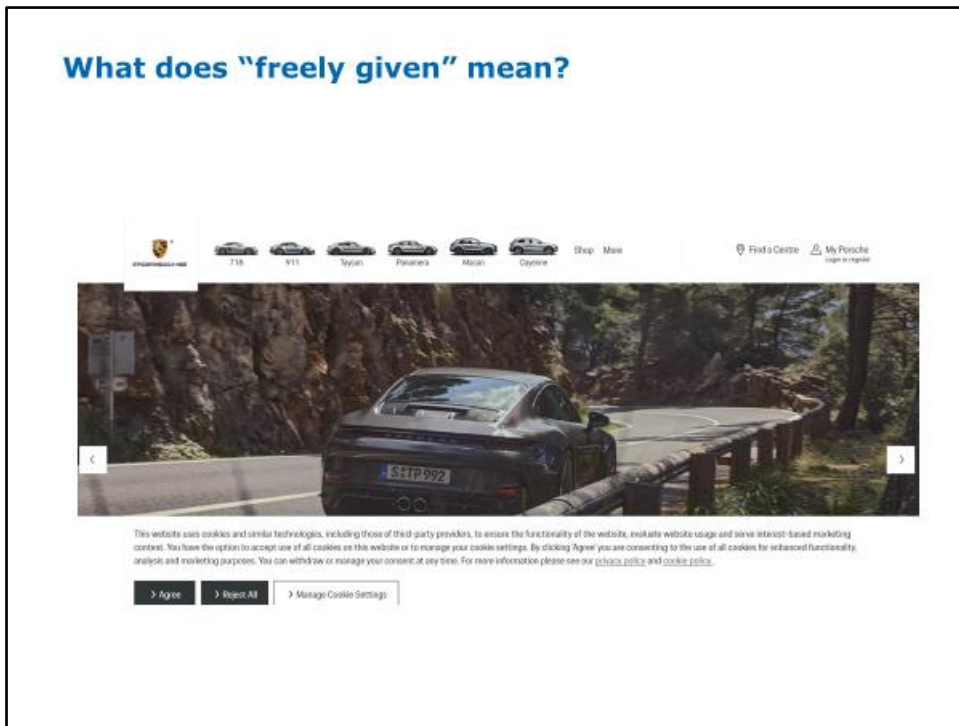
16

16

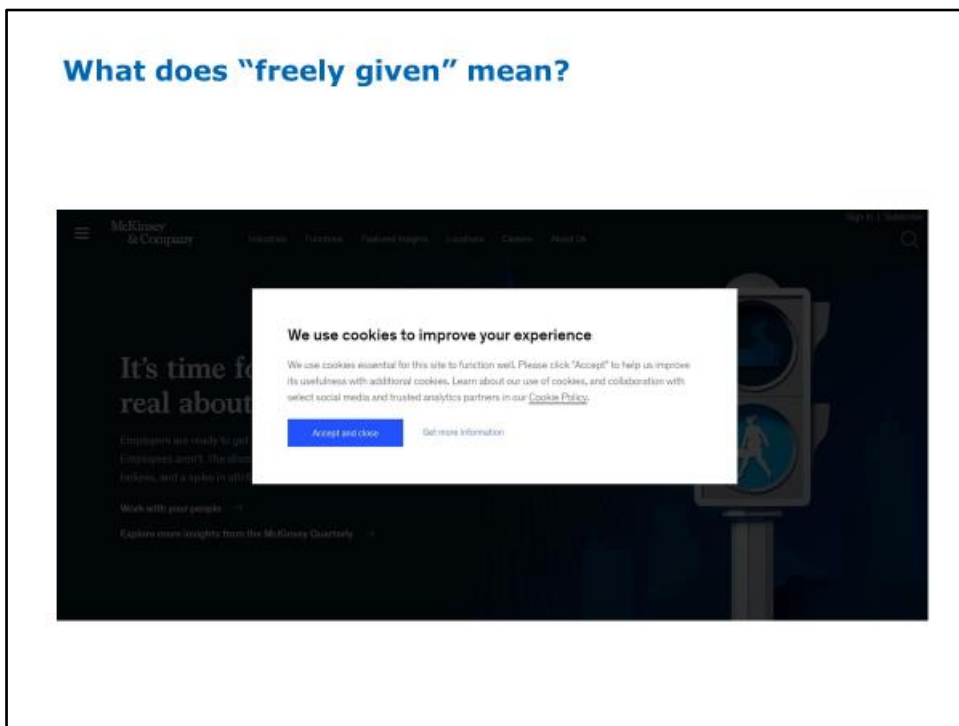
What does "freely given" mean?

- When asking for consent, we have to make clear to the user that he can make a real choice.
- We have to provide at least two options to him

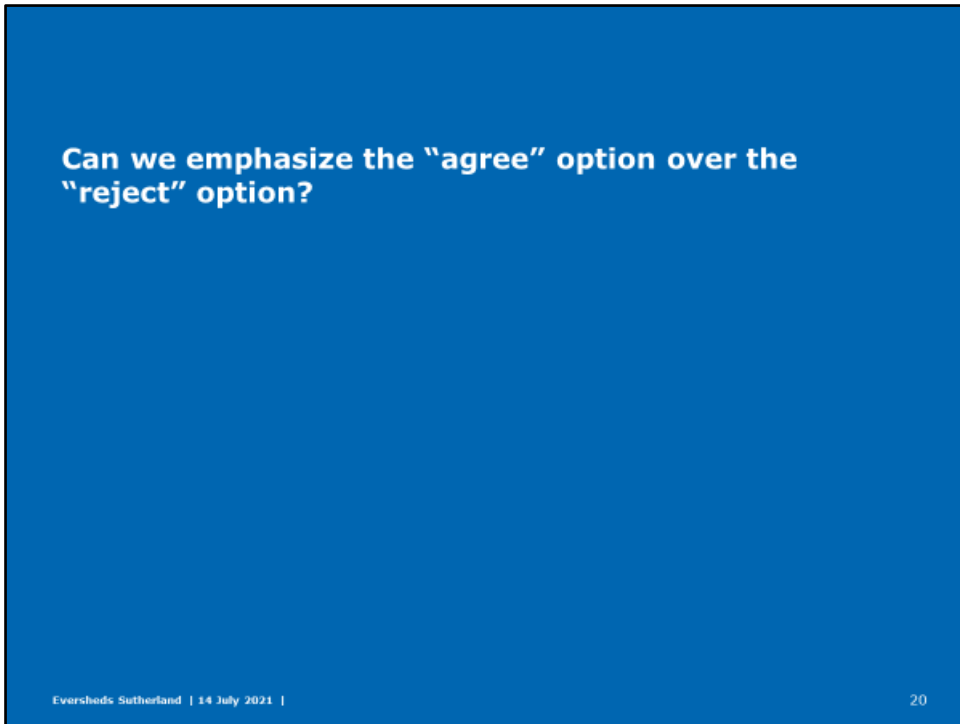
17



18



19



20

Can we emphasize the "agree" option over the "reject" option?

- Not clear if or to what extent emphasizing the "agree" option over the "reject" option (e.g. by using different colours or sizes) to influence the user towards the "agree" option is lawful:

We need your consent to set cookies on your device.
To agree, click "Accept" below.

Accept

[Reject](#) [More information](#)

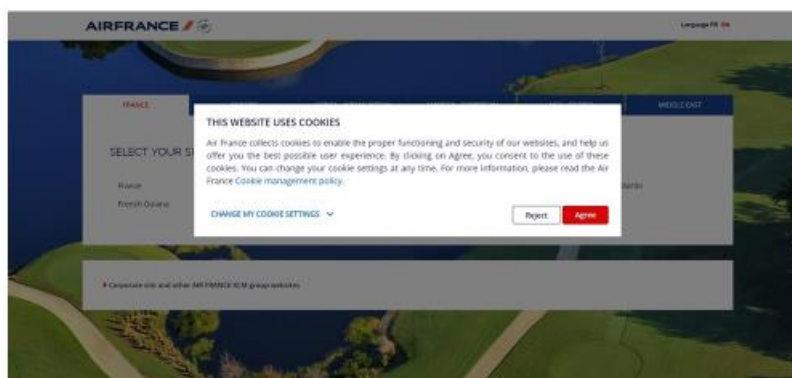
21

Can we emphasize the "agree" option over the "reject" option?

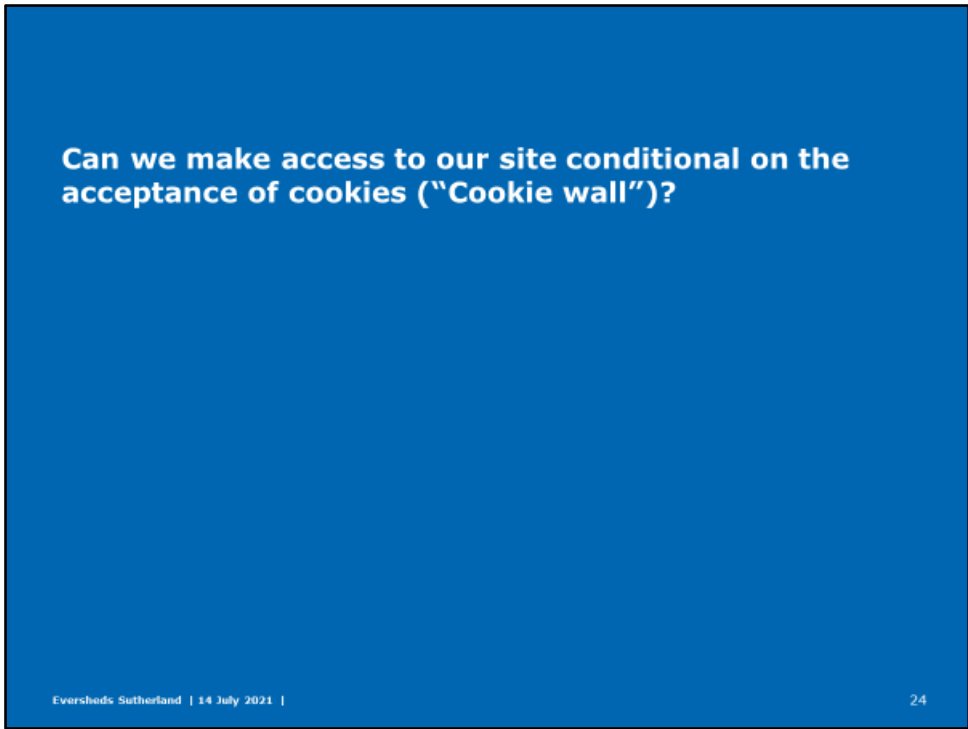
- UK data protection authority: "A consent mechanism that emphasises 'agree' or 'allow' over 'reject' or 'block' represents a non-compliant approach, as the online service is influencing users towards the 'accept' option."
- Lower-Saxony data protection authority: "If nudging is used by the controller with the aim of inducing the data subject to give consent, this may violate different legal requirements for consent under data protection law, depending on the specific design. It is clear that there are limits to permitted nudging and that behavioural manipulation can lead to invalidity of consent."

22

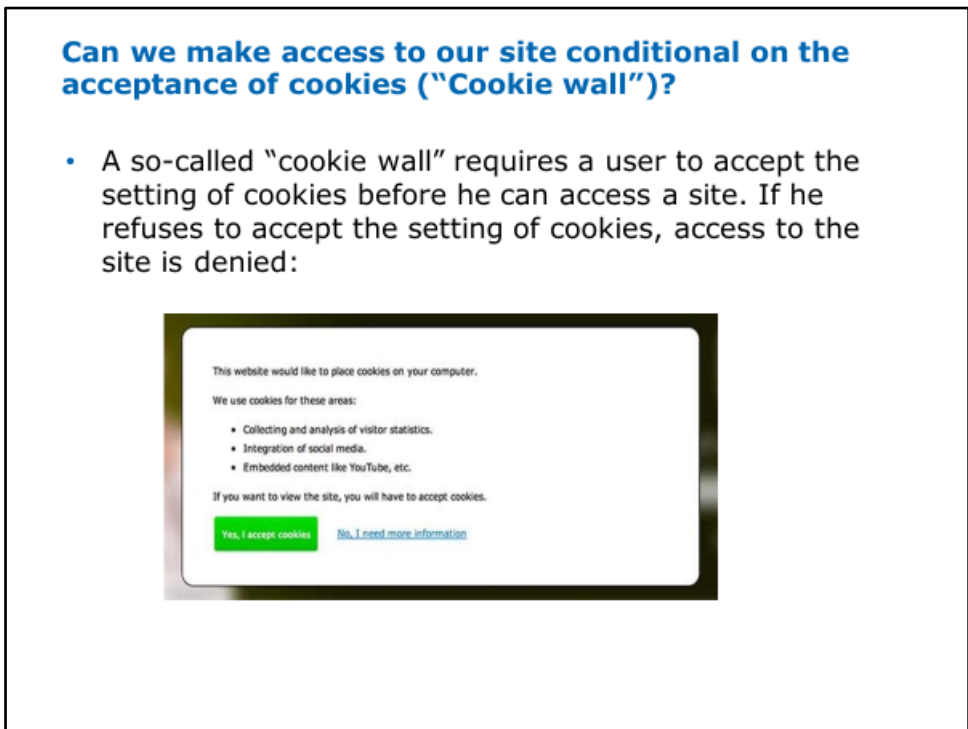
Can we emphasize the "agree" option over the "reject" option?



23



24



25

Can we make access to our site conditional on the acceptance of cookies ("Cookie wall")?

- Not clear if or to what extent the use of "cookie walls" is lawful
- EDPB: *"In order for consent to be freely given, access to services and functionalities must not be made conditional on the consent of a user to the storing of information, or gaining of access to information already stored, in the terminal equipment of a user (so called cookie walls)"*
 - **No risk approach**: If the user does not accept cookies, we still grant full access to our site (No consent = full access).
 - **Low-medium risk approach**: If the user does not accept cookies, we refuse access to some parts of our site (No consent = limited access).
 - **High risk approach**: If the user does not accept cookies, we refuse access to our entire site (No consent = no access).

26

Can we make access to our site conditional on the acceptance of cookies or on the acceptance of a payment ("Cookie or pay wall")?

27

Can we make access to our site conditional on the acceptance of cookies or on the acceptance of a payment (“Cookie or pay wall”)?

- A so-called “cookie or pay wall” requires a user to accept the setting of cookies or to make a payment before he can access a site. If he refuses to accept the setting of cookies or to make a payment, access to the site is denied:



28

Can we make access to our site conditional on the acceptance of cookies or on the acceptance of a payment (“Cookie or pay wall”)?

- Data protection authorities (e.g. the Austrian Data Protection Authority) have already accepted “cookie or pay wall” approaches
- Arg.: User has an alternative way to access the site without consenting to cookies.
- When using a “cookie or pay wall”, we must set a price which is not inappropriately high with regard to our service provided to the user.

29

What does "specific" mean?

given prior;
freely given;
specific;
informed;
indicated unambiguously;
revocable at any time.

Eversheds Sutherland | 14 July 2021 |

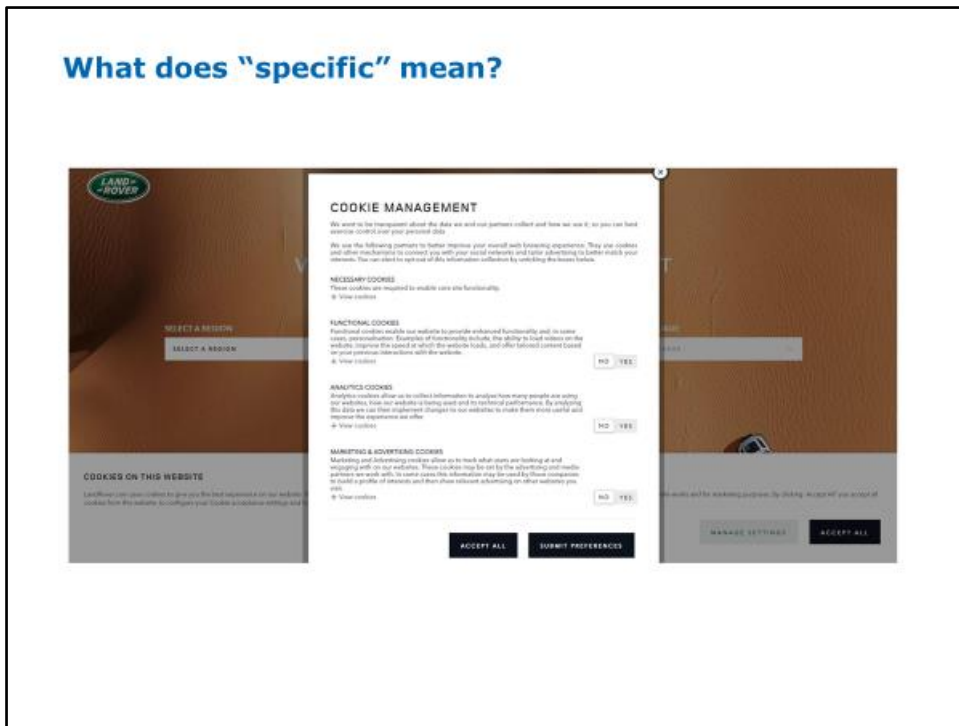
30

30

What does "specific" mean?

- If we pursue several purposes, we must separate these purposes and obtain consent for each purpose ("granularity").
- Rule of thumb: "One purpose, one tick box. Two purposes, two tick boxes."

31



32

What does "informed" mean?

given prior;
freely given;
specific;
informed;
indicated unambiguously;
revocable at any time.

Eversheds Sutherland | 14 July 2021 | 33

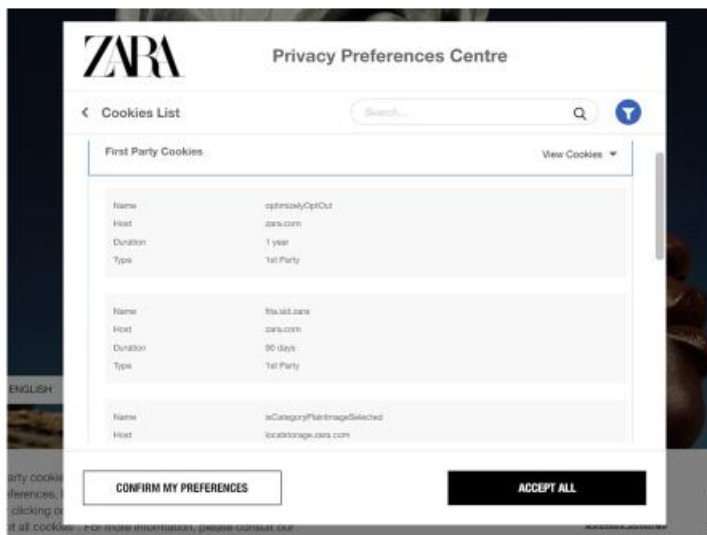
33

What does "informed" mean?

- "Informed" means that we have to inform the user about the use of cookies when asking for consent (e.g. by displaying a link to a designated location where all the types of cookies used by our site are presented).
- We have to provide at least the following information on cookies to the user:
 - Name of the cookie
 - Purpose of the cookie
 - Lifespan of the cookie (session; persistent + expiration date)
 - Third party cookies or third party access to data collected by the cookies on the site

34

What does "informed" mean?



35

What does "indicated unambiguously" mean?

given prior;

freely given;

specific;

informed;

indicated unambiguously;

revocable at any time.

36

What does "indicated unambiguously" mean?

- The user must demonstrate his consent by a positive action or other active behaviour:
 - Typical compliant mechanisms: By clicking on a button or link; by ticking a blank box.
 - Typical non-compliant mechanisms: By accepting pre-ticked "Accept"-boxes; By continuing to use our site.

37

What does "indicated unambiguously" mean?



38

What does "indicated unambiguously" mean?



39

What does "revocable at any time" mean?

given prior;
freely given;
specific;
informed;
indicated unambiguously;
revocable at any time.

Eversheds Sutherland | 14 July 2021 |

40

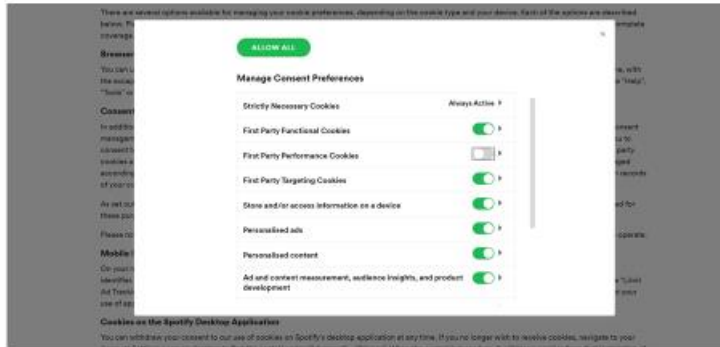
40

What does "revocable at any time" mean?

- User must be able to withdraw his consent in case he has changed his mind about cookies.
- We need to be technically capable to "reset" the cookies ("opt-out" mechanism)

41

What does "revocable at any time" mean?



42

EVERSHEDS
SUTHERLAND

Constantin Herfurth

Associate Data Protection & Cybersecurity
constantinherfurth@eversheds-
sutherland.com

Eversheds Sutherland (Germany)
Rechtsanwälte Steuerberater Solicitors
Partnerschaft mbB

Brienner Straße 12
80333 München



eversheds-sutherland.com

This information pack is intended as a guide only. Whilst the information it contains is believed to be correct, it is not a substitute for appropriate legal advice. Eversheds Sutherland (International) LLP can take no responsibility for actions taken based on the information contained in this pack.
© Eversheds Sutherland 2020. All rights reserved.

43

Materials | Compact

The new EU law for data and services

Jan Weber, Legal assistant

Hanover, September 2021

The digital age brings many new challenges, also for European consumer protection law. Therefore, the EU has enacted two packages of measures to strengthen consumer protection and adapt it to new realities.

This is to be ensured by the new directives on the provision of digital content (Digital Services Directive) and on the sale of goods (Sale of Goods Directive) as well as the directive on better enforcement and modernization of the Union's consumer protection rules (Omnibus Directive), which has its origins in the New Deal for Consumers legislative initiative. As a result, in 2019 the cornerstone has been laid for numerous new regulations relating to consumer protection: in contract and fair-trading law as well as in "digital contracts", but also for competition law. The directive has already been transposed into national law and will come into force as of 01.01.2022.

The following section discusses which changes the Digital Services Directive will have on entrepreneurs and consumers in B2C business. The changes that entrepreneurs and consumers will face as a result of the Omnibus Directive are discussed in the Compact "*New EU Law for Digital Consumer Protection*", October 2020.

Digital Content Provision Directive (Directive (EU) 2019/770)

The Digital Services Directive finds its origin in the Consumer Sales Directive (1999/44/EC) and constitutes a milestone for European contract law. The aim of the directive is to unify the national digital markets of the member states into a common digital single market (Art. 4). The resulting and controversial full harmonization is intended to guarantee a Europe-wide minimum standard of consumer protection in digital transactions.

Development of a new type of contract?

The Digital Services Directive does not contain any regulations on possible new types of contracts. In this respect, the question arises as to what type of contract the "creation / provision of data and services" can be classified as. In the foreground are initially service, purchase or rental contracts and a contract of its own type (*sui generis*).

Since rights of use often represent the actual subject matter of the service, what comes to mind first is a license agreement. Nevertheless, the type of contract required depends on the actual subject matter. The Digital Services Directive regulates the content of B2C contracts whose subject matter is the provision of digital content and data in the form of music and online videos (e.g., Spotify, YouTube), as well as services that offer the possibility of creating, processing, or storing data in digital form (e.g., software-as-a-service, cloud services), or services that enable the exchange of data (e.g., social media, online games). Due to the numerous possibilities for the provision of digital content or digital services – such as transmission on a physical medium, downloading to consumer devices, streaming, or enabling access to storage capacity for digital content or for the use of social media – the Digital Services Directive applies regardless of the type of medium used for the transmission of data or the granting of access to the digital content or digital services. However, Internet access services are excluded.

Accordingly, the type of contract is likely to be a mixed-type contract, the focus of which will be on rental/lease law, and which will also constitute a license agreement.

Purchase of goods and other services

The demarcation between the Sale of Goods Directive and the Digital Services Directive is of paramount importance for the consumer, as it determines whether the consumer must assert his rights against the seller of the physical IoT product or the provider of digital goods. The demarcation usually takes place via the content of the contract.

The Sale of Goods Directive contains rules on certain requirements for contracts for the sale of goods. This also includes "goods with digital elements". These are goods that contain digital content or services or are linked to them in such a way that the goods would not be able to perform their functions without this digital content or service (Article 3 (3) of the Directive). In addition, in case of doubt, the seller of goods is to be liable for the contractual conformity of those digital contents and digital services that are included in or connected to an IoT product from the outset. Consequently, the seller bears considerable risks. However, he can avoid these if he expressly agrees in the contract that the digital goods are not dependent on the product. In addition, he must try to hedge the risk through a detailed back-to-back agreement with the producer of the digital elements. Comparing both directives, it must be noted that the consumer rights of the Sale of Goods Directive do not go as far as those of the Digital Services Directive.

Personal data as counter-performance

One of the new basic ideas of the Digital Services Directive is to allow counter-performance not only in the form of money, but also in the form of personal data or a combination of both. This shall apply to contracts that offer the provision of digital content and digital services where the consumer's counter-performance consists of providing the entrepreneur with his or her personal data for commercial use. However, personal data will not be accepted as a new means of payment if it is processed solely for the purpose of providing the digital content or services or for the purpose of complying with legal requirements and the trader does not process it for any other purpose.

The use of the term "personal data" corresponds to the definition in the General Data Protection Regulation (GDPR) in Art. 4 No. 1 GDPR. Thus, the data processing is subject to the level of protection of the GDPR. However, the very idea of accepting personal data in return could conflict with the protective purpose of the GDPR. Accordingly, on the one hand, consumers could be incentivized to offer their personal data - which are supposed to be afforded a higher level of protection under the GDPR - in exchange for comprehensive warranty rights, guarantees and extensive liability on the part of the contractual partner. On the other hand, the EU is reacting to the current reality, in which companies have long been paying consumers with data, and is enabling consumers to receive a better service in return. Classic examples of consumers already paying with their data can be found in the areas of "free" apps, social networks, the use of "smart products" and cookies, which generate personalized advertising, among other things. Consequently, the Digital Services Directive can bring about greater consumer protection in these areas.

Innovations in consumer law

In accordance with its purpose, the Digital Services Directive leads to numerous changes in consumer law, the most important of which are examined in more detail below.

Conformity with the contract

According to the Digital Services Directive, a product is now only in conformity with the contract if it has a large number of objective performance characteristics. This is contrary to the previous system of Section 434 of the German Civil Code (BGB), in which what matters most is what has been contractually agreed (subjective features). Possible performance features can be, among others, functionality, compatibility, continuity, and safety of the product. But also "public statements" of the entrepreneur shall become objective criteria, whereby especially advertising statements become part of the "conformity with the contract". In any case, the seller must deliver what the consumer can "reasonably expect" for goods of the respective type, Art. 7 and 8 Digital Services Directive.

Duty to update

Article 8 (2) b of the Digital Services Directive introduces a further novelty and a further break in the system. According to this, an objective requirement arises in such a way that the digital goods must be updated (post-contractually) even if the contract only stipulates a one-time provision, but the consumer may reasonably expect the update based on the nature and purpose of the contract and considering the circumstances. The resulting expansion of the scope of obligations gives rise to the problem that the provider must price in the costs of future updating obligations from the outset (ex-ante), although the scope, number and duration of these future obligations depend on many factors and are often only determined ex post. The exact scope of the duty to update is currently still unclear, and case law will have to determine it.

No waiver

Another important point is that the objective requirements cannot be unilaterally waived by the entrepreneur in his general terms and conditions. A deviation is only possible if the consumer is already aware of it when the contract is concluded and expressly agrees to it in a separate declaration.

Warranty rights for digital content or digital services

The Digital Services Directive also provides the consumer with warranty rights similar to those under sales law. Thus, in the event of non-contractual performance, the consumer can demand that the digital content or digital services be restored to their contractual condition, a pro-rata price reduction or termination of the contract. Failures in the provision of the service can also lead to termination of the contract.

Change in the duration of the reversal of the burden of proof

Another important change is the duration of the reversal of the burden of proof in the case of consumer sales. Previously, Section 477 of the German Civil Code stipulated i.e. that in the event of a material defect within six months of the transfer of risk, it was presumed that the defect already existed at the time of the transfer of risk. Thus, the burden of proof is on the seller. The Digital Services Directive extends this period by a further six months and thus to a full year. In the case of a one-time exchange of digital content or services, the reversal of the burden of proof will apply for up to one year after provision, whereas it will apply to continuing obligations for their entire duration.

How to react? Suggestions for companies

The Digital Services Directive has already been transposed into German law. The changes will apply from January 1, 2022. It remains to be seen whether the legislature has succeeded in the complex task of implementing the directive in a compliant manner. Companies should now at the latest deal with the legal innovations already published and adapt their business models and consumer contracts to these in order to avoid costly warnings from consumer protection associations and competitors. The earlier the problem is addressed, the higher the quality of the solution.

+ + +

Chapter Six

Data Protection (National)

THE GENERAL DATA PROTECTION REGULATION

Prof. Dr. Christiane Trüe LL.M.
University of Bremen

Counsel to Herfurth & Partner
Hannover / Brussels



1

*Understanding data protection law
is like nailing jelly to a wall'*

2

OVERVIEW

- Legal Basis: Application of GDPR
- Definitions
- Conflicting Basic Rights and Interests
- Legal Consequences of Infringement:
Liability and Fines

3

APPLICATION

4

APPLICATION OF GDPR

- Regulation (EU) 2016/679
- Entered into force in May 2018
- Precedence before Member State Law
- Direct application in EU
- Supplementation by Member State legislation

5

APPLICATION OF GDPR

- Until 2018: Member State data protection law
- Harmonised by EU data protection directive 95/46/EC
- Implemented in Germany:
 - 1x Federal Data Protection Statute (Bundesdatenschutzgesetz)
 - 16x Federal States' data protection statutes
- Ok for administration/public services
- Good for business in internal market?
- 1995: different computer era before Social Media etc

6

APPLICATION OF GDPR

- Framework act – continued existence of federal states' and federal law with slight differences
- Acts supplementing the GDPR:
 - 1x Federal Data Protection Statute (Bundesdatenschutzgesetz)
 - 16x Federal States' data protection supplementary statutes
 - E.g. Bremisches Ausführungsgesetz zur EU-Datenschutz-Grundverordnung (BremDSGVOAG)
 - Alternative: Federal states' Treaty (Staatsvertrag)
- EU: Implementing Regulation for EU authorities and agencies etc

7

AIMS OF GDPR

- Better data access, more transparency, more control for data subjects
- Closure of protection gaps
- Uniform provisions for all Member States/authorities/court interpretation
- Cross-border co-operation of data protection authorities within EU

8

SCOPE OF APPLICATION OF GDPR

Article 3 Territorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
 - a. the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
 - b. the monitoring of their behaviour as far as their behaviour takes place within the Union.
3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

9

SCOPE OF APPLICATION OF GDPR

Article 2 Material scope

(1) This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. ...

10

SCOPE OF APPLICATION OF GDPR

(2) This Regulation does not apply to the processing of personal data:

- a. in the course of an activity which falls outside the scope of Union law;
- b. by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU; -> Common Foreign and Security Policy
- c. by a natural person in the course of a purely personal or household activity;
- d. by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. -> separate Directive

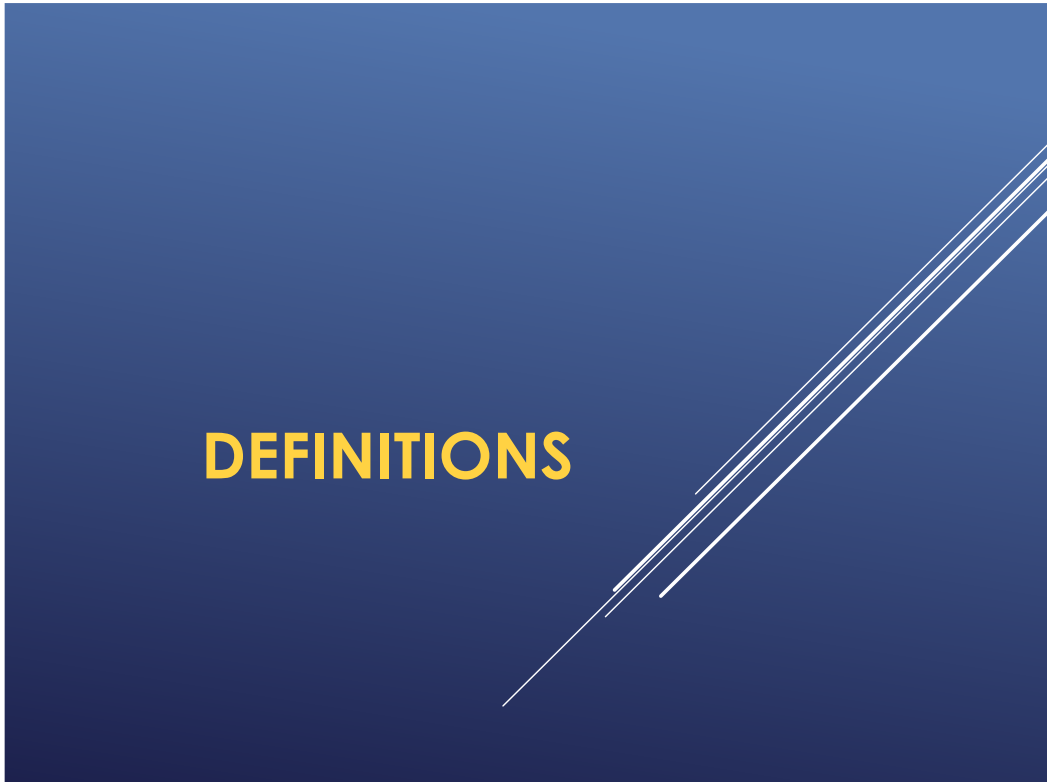
11

SCOPE OF APPLICATION OF GDPR

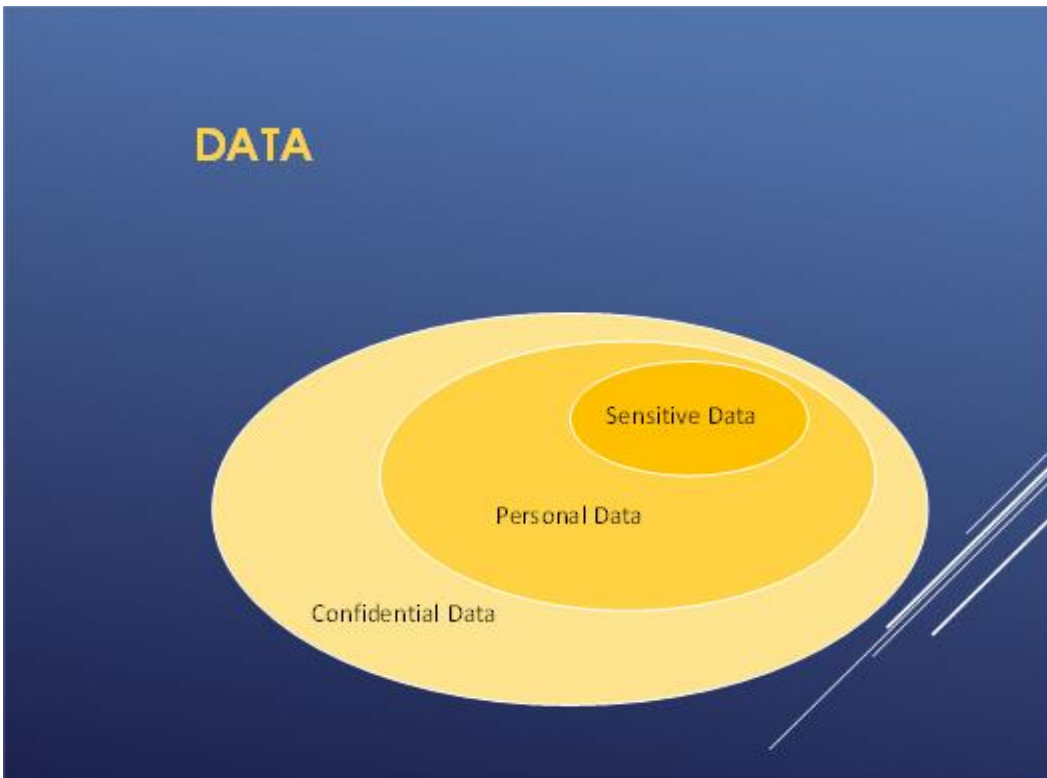
Article 3 Territorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
 - a. the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
 - b. the monitoring of their behaviour as far as their behaviour takes place within the Union.
3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

12



13



14

DEFINITIONS - ART. 4 GDPR PERSONAL DATA

- 1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject');
- 2) an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

15

PERSONAL DATA

- ▶ Name
- ▶ Date of Birth
- ▶ Gender
- ▶ Address
- ▶ Phone Number
- ▶ Email address
- ▶ Membership Number
- ▶ IP Address
- ▶ Browser cookies
- ▶ Photograph / videos etc



16

SENSITIVE DATA - ART. 4 NO 13, 14, 15 GDPR

Specifically protected:

1. '*genetic data*' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;
2. '*biometric data*' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;
3. '*data concerning health*' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

17

PROCESSING OF SENSITIVE DATA

Sensitive Data – prohibition of processing (subject to exceptions including consent or legitimate purpose): Art. 9

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or
2. trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited. ...

18

SPECIAL CATEGORIES OF DATA

GROUND LABS

GDPR: Types of Data under Protection

Personal Data	Sensitive Personal Data
Names	Health Data
Location Data	General Data
Identification Numbers	Biometric Data
IP Addresses	Racial or Ethnic Data
Cookie Data	Political Opinions
RFID Tags	Sexual Orientation

GROUNDLABS.COM

19

SPECIAL CATEGORIES OF DATA

Example of a special category of data

<h4 style="margin: 0;">BIOMETRIC DATA</h4> <ul style="list-style-type: none"> facial recognition fingerprints voice recognition iris scanning palprint verification retina recognition ear shape recognition 	<h4 style="margin: 0;">HEALTH DATA</h4> <ul style="list-style-type: none"> patient medical history data on disability illnesses, medical diagnosis, medical treatment, medical opinions fitness tracker data 	<h4 style="margin: 0;">GENETIC DATA</h4> <ul style="list-style-type: none"> chromosomal analysis DNA analysis RNA analysis
---	---	---

20

DATA PROCESSING PRINCIPLES - ART 5 (1) GDPR

Important principles:

- lawfulness, fairness and transparency
-> what does that mean?
- specified, explicit and legitimate purposes only
-> what does that mean?
- data minimization
-> what does that mean?

21

DATA PROCESSING PRINCIPLES - ART 5 (1) GDPR

Personal data shall be: ...

- a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
- b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; ...
- c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')

22



23



24

GDPR OBJECTIVES

Article 1 Subject matter and objectives

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.
2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.
3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

25

CONFLICTING BASIC RIGHTS/HUMAN RIGHTS

⇒ Individual Rights

⇒ Condition of progress of society: Necessity of open discourse

26

CONFLICTING BASIC RIGHTS/HUMAN RIGHTS: EU FUNDAMENTAL RIGHTS CHARTA

Article 7 Respect for private and family life

Everyone has the right to respect for his or her private and family life, home and communications.

Article 8 Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

27

RIGHTS OF THE DATA SUBJECT

- ▶ Access (Art. 15 GDPR)
- ▶ Rectification (Art. 16 GDPR)
- ▶ Be forgotten (Art. 17 GDPR)
- ▶ Data portability (Art. 20 GDPR)
- ▶ Right to object (Art. 21 GDPR)

28

INFRINGEMENTS LIABILITY & FINES

29

PROCEDURAL AND INSTITUTIONAL PROTECTION OF DATA

- Security of Processing data by technical and organizational measures against unlawful access or loss of data (Art. 32);
- Obligation of Member States to maintain one or more independent supervisory authorities (Art. 51);
 - European Data Protection Board (EDPB) (Art. 68)
 - Provides Guidelines und Codes of best Practice
- Obligation of Data processors and controllers to
 - Keep records of data processing
 - Designate data protection officers (Art. 37)
 - Codes of Conduct (Art. 40)
 - Duty to notify of personal data breaches
 - Data protection impact assessment

30

PROCEDURAL AND INSTITUTIONAL PROTECTION OF DATA

- Right to lodge a complaint with a supervisory authority (Art. 77)
- Right to an effective judicial remedy against a supervisory authority (Art. 78)
- Right to an effective judicial remedy against a controller or processor (Art. 79)
- Right to compensation and liability (Art. 82)

31

LIABILITY FOR BREACHES

- For material and non-material damage
- Joint and several liability: everyone involved in the breach on the whole damage
- Art. 82 GDPR



32

FINES

- shall in each individual case be effective, proportionate and dissuasive'
- up to € 10 mio / € 20 mio
- Undertakings up to 2%/4% turn-over
- Art. 83 GDPR



33

DATA PROTECTION OFFICER (DPO)

DPO qualification

- ▶ Expertise in Data Protection & privacy laws, in depth understanding of the GDPR
- ▶ Knowledge of specific business sector of the company
- ▶ Knowledge of the administrative rules & procedures
- ▶ Integrity & high professional ethics



34

PROCEDURAL AND INSTITUTIONAL PROTECTION OF DATA

Art. 32 Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement **appropriate technical and organisational measures** to ensure a level of security appropriate to the risk, including inter alia as appropriate:
 - a) the pseudonymisation and encryption of personal data;
 - b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
 - c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
 - d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing....

35

TOPICS

Topic 1:

Which provisions exist to balance privacy and data protection against the rights to information and commercial activity? Are they adequate?

Topic 2:

There are procedural instruments for data protection where data processing is permitted. Are they adequate?

Topic 3:

The aims of the GDPR are better data access, more transparency, more control for data subjects, closure of protection gaps, uniform provisions for all Member States/authorities/court interpretation, cross-border co-operation of data protection authorities within EU – how far are these achieved?

36

THANK YOU FOR LISTENING

Prof. Dr. Christiane Trüe LL.M.
University of Bremen

Counsel to Herfurth & Partner
Hannover / Brussels

truee@herfurth.de



Questions and Answers

Data Protection

Does a Data Protection Act or any other data protection law exist in your country?

Cheril (China):

Judging from the existing laws in China, data security is only mentioned in the Civil Code of the People's Republic of China and Cyber Security Law of the People's Republic of China. Recently, the Chinese legislature deliberated and passed the Data Security Law of the People's Republic of China, which will be officially implemented on September 1st, 2021. It is the Chinese first special law on data security when it enters into force.

This law has the following advantages: First, the definition of "data" is clearly defined: the term "data" in the law refers to any electronic or other recording of information, which was never being clearly defined before. Second, it clarifies the obligations of data processing activities boundaries. "Data processing" includes but not limited to the collection, storage, use, processing, transmission, provision, and public disclosure of data. Third, the state shall establish a categorized and hierarchical data protection system to provide categorized and hierarchical protection for data based on the importance of data in economic and social development and the degree of harm caused by data tampering, destruction, or divulgence or illegal acquisition or utilization of data to national security, public interest, or lawful rights and interests of individuals and organizations.

All in all, for all aspects and links involved in data security supervision and protection, the "Data Security Law" is more of an outline and has made institutional arrangements. Some specific rules or details have yet to be explored and summarized in practice, as well as other supporting facilities in the future. The laws and regulations are further clarified.

Wenzhu Lan (China):

Internet security Law and The data security law which shall come into force as of September 1, 2021 and Two administrative regulations, twenty-seven departmental rules and one judicial interpretation

Ana Marija Đurić (Croatia):

Yes, Croatia has an Act on the Implementation of the General Regulation on Data Protection.

L. Tuncer (Netherlands):


Yes, the GDPR (AVG) applies in The Netherlands, also there is a law called 'Trade secrets protection law' (WBB) implemented recently, intended to prevent illegal distribution and theft of trade secrets.

Zoë Jardim (Brazil):

Yes it did, as mentioned above. In Brazil we have the Lei Geral da Proteção de Dados.

Chapter Seven

IP & IT Information Websites



Sources of Information for
IP and IT


Alliuris Summer School 2021

22 July 2021

Antonia Herfurth
Attorney at law in Hanover and
Munich
Herfurth & Partner, Hanover

1

Information Sources IP and IT | herfurth.partner



Source: <https://makeameme.org/meme/sources-sources-everywhere>

22 July 2021 | Alliuris Summer School 2021

2

2

Information Sources IP and IT | herfurth.partner

Overview

- Eur-Lex 
- DLA Piper – Data Protection Laws of the World 
- TLDRLegal 
- Choose a Licence
- Online libraries 
- IP offices and databases 







22 July 2021 | Alliuris Summer School 2021 3

3


Information Sources IP and IT | herfurth.partner

Eur-Lex

22 July 2021 | Alliuris Summer School 2021 4

4

Information Sources IP and IT | herfurth.partner




Source: <https://eur-lex.europa.eu/homepage.html?locale=en>

22 July 2021 | Alluris Summer School 2021

5

5

Information Sources IP and IT | herfurth.partner



Source: <https://eur-lex.europa.eu/browse/summaries.html>

22 July 2021 | Alluris Summer School 2021

6

6

Information Sources IP and IT | herfurth.partner

The screenshot shows the 'Digital single market' summary page on the EU Legislation website. The page title is 'Digital single market'. The main content area includes a blue circular icon with a white 'i' and the text: 'Under the Treaty on the Functioning of the European Union (Articles 179-180), the EU aims to open up digital opportunities for people and businesses, making full use of the potential of digital data to benefit the economy and society. The EU aims to make its single market fit for the digital age. This means eliminating unnecessary regulatory barriers and moving from individual national markets to a single EU-wide rulebook.' Below this, there are several bullet points: 'General rules', 'Electronic communication networks', 'Personal data & privacy rules', 'EU copyright & audiovisual rules', 'EU data economy & data protection', and 'Archived summaries'. A 'See also:' section lists 'Audiovisual and media' and 'Internal market'. The source URL is <https://eur-lex.europa.eu/summary/chapter/31.html>. The footer of the screenshot shows '22 July 2021 | Alliuris Summer School 2021' and the number '7'.

Source: <https://eur-lex.europa.eu/summary/chapter/31.html>

22 July 2021 | Alliuris Summer School 2021 7

7

Information Sources IP and IT | herfurth.partner

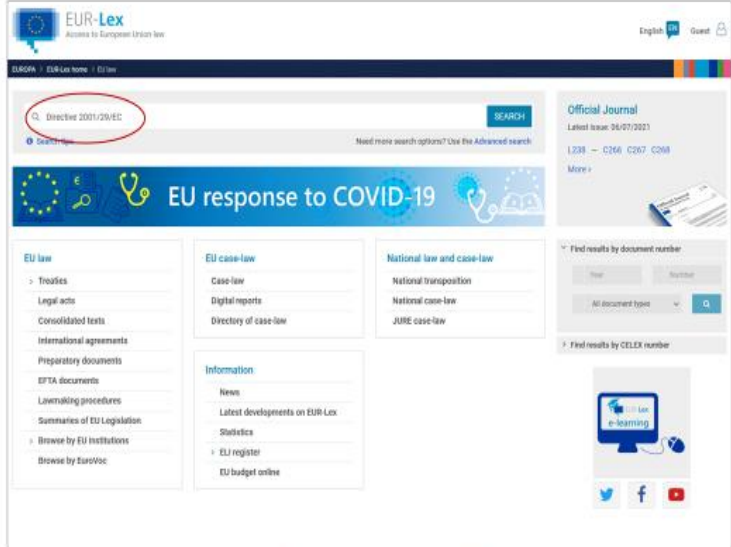
The screenshot shows the 'EU copyright & audiovisual rules' summary page on the EU Legislation website. The page title is 'EU copyright & audiovisual rules'. The main content area includes the text: 'Regulation implementing the Marrakesh Treaty in the EU Copyright and related rights in the Digital Single Market'. Below this, there are two main sections: 'Copyright' and 'EU audiovisual rules'. The 'Copyright' section lists: 'Wider access to copyright material – orphan works', 'The Marrakesh Treaty', 'Directive implementing the Marrakesh Treaty in the EU', 'Resale right for the benefit of the author of an original work of art', 'Copyright and related rights: term of protection', 'Copyright and related rights in the information society', 'Computer programs – legal protection', 'Legal protection: databases', 'Copyright and related rights: satellite broadcasting and cable retransmission', 'Rental, lending and certain other rights related to copyright in the field of intellectual property', and 'Copyright – broadcasters' online transmissions and retransmissions of television and radio programmes'. The 'EU audiovisual rules' section lists: 'Enjoying online content without borders', 'Beijing Treaty on Audiovisual Performances', 'Audiovisual Media Services Directive (AVMSD)', and 'Improving the online licensing of music across the EU'. The source URL is <https://eur-lex.europa.eu/summary/chapter/3109.html>. The footer of the screenshot shows '22 July 2021 | Alliuris Summer School 2021' and the number '8'.

Source: <https://eur-lex.europa.eu/summary/chapter/3109.html>

22 July 2021 | Alliuris Summer School 2021 8

8

Information Sources IP and IT | herfurth.partner



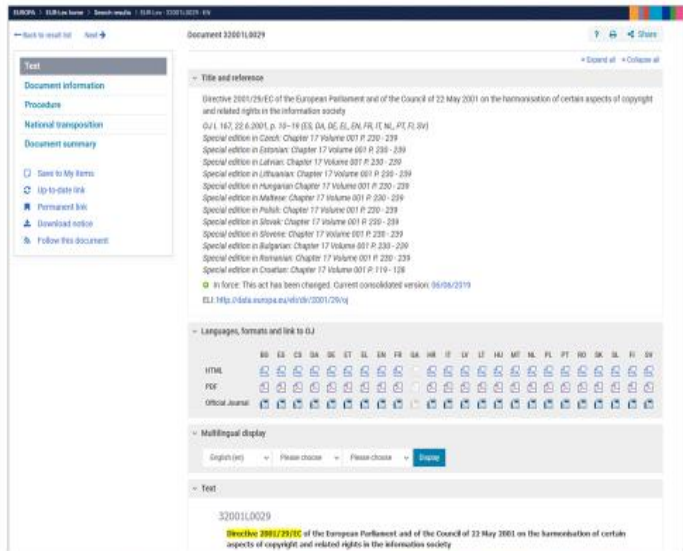
Source: <https://eur-lex.europa.eu/homepage.html?locale=en>

22 July 2021 | Alluris Summer School 2021

9

9

Information Sources IP and IT | herfurth.partner



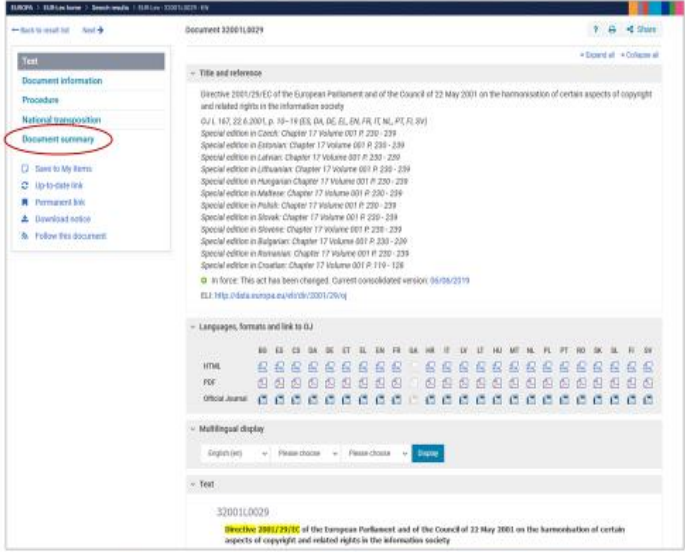
Source: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32001L0029&qid=1625588767971>

22 July 2021 | Alluris Summer School 2021

10

10

Information Sources IP and IT | herfurth.partner



Document 32001L0029

Document information

Procedure

National transposition

Document summary

Save to My Items

Up-to-date link

Permanent link

Download notice

Follow this document

Title and reference

Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society

OJ L 167, 22.6.2001, p. 10–19 (ES, DA, DE, EL, EN, FR, IT, NL, PT, FI, SV)

Special edition in Czech: Chapter 17 Volume 001 P 220–239

Special edition in Estonian: Chapter 17 Volume 001 P 230–239

Special edition in Latvian: Chapter 17 Volume 001 P 230–239

Special edition in Lithuanian: Chapter 17 Volume 001 P 230–239

Special edition in Hungarian Chapter 17 Volume 001 P 220–239

Special edition in Maltese: Chapter 17 Volume 001 P 230–239

Special edition in Polish: Chapter 17 Volume 001 P 220–239

Special edition in Slovak: Chapter 17 Volume 001 P 220–239

Special edition in Slovene: Chapter 17 Volume 001 P 220–239

Special edition in Bulgarian: Chapter 17 Volume 001 P 230–239

Special edition in Romanian: Chapter 17 Volume 001 P 220–239

Special edition in Croatian: Chapter 17 Volume 001 P 119–126

In force. This act has been changed. Current consolidated version: 06/09/2019

EU: <http://data.europa.eu/eli/dir/2001/29/oj>

Languages, formats and link to OJ

	ES	EL	CZ	DA	DE	ET	FI	FR	GA	HR	IT	LV	LT	HU	MT	NL	PL	PT	RO	SK	SL	SV
HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML
PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF
Official Journal	Official Journal	Official Journal	Official Journal	Official Journal	Official Journal	Official Journal	Official Journal	Official Journal	Official Journal	Official Journal	Official Journal	Official Journal	Official Journal	Official Journal	Official Journal	Official Journal	Official Journal	Official Journal	Official Journal	Official Journal	Official Journal	Official Journal

Multilingual display

English (en) | Please choose | Please choose | [Print](#)

Text

32001L0029

Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society

Source: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32001L0029&qid=1625588767971>

22 July 2021 | Alluris Summer School 2021

11

11

Information Sources IP and IT | herfurth.partner

Copyright and related rights in the information society

SUMMARY OF:

[Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society](#)

SUMMARY

WHAT DOES THE DIRECTIVE DO?

The directive aims to adapt legislation on copyright and related rights to technological developments and particularly to the information society, while providing for a high level of protection of intellectual property. In addition, it implements 2 international treaties that were concluded in December 1996: the [WIPO Copyright Treaty](#) and the [WIPO Performances and Phonograms Treaty](#).

It is 1 of the 10 directives, including those on the enforcement of intellectual property rights, orphan works, and the collective management of copyright and related rights, which together comprise the EU's copyright legislation.

KEY POINTS

The directive harmonises key rights granted to authors and neighbouring rightsholders (the reproduction right, the right of communication to the public and the distribution right) and — to a lesser degree — exceptions and limitations to these rights. It also harmonises the protection of technological measures and of rights management information, sanctions and remedies.

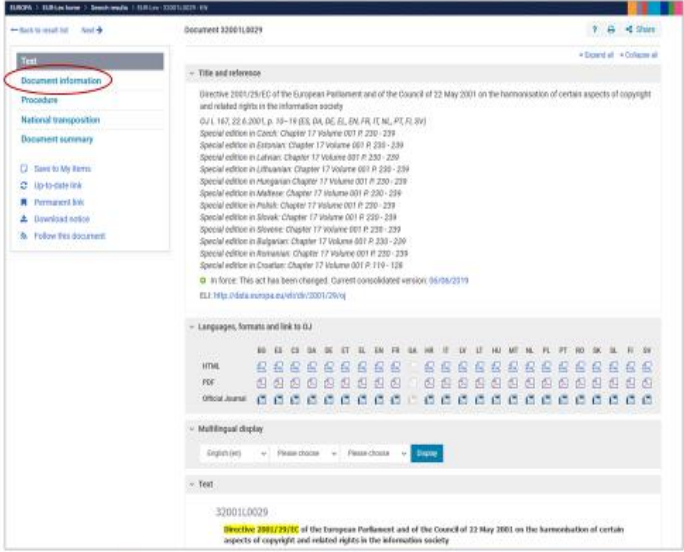
Source: <https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32001L0029>

22 July 2021 | Alluris Summer School 2021

12

12

Information Sources IP and IT | herfurth.partner



Document 32001L0029

Title and reference

Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society

OJ L 167, 22.6.2001, p. 10–19 (ES, DA, DE, EL, EN, FR, IT, NL, PT, FI, SV)

Special edition in Czech: Chapter 17 Volume 001 P 220–239

Special edition in Estonian: Chapter 17 Volume 001 P 230–239

Special edition in Latvian: Chapter 17 Volume 001 P 230–239

Special edition in Lithuanian: Chapter 17 Volume 001 P 230–239

Special edition in Hungarian Chapter 17 Volume 001 P 220–239

Special edition in Maltese: Chapter 17 Volume 001 P 230–239

Special edition in Polish: Chapter 17 Volume 001 P 220–239

Special edition in Slovak: Chapter 17 Volume 001 P 220–239

Special edition in Slovene: Chapter 17 Volume 001 P 220–239

Special edition in Bulgarian: Chapter 17 Volume 001 P 230–239

Special edition in Romanian: Chapter 17 Volume 001 P 230–239

Special edition in Croatian: Chapter 17 Volume 001 P 119–126

In force. This act has been changed. Current consolidated version: 06/09/2019

EU: <http://data.europa.eu/eli/dir/2001/29/oj>

Languages, formats and link to OJ

	BG	ES	CS	DA	DE	EL	EN	FR	GA	HR	IT	LV	LT	HU	MT	NL	PL	PT	RO	SK	SL	FI	SV
HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML
PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF
Official Journal	Official Journal	Official Journal	Official Journal	Official Journal	Official Journal	Official Journal	Official Journal	Official Journal	Official Journal	Official Journal	Official Journal	Official Journal	Official Journal	Official Journal	Official Journal	Official Journal	Official Journal	Official Journal	Official Journal	Official Journal	Official Journal	Official Journal	Official Journal

Multilingual display

English (en) | Please choose | Please choose | [Print](#)

Text

32001L0029

Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society

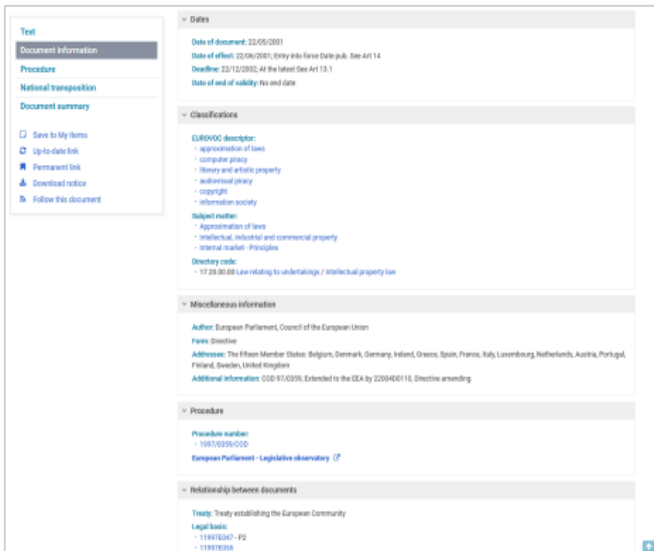
Source: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32001L0029&qid=1625588767971>

22 July 2021 | Alluris Summer School 2021

13

13

Information Sources IP and IT | herfurth.partner



Text

Document information

Procedure

National transposition

Document summary

Save to My Items

Up-to-date link

Permanent link

Download notice

Follow this document

Dates

Date of document: 22/05/2001

Date of effect: 22/06/2001; Entry into force date/pub. see Art 14

Deadline: 22/12/2002; at the latest (see Art 13.1)

Date of end of validity: no end date

Classifications

EUROVOC descriptor:

- approximation of laws
- computer piracy
- history and author's property
- intellectual property
- copyright
- information society

Subject matter:

- approximation of laws
- intellectual, industrial and commercial property
- internal market- Principles

Directory code:

- 17.25.00.00 Law relating to undertakings; intellectual property law

Miscellaneous information

Author: European Parliament, Council of the European Union

Part of: Directive

Addressed to: The fifteen Member States: Belgium, Denmark, Germany, Ireland, Greece, Spain, France, Italy, Luxembourg, Netherlands, Austria, Portugal, Finland, Sweden, United Kingdom

Additional information: COD 97.0335; Extended to the EEA by 2004/00116; Directive amending

Procedures

Procedure number:

- 1997/0335/000

European Parliament - Legislative observatory [LP](#)

Relationship between documents

Treaty: Treaty establishing the European Community

Legal basis:

- 11987307 - P2
- 11987308

Source: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32001L0029&qid=1625588767971>

22 July 2021 | Alluris Summer School 2021

14

14

Information Sources IP and IT | herfurth.partner

Text

Document information

Procedure

National transposition

Document summary

- Save to My items
- Up-to-date link
- Permanent link
- Download notice
- Follow this document

Affected by case:

- A04P2 Declared valid 62004CJ0479
- A04P2 Interpreted by 62004CJ0479
- A03P1 Interpreted by 62005CJ0306
- Interpreted by 62006CA0275
- article 4.1 Interpreted by 62006CA0456
- Interpreted by 62006CJ0275
- A04P1 Interpreted by 62006CJ0456
- article 5.1 PT A) interpretation requested by 62007CN0557
- article 8.3 interpretation requested by 62007CN0557
- A08P3 Interpreted by 62007CO0557
- article 2 Interpreted by 62008CA0005
- article 5.1 Interpreted by 62008CA0005
- article 5.5 interpreted by 62008CA0005
- article 5.2 .B Interpreted by 62008CA0467
- A02 Interpreted by 62008CJ0005
- A05P1 Interpreted by 62008CJ0005
- A02LA Interpreted by 62008CJ0403
- A03P1 Interpreted by 62008CJ0403
- A05P1 Interpreted by 62008CJ0403
- A05P2LB Interpreted by 62008CJ0467
- article 5.5 interpretation requested by 62008CN0005
- article 2 interpretation requested by 62008CN0005
- article 5.1 interpretation requested by 62008CN0005
- article 2 interpretation requested by 62008CN0403
- article 3 interpretation requested by 62008CN0403

Source: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32001L0029&qid=1625588767971>

22 July 2021 | Alluris Summer School 2021

15

15

Information Sources IP and IT | herfurth.partner

Explanation

A04P2 = Article 4 para. 2

Affected by case:

- A04P2 Interpreted by 62004CJ0479

Case C-479/04

Source: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32001L0029&qid=1625588767971>

22 July 2021 | Alluris Summer School 2021

16

16

Information Sources IP and IT | herfurth.partner

Explanation

A04P2 = Article 4 para. 2

Affected by case:

- A04P2 Interpreted by 62004CJ0479

Case C-479/04

- CC = Opinion of Advocate General
- CN = Reference for a preliminary ruling
- CJ = Judgement of the Court
- CO = Order of the Court
- CA = Published in the Official Journal of the EU

Source: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32001L0029&qid=1625588767971>

22 July 2021 | Alluris Summer School 2021

17

17

Information Sources IP and IT | herfurth.partner

		(1)
Amended	Judgment of the Court (Grand Chamber) of 12 September 2006. #Laserdisken ApS v	Addition article 12 paragraph (e)
Amended	Kulturministeriet. #Reference for a preliminary ruling: Østre Landsret - Denmark. #Directive 2001/29/EC - Harmonisation of certain aspects of copyright and related rights in the information society - Article 4 - Distribution rights - Rule of exhaustion - Legal basis - International agreements - Competition policy - Principle of proportionality - Freedom of expression - Principle of equal treatment - Articles 151 EC and 153 EC. #Case C-479/04.	Replacement article 5 paragraph
All codified		
- 06		
- 10		
- 22		
Subsidiary		
- Annotated		
Affected by		
- A04P2 Interpreted by 62004CJ0479		
- A03P1 Interpreted by 62005CJ0306		
- Interpreted by 62006CA0275		
- article 4.1 Interpreted by 62006CA0456		
- Interpreted by 62006CJ0275		
- A04P1 Interpreted by 62006CJ0456		
- article 5.1 PT A) interpretation requested by 62007CN0557		
- article 8.3 Interpretation requested by 62007CN0557		
- A08P3 Interpreted by 62007CO0557		

Source: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32001L0029&qid=1625588767971>

22 July 2021 | Alluris Summer School 2021

18

18

Information Sources IP and IT | herfurth.partner

Document 62008CN0005

Title and reference

Case C-5/08: Reference for a preliminary ruling from the Højesteret (Denmark) lodged on 4 January 2008 – Infopaq International A/S v Danske Dagblades Forening
OJ C 64, 8.3.2008, p. 28–29 (BG, ES, CS, DA, DE, ET, EL, EN, FR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)

Languages, formats and link to OJ

HTML, PDF, Official Journal

Multilingual display

English (en) | Please choose | Please choose | Display

Text

8.3.2008 | EN | Official Journal of the European Union | C 64/28

Reference for a preliminary ruling from the Højesteret (Denmark) lodged on 4 January 2008 — Infopaq International A/S v Danske Dagblades Forening
(Case C-5/08)
(2008/C 64/1)

Language of the case: Danish

Source: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62008CN0005>

22 July 2021 | Alluris Summer School 2021

19

19

Information Sources IP and IT | herfurth.partner

Document 62008CN0005

Title and reference

Case C-5/08: Reference for a preliminary ruling from the Højesteret (Denmark) lodged on 4 January 2008 – Infopaq International A/S v Danske Dagblades Forening
OJ C 64, 8.3.2008, p. 28–29 (BG, ES, CS, DA, DE, ET, EL, EN, FR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)

Source: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62008CN0005>

22 July 2021 | Alluris Summer School 2021

20

20

Information Sources IP and IT | herfurth.partner

Document 62008CJ0005

Title and reference

Judgment of the Court (Fourth Chamber) of 16 July 2009.
Infopaq International A/S v Danske Dagblades Forening.
Reference for a preliminary ruling: Højesteret - Denmark.
Copyright - Information society - Directive 2001/29/EC - Articles 2 and 5 - Literary and artistic works - Concept of 'reproduction' - Reproduction 'in part' - Reproduction of short extracts of literary works - Newspaper articles - Temporary and transient reproductions - Technological process consisting in scanning of articles followed by conversion into text file, electronic processing of the reproduction, storage of part of that reproduction and printing out.
Case C-5/08.
European Court Reports 2009 I-06569
ECLI identifier: ECLI:EU:C:2009:465

Source: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62008CJ0005>

22 July 2021 | Alluris Summer School 2021 21

21

Information Sources IP and IT | herfurth.partner

DLA Piper – Data Protection Laws of the World

22 July 2021 | Alluris Summer School 2021 22

22

Information Sources IP and IT | herfurth.partner

Source: <https://www.dlapiperdataprotection.com/>

22 July 2021 | Alliuris Summer School 2021

23

23

Information Sources IP and IT | herfurth.partner

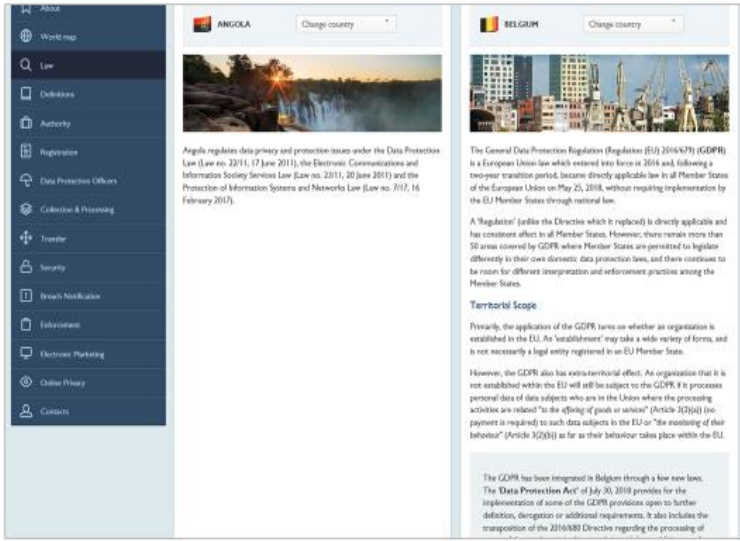
Source: <https://www.dlapiperdataprotection.com/>

22 July 2021 | Alliuris Summer School 2021

24

24

Information Sources IP and IT | herfurth.partner



Source: <https://www.dlappierdataprotection.com/index.html?c=AO&c2=BE&go-button=GO&t=law>

22 July 2021 | Alliuris Summer School 2021

25

25

Information Sources IP and IT | herfurth.partner

TLDRLegal

22 July 2021 | Alliuris Summer School 2021

26

26

Information Sources IP and IT | herfurth.partner

Source: <https://tldrlegal.com/>

22 July 2021 | Alliuris Summer School 2021

27

27

Information Sources IP and IT | herfurth.partner

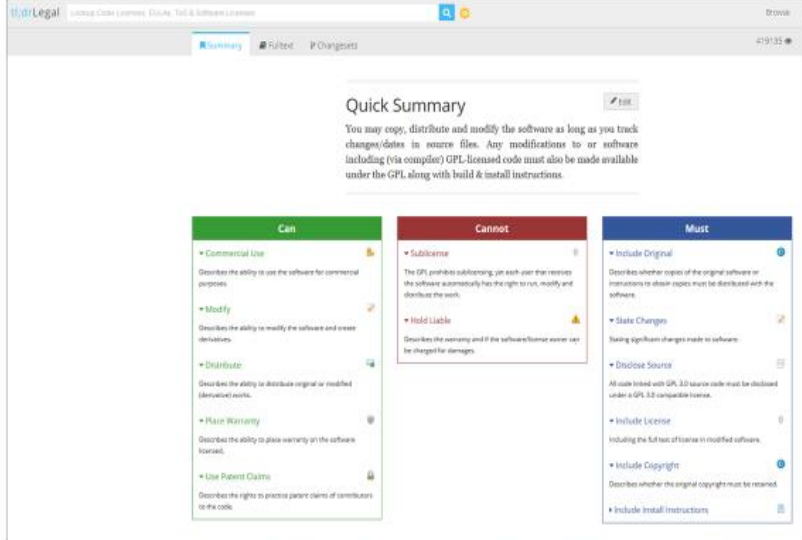
Source: [https://tldrlegal.com/license/gnu-general-public-license-v3-\(gpl-3\)](https://tldrlegal.com/license/gnu-general-public-license-v3-(gpl-3))

22 July 2021 | Alliuris Summer School 2021

28

28

Information Sources IP and IT | herfurth.partner



Quick Summary

You may copy, distribute and modify the software as long as you track changes/dates in source files. Any modifications to or software including (via compilation) GPL-licensed code must also be made available under the GPL, along with build & install instructions.

Can	Cannot	Must
<ul style="list-style-type: none">Commercial Use Describes the ability to use the software for commercial purposes.Modify Describes the ability to modify the software and create derivatives.Distribute Describes the ability to distribute original or modified (derivative) works.Place Warranty Describes the ability to place warranty on the software license.Use Patent Claims Describes the rights to prevent patent claims of contributors to the code.	<ul style="list-style-type: none">Sublicense The GPL prohibits sublicensing, an each user that receives the software automatically has the right to copy, modify and distribute the work.Hold Liable Describes the warranty and if the software/launcher vendor can be charged for damages.	<ul style="list-style-type: none">Include Original Describes whether copies of the original software or translations to other scripts must be distributed with the software.State Changes Stating significant changes made to software.Disclose Source All code linked with GPL 3.0 source code must be disclosed under a GPL 3.0 compatible license.Include License Including the full text of license in modified software.Include Copyright Describes whether the original copyright must be retained.Include Install Instructions

Source: [https://tldrlegal.com/license/gnu-general-public-license-v3-\(gpl-3\)](https://tldrlegal.com/license/gnu-general-public-license-v3-(gpl-3))

22 July 2021 | Alluris Summer School 2021

29

29

Information Sources IP and IT | herfurth.partner

Choose a Licence

22 July 2021 | Alluris Summer School 2021

30


30

Information Sources IP and IT | herfurth.partner

Choose an open source license


An open source license protects contributors and users, businesses and savvy developers won't touch a project without this protection

Which of the following best describes your situation?




I need to work in a community.

Use the license preferred by the community you're contributing to or depending on. Your project will fit right in.
If you have a dependency that doesn't have a license, ask its maintainers to add a license.



I want it simple and permissive.

The MIT License is short and to the point. It lets people do almost anything they want with your project, like making and distributing closed source versions.
Be careful: MIT, BSD, and Apache use the MIT License.



I care about sharing improvements.

The GNU GPLv3 also lets people do almost anything they want with your project, except distributing closed source versions.
Remember: Bash and GIMP use the GNU GPLv3.

What if none of these work for me?

My project isn't software.


There are licenses for that!

I want more choices.

More licenses are available.

I don't want to choose a license.

Here's what happens if you don't!

The content of this site is licensed under the Creative Commons Attribution 3.0 Unported License. About Terms of Service Help Improve This page
Created with  by GitHub, Inc. and You!

Source: <https://choosealicense.com/>

22 July 2021 | Alluris Summer School 2021 31

31

Information Sources IP and IT | herfurth.partner

Home

Licenses

Open source licenses grant permission for anyone to use, modify, and share licensed software for any purpose, subject to conditions preserving the provenance and openness of the software. The following licenses are sorted by the number of conditions, from most (GNU AGPLv3) to none (MIT license). Notice that the popular licenses featured on the [home page](#) (GNU GPLv3 and MIT) fall within this spectrum.

If you're looking for a reference table of every license on choosealicense.com, see the [appendix](#).

GNU AGPLv3

Permissions of this strongest copyleft license are conditioned on making available complete source code of licensed works and modifications, which include larger works using a licensed work, under the same license. Copyright and license notices must be preserved. Contributors provide an express grant of patent rights. When a modified version is used to provide a service over a network, the complete source code of the modified version must be made available.

Permissions	Conditions	Limitations
<input checked="" type="checkbox"/> Commercial use	<input checked="" type="checkbox"/> Disclosure source code	<input checked="" type="checkbox"/> Liability
<input checked="" type="checkbox"/> Distribution	<input checked="" type="checkbox"/> License and copyright notices	<input checked="" type="checkbox"/> Warranty
<input checked="" type="checkbox"/> Modification	<input checked="" type="checkbox"/> Attribution use in distribution	
<input checked="" type="checkbox"/> Patent use	<input checked="" type="checkbox"/> Same license	
<input checked="" type="checkbox"/> Private use	<input checked="" type="checkbox"/> State changes	

[View full GNU Affero General Public License v3.0 »](#)

GNU GPLv3

Permissions of the strong copyleft license are conditioned on making available complete source code of licensed works and modifications, which include larger works using a licensed work, under the same license. Copyright and license notices must be preserved. Contributors provide an express grant of patent rights.

Permissions	Conditions	Limitations
<input checked="" type="checkbox"/> Commercial use	<input checked="" type="checkbox"/> Disclosure source code	<input checked="" type="checkbox"/> Liability
<input checked="" type="checkbox"/> Distribution	<input checked="" type="checkbox"/> License and copyright notices	<input checked="" type="checkbox"/> Warranty
<input checked="" type="checkbox"/> Modification	<input checked="" type="checkbox"/> Same license	
<input checked="" type="checkbox"/> Patent use	<input checked="" type="checkbox"/> State changes	
<input checked="" type="checkbox"/> Private use		

[View full GNU General Public License v3.0 »](#)

GNU LGPLv3

Permissions of this copyleft license are conditioned on making available complete source code of licensed works and modifications under the same license of the GNU GPLv3. Copyright and license notices must be preserved. Contributors provide an express grant of patent rights. However, a larger work using the licensed work through interfaces

Permissions	Conditions	Limitations
<input checked="" type="checkbox"/> Commercial use	<input checked="" type="checkbox"/> Disclosure source code	<input checked="" type="checkbox"/> Liability
<input checked="" type="checkbox"/> Distribution	<input checked="" type="checkbox"/> License and copyright notices	<input checked="" type="checkbox"/> Warranty
<input checked="" type="checkbox"/> Modification	<input checked="" type="checkbox"/> Same license (library)	
<input checked="" type="checkbox"/> Patent use	<input checked="" type="checkbox"/> State changes	
<input checked="" type="checkbox"/> Private use		

[View full GNU Lesser General Public License v3.0 »](#)

Source: <https://choosealicense.com/licenses/>

22 July 2021 | Alluris Summer School 2021 32

32

Information Sources IP and IT | [herfurth.partner](#)

Online libraries

22 July 2021 | Alluris Summer School 2021 35

35

Information Sources IP and IT | [herfurth.partner](#)

- SSRN (Social Science Research Network)
<https://www.ssrn.com/index.cfm/en/>
- Slaw – Canada’s Online Legal Magazine
<http://www.slaw.ca/>
- British and Irish Legal Information Institute
<https://www.bailii.org/>
- Online commentary on German Act against Unfair Competition (in German)
<https://www.omsels.info/>



22 July 2021 | Alluris Summer School 2021 36

36

Information Sources IP and IT | [herfurth.partner](#)

IP offices and databases

22 July 2021 | Alliuris Summer School 2021 37

37

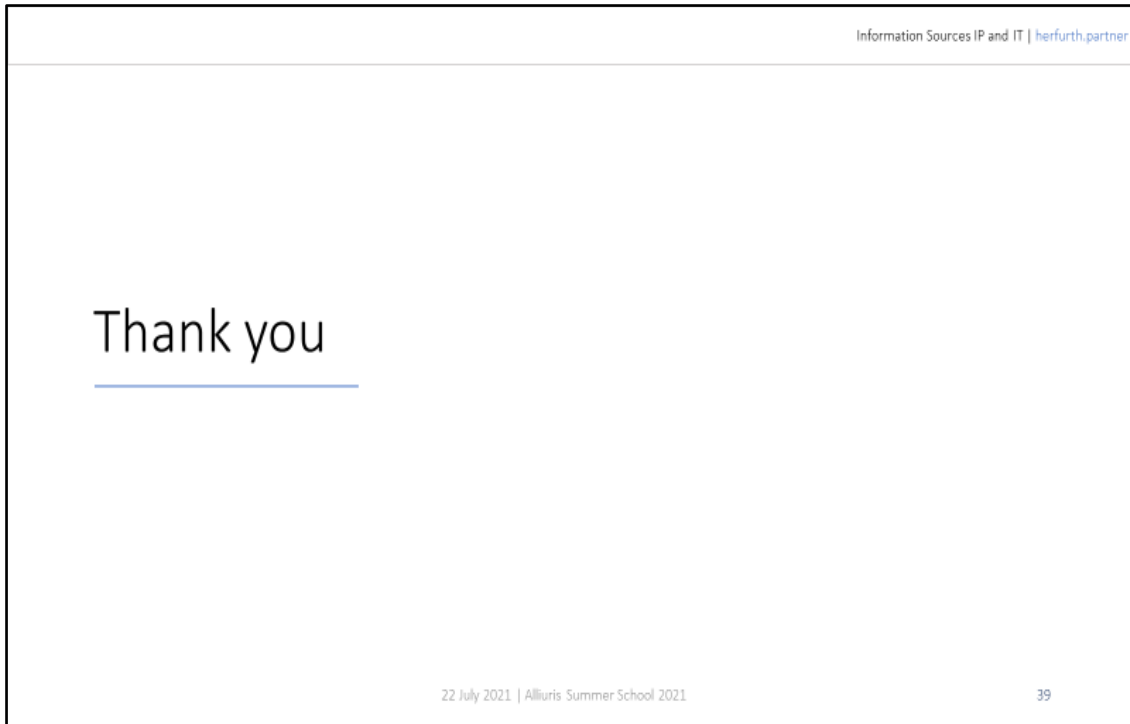
Information Sources IP and IT | [herfurth.partner](#)

- WIPO: <https://www.wipo.int/portal/en/index.html>
- WIPO Lex database: <https://wipolex.wipo.int/en/main/legislation>
- WIPO's database for patents, trade marks and designs: <https://ipportal.wipo.int/>
- EUIPO: <https://euipo.europa.eu/ohimportal/en>
- EUIPO's database eSearch plus: <https://euipo.europa.eu/eSearch/>
- TMview database: <https://www.tmdn.org/tmview/#/tmview>
- Chinese Trade Mark Office: <http://wcjs.sbj.cnipa.gov.cn/txnT01.do>



22 July 2021 | Alliuris Summer School 2021 38

38



39




Antonia Herfurth
Rechtsanwältin (D) ,

herfurth_antonia@herfurth.de

Chapter Eight

Trade Mark Protection in Europe



EU Trade Marks

Antonia Herfurth | Attorney at law in Hanover and Munich | Herfurth & Partner, Hanover




22 July 2021 | Alluris Summer School 2021

1




EU Trade Marks | [herfurth.partner](#)

Numbers and Facts




TOP 3 Member States with most registered EUTMs (all years):

 Germany 316,331	 Italy 159,222	 Spain 139,977
---	---	---




TOP 3 EUTM applications by country in 2020:

 China 15,799	 Germany 11,947	 USA 7,740
--	--	---

TOP 3 EUTM applications by country (all years):

 Germany 379,079	 USA 338,426	 UK 213,612
---	---	--

TOP 3 countries with most registered EUTMs (all years):

 Germany 316,331	 USA 280,393	 UK 177,220
---	---	---

TOP 3 classes of goods and services:


- 9 - Electronic apparatus and instruments; computer hardware; software, optical apparatus and instruments
- 35 - Advertising; business management, organisation and administration; office functions
- 42 - Scientific and technological services

22 July 2021 | Alluris Summer School 2021

2

EU Trade Marks | herfurth.partner

Most famous trade marks from EU Member States



Source: <https://www.pinterest.de/pin/what-the-most-famous-brands-are-from-each-state-531002612285368228/>

22 July 2021 | Alluris Summer School 2021

3

3

EU Trade Marks | herfurth.partner

Basics

22 July 2021 | Alluris Summer School 2021

4

4

EU Trade Marks | herfurth.partner


- a trade mark
 - identifies the **origin** of goods and services
 - guarantees consistent **quality** by showing an organisation's commitment to its users and consumers
 - is a form of **communication**, a basis for publicity and advertising
 - can be one of the most important **assets** of a company
- Article 4 EUTMR:
An EU trade mark may consist of **any signs**, in particular words, including personal names, or designs, letters, numerals, colours, the shape of goods or of the packaging of goods, or sounds, provided that such signs are capable of:
 - (a) **distinguishing** the goods or services of one undertaking from those of other undertakings; and
 - (b) being **represented** on the Register of European Union trade marks ("the Register"), in a manner which enables the competent authorities and the public to determine the clear and precise subject matter of the protection afforded to its proprietor.

22 July 2021 | Alliuris Summer School 2021


5

5


EU Trade Marks | herfurth.partner




sound mark



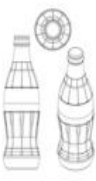
word mark




combined word and figurative mark




colour mark




shape mark



pattern mark



figurative mark



position mark

Source video: <https://www.youtube.com/watch?v=ANQQv-dGQJA>

22 July 2021 | Alliuris Summer School 2021

6

6

EU Trade Marks | [herfurth.partner](#)



Trade Mark Registration

22 July 2021 | Alliuris Summer School 2021 7

7

EU Trade Marks | [herfurth.partner](#)

Examination scheme (1/5)

- I. Absolute grounds of refusal, Article 7 EUTMR
 1. Fulfilling the definition of a trade mark, Articles 7 (1) (a), 4 EUTMR
 - 1.1. Is it a sign?
= words, letters, numbers, images, shapes, colours, position, pattern, holograms, multimedia signs, sounds, but also other signs, Article 4 EUTMR
 - 1.2. Is the sign capable of distinguishing the goods or services of one undertaking from those of other undertakings, Article 4 (a) EUTMR?
→ abstract ability to serve as a badge of origin
 - 1.3. Permanent representation on the Register, Article 4 (b) EUTMR
 →  , but in EU difficult with taste, smell and tactile
Source video: <https://www.youtube.com/watch?v=ANQQv-dGDJA>

8

Examination scheme (2/5)

2. Distinctiveness, Article 7 (1) (b) EUTMR

= sign serves to identify the goods and/or services as **originating from particular undertaking**, and thus to **distinguish** that product from those of other undertakings

distinctive:

- suggestive: consumer must use imagination to create connection to the sign's product or service, e.g. "Puma" suggests speed but the word is not connected to sportswear
- fanciful: creation of a new word such as "Kodak"
- arbitrary: if word already exists but is used by undertaking in a way that is not connected to ordinary meaning, such as "Apple" for computers

lack of distinctiveness:

- descriptive terms providing information about kind, quality, quantity, purpose of goods/services
- common colours or shapes (**but** colour combinations or colours unusual for good/service might be distinctive, e.g. purple for chocolate)
- common appeals (to buy) ("Buy it", "GetItRight", "Test it")
- descriptions for use

22 July 2021 | Alliuris Summer School 2021

9

9

Examination scheme (3/5)

3. No descriptiveness, Article 7 (1) (c) EUTMR

= sign must **not** have a **meaning** which is **immediately perceived** by relevant public as providing information about respective goods or services

descriptive:

- kind of goods/services ("Pearl" for wines and sparkling wines, "Apple" for fruit)
- quality ("light", "fresh", "extra")
- quantity (24 carat for jewellery, "six pack" for beer)
- intended purpose ("Trustedlink" for goods and services in IT)
- time of production or of rendering of the service ("evening news", "24 hours")
- language issues (e.g. pseudo-anglicisms)
- geographical names
- contrary to public policy or acceptable principles of morality

22 July 2021 | Alliuris Summer School 2021

10

10

EU Trade Marks | [herfurth.partner](#)

Examination scheme (4/5)

4. Customary signs or indication, Article 7 (1) (d) EUTMR
5. Exclusion of functional signs, Article 7 (1) (e) EUTMR
6. Deceptive trade marks, Article 7 (1) (g) EUTMR
7. Other grounds according to Article 7 (1) (f)-(m) EUTMR
8. Distinctiveness/descriptiveness through use, Article 7 (3) EUTMR?
→ only applicable to grounds of Article 7 (1) (b)-(d) EUTMR

II. Relative grounds of refusal, Article 8 EUTMR

= prior rights, e.g. older trade mark application or registration
→ not examined ex officio by EUIPO, only where raised by rightholder of prior right

22 July 2021 | Alluris Summer School 2021

11

11

EU Trade Marks | [herfurth.partner](#)

Examination scheme (5/5): Additional points to check

III. Classification for goods and services

- **Nice Classification**: internationally agreed list of certain goods and services, comprises of 45 classes (34 classes of goods, 11 classes of services) and about 10,000 terms in total
- **Harmonised Database**: additional classification database, jointly developed by EUIPO and national trade mark offices in EU → provides 73,000 harmonised terms accepted in EU → Harmonised Database (HDB) is provided through the common platform "TMclass"

IV. Payment of fees

- must be paid within 1 month
- application fee (for one class) → 1,000.00 €
- application fee for electronic filing (for one class) → 850.00 €
- class fee for second class → 50.00 €
- class fee for third and each additional class per class → 150.00 €

22 July 2021 | Alluris Summer School 2021

12

12

EU Trade Marks | herfurth.partner

Duration of application procedure

- regularly completed by the *European Union Intellectual Property Office* (EUIPO) in about **5 to 6 months**
- in some special cases, fast track proceedings possible → immediate payment of fees → registration will be completed faster, about 4 months

Registration

- if all application requirements are fulfilled, trade mark is entered in Register and registration is published in all 23 official languages, Article 51 (1) EUTMR

22 July 2021 | Alluris Summer School 2021


13

13

EU Trade Marks | herfurth.partner

Scope of protection

- EU trade mark covers **entire territory of EU** (dark blue countries in picture), the geographical scope can not be limited to certain Member States
- therefore, EU trade mark only registrable when sign is capable of being trade mark in **all** Member States, so if ground of refusal exists in one Member State, EU trade mark not registrable
- in general, EU trade mark and national trade mark, e.g. Dutch trade mark, can stand next to each other, Recital 8 EUTMR
- duration of protection of a registered trade mark is **10 years** from date of application, however, can be **renewed indefinitely** for 10 years in each case, Article 52 EUTMR



Source:
https://de.wikipedia.org/wiki/Europ%C3%A4ische_Union#/media/Datei:EU-candidate_countries_map.svg

22 July 2021 | Alluris Summer School 2021





14

14

EU Trade Marks | herfurth.partner

Form for trade mark application

- EasyFiling Form, Five Step Form and Advanced Form available on website of EUIPO
- accessible under:
<https://euipo.europa.eu/ohimportal/en/apply-now>

EasyFiling Form 	Five Step Form	Advanced Form
Designed for SMEs and individuals within the European Economic Area, without a legal representative	Tailored for intellectual property experts when handling straightforward cases	Tailored for intellectual property experts when handling complex cases
Choose your language: English (en)	Choose your language: English (en)	Choose your language: English (en)
Apply Now	Apply Now	Apply Now
Word or figurative trade marks only	Word, figurative, shape or sound marks	All types of marks
Pre-defined goods & services	Pre-defined goods & services	Lets the user upload their own list of goods & services (including from the Goods & Services Builder) Class 35 and 37 assistant
Immediate credit card payment	Immediate credit card payment, bank transfer or current account payment	Immediate or deferred (one month) credit card payment, bank transfer or current account payment
		 Optimized
<ul style="list-style-type: none"> Guided Form (virtual assistant) Mobile devices friendly Allows one applicant only 	<ul style="list-style-type: none"> Lets the user save drafts in the User Area Lets the user add an additional applicant Lets the user appoint a representative 	<ul style="list-style-type: none"> Lets the user save drafts in the User Area Lets the user add an additional applicant Lets the user appoint a representative

22 July 2021 | Alliuris Summer School 2021

15

15

EU Trade Marks | herfurth.partner

Attacking the Trade Mark

22 July 2021 | Alliuris Summer School 2021

16

16

EU Trade Marks | [herfurth.partner](#)

At the EUIPO

22 July 2021 | Alliuris Summer School 2021 17

17

EU Trade Marks | [herfurth.partner](#)

Opposition, Article 46 EUTMR

- on the relative ground that opponent's trade mark has **earlier priority**
- opponent is owner of older trade mark
- filed within 3 months from the date of publication of the application
- opposition fee of 320.00 € to be paid within opposition period of 3 months

Revocation and cancellation, Article 58 EUTMR

- on the ground that attacked trade mark has **not been used** within the last 5 years or the trade mark has become **common name** for goods and services or trade mark **misleads** public, especially as to nature, quality or geographical origin
- by any third party
- filed anytime but not earlier than after the date of publication of the registration, in case of non-use not early than 5 years after the date of publication of the registration
- payment of application fee of 630.00 €

22 July 2021 | Alliuris Summer School 2021 18

18

EU Trade Marks | herfurth.partner

Cancellation due to invalidity based on absolute grounds, Article 59 EUTMR

- based on absolute grounds laid down in Article 7 EUTMR: i.e. **lack of protectability** (e.g. trade mark has no distinctive character, trade mark is descriptive) or **bad faith** of the proprietor when filing the trade mark application
- by any third party
- filed anytime but not earlier than the date of publication of the registration
- payment of application fee of 630.00 €

Cancellation due to invalidity based on relative grounds, Article 60 EUTMR

- on the relative ground that applicant's trade mark has **earlier priority** or applicant is holder of other earlier right such as name, copyright, industrial property right
- applicant is owner of older trade mark or other earlier right
- filed anytime but not earlier than the date of publication of the registration
- payment of application fee of 630.00 €

22 July 2021 | Alliuris Summer School 2021

19

19

Trade Marks in Germany | Transnational IP Contracts

The diagram shows a horizontal timeline starting with 'Trade mark application' and ending with 'Registration of trade mark'. A bracket below the timeline indicates the 'Opposition period EU (3 months)' with the condition '- opponent's trade mark has earlier priority'. A larger bracket below the timeline indicates 'Revocation and cancellation' with three sub-points: '- trade mark has become common name or misleads public', 'Cancellation due to invalidity based on absolute grounds' (with sub-point '- absolute grounds, e.g. trade mark has no distinctive character or is descriptive'), and 'Cancellation due to invalidity based on relative grounds' (with sub-point '- applicant's trade mark has earlier priority'). A final bracket at the end of the timeline indicates 'Revocation and cancellation' with the condition '- trade mark not used within last 5 years'.

24 and 25 June 2021 | University of Göttingen | UPIT LL.M. 2020/2021

20

20

EU Trade Marks | [herfurth.partner](#)

At the Courts

22 July 2021 | Alliuris Summer School 2021 21

21

EU Trade Marks | [herfurth.partner](#)

Actions before civil courts

- first, consideration of **milder measures** such as request for authorisation, warning letter, cease and desist declaration
- if there is urgency, a **preliminary injunction** offers provisional legal protection
- for preliminary injunction, ground of infringement and ground for urgency must be presented to court
- filed with the national civil courts
- with the **main action**, all remedies based on infringement of intellectual property right can be followed
- common claims at civil courts are:
 - **right to an injunction**, see Article 11 Enforcement Directive (2004/48/EC)
 - **rendering of information and account**, see Article 8 Enforcement Directive
 - **surrender, destruction and recall rights**, see Article 10 Enforcement Directive
 - **damages**, see Article 13 Enforcement Directive
- filed with the national civil courts → respective national court is competent to order measures in all Member States

22 July 2021 | Alliuris Summer School 2021 22

22

EU Trade Marks | herfurth.partner

Actions before criminal courts

- measures under criminal law apply when counterfeiting and piracy activities are involved
- criminal actions must be brought at **national level** using the relevant national criminal law, see also Article 137 (2) EUTMR
- but, enforcement rules for intellectual property are **not harmonised** in EU, as a result, the options available vary considerably and it is not always possible to apply criminal law enforcement measures in the same way in every Member State
- if criminal law rules exist, national enforcement and prosecution authorities in the relevant EU jurisdiction must be contacted
- example: in Germany, wilful infringement of EU trade mark is punishable, Section 143a German Trade Mark Act, request to prosecute infringement must be submitted to police or public prosecutor's office

22 July 2021 | Alluris Summer School 2021 23

23

EU Trade Marks | herfurth.partner

	Proceedings before German DPMA	Ordinary court proceedings in Germany
Duration	in practice, often 9-12 months	depends, but often not longer than DPMA proceedings
Costs	cheaper (DPMA fees + lawyer's fees etc. → total of about 2,000.00 € - 3,000.00 €)	more expensive (costs based on amount in dispute, often around 50,000.00 €; court fees + lawyer's fees etc. → total of about 8,000.00 € - 10,000.00 €)
Appeal	appeal possible (1st appeal: <i>Erinnerung</i> to DPMA or <i>Beschwerde</i> to Federal Patent Court → 2nd appeal: (in case of <i>Erinnerung</i>) <i>Beschwerde</i> to FPC or (in case of <i>Beschwerde</i>) <i>Rechtsbeschwerde</i> to German Federal Court of Justice)	appeal possible (1st appeal: <i>Berufung</i> to Higher Regional Court → 2nd appeal: <i>Revision</i> to German Federal Court of Justice)
Other		if necessary, puts more pressure on other party

22 July 2021 | Alluris Summer School 2021 24

24

EU Trade Marks | [herfurth.partner](#)

Involvement of an EU Lawyer?

22 July 2021 | Alliuris Summer School 2021 25

25

EU Trade Marks | [herfurth.partner](#)

- generally, persons having their domicile or their principal place of business or a real and effective industrial or commercial establishment within the European Economic Area (EEA), which consists of the EU, Iceland, Liechtenstein and Norway, are **not required to be represented** in any proceedings before the EUIPO
- however, natural persons **not** domiciled in or legal persons that do **not** have their principal place of business or a real and effective industrial or commercial establishment in the EEA **must** be represented by a representative based within the EEA
- this obligation exists in all proceedings before the EUIPO, except for the act of filing an application for an EU trade mark

22 July 2021 | Alliuris Summer School 2021 26

26

EU Trade Marks | [herfurth.partner](#)

Useful Links

22 July 2021 | Alliuris Summer School 2021 27

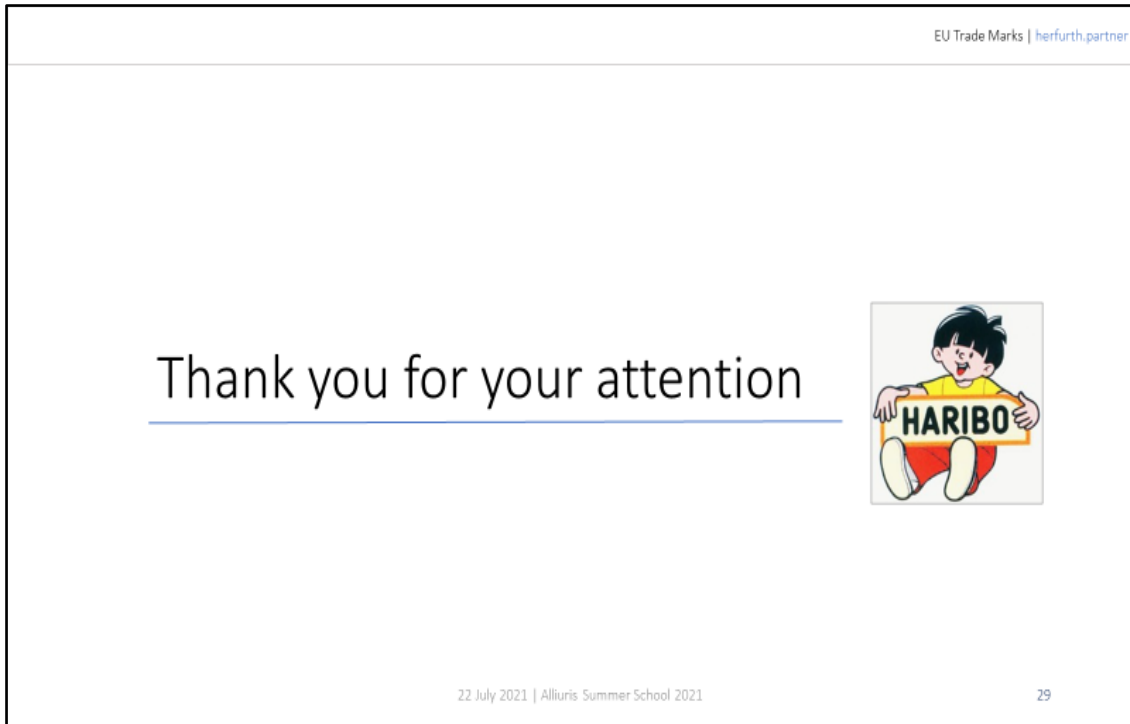
27

EU Trade Marks | [herfurth.partner](#)

- Regulation on the European Union trade mark (EUTMR) (available in 24 languages): <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R1001>
- Official website of the EUIPO: <https://euipo.europa.eu/ohimportal/en/home>
- Trade mark basics: <https://euipo.europa.eu/ohimportal/en/trade-marks-basics>
- EUIPO Trade Mark Guidelines: <https://guidelines.euipo.europa.eu/binary/1922895/2000000000>
- EUIPO online forms: <https://euipo.europa.eu/ohimportal/en/online-services>
- Checklist for trade mark registration: <https://euipo.europa.eu/ohimportal/en/checklist>
- FAQs about trade marks: <https://euipo.europa.eu/ohimportal/en/help>

22 July 2021 | Alliuris Summer School 2021 28

28



29



Antonia Herfurth
Rechtsanwältin (D) ,

herfurth_antonia@herfurth.de

Questions and Answers

Intellectual Property

What kind of infringements of IP rights are most common and/or significant in your country?

Cheril (China):

Copyright infringement cases are most common, among which image copyright infringement accounts for more than half of it. The subjects of direct infringement include not only agencies, enterprises and institutions, but also individual industrial and commercial households and individuals. We media users' infringements on platforms such as Weibo, WeChat, blog, and Tieba are also very common. The industry of the user of the picture is not limited to the Internet industry, including all industry entities that need to use the Internet for business or development. The main reason for the infringement is the unclear rights subject, unclear rights status, and unblocked authorization channels and insufficient copyright protection awareness of the users of the images in the image market.

Wenzhu Lan (China):

Trademark infringement

Ana Marija Đurić (Croatia):

Regarding the statistics, most common infringements of IP are violation of copyright regulations, violation of trademark and other markings, violation of regulations on patents and technical improvements.

L. Tuncer (Netherlands):

Copyright law, portrait right, trademark law.

Zoë Jardim (Brazil):

The most common cybercrimes in Brazil are: slander, insults, defamation, revealing the secrets of others, disclosure of intimate material such as photos and documents, obscene acts, apology for crime, prejudice/racism and pedophilia.

What are the biggest challenges with regard to data protection in your country?

Cheril (China):

The biggest challenge of data protection is to balance the interests of personal data rights protection and enterprise technological innovation. The interests of the data field are not single, but diversified. From the perspective of the interrelationship of data interests, diversified data interests are actually the interests of "overlapping coexisting forms", which are different from the mutual separation of interests of "parallel coexisting forms". Data interests are plural protection interests that are "overlapped and combined" by interests of different subjects, fields, and attributes. This plural protection interest is manifested as a competition of infringement of data public interest and infringement of data private interest. Acts that infringe on the interests of users may also coincide with acts that infringe on the interests of operators. Acts that infringe on emerging interests coincide with acts that infringe on traditional interests. Therefore, the interest content involved in data legislation is very complicated, and the one-dimensional "right-relief" legislative path is far from meeting the needs of diversified interest adjustment. What's more, to realize the protection of data, it is necessary to clarify the ownership, nature, content and boundaries of data rights, but there is a conflict between data privacy and the inherent nature of data. Data privacy emphasizes exclusivity, however, this is exactly the opposite of the logic of data generation and development. The value of data comes from its relevance, sharing, and openness. "The more relevant big data is, the more valuable it is, and the more open it is, the more valuable it is". It is on the basis of data sharing that the restriction of regional, narrow, and closed operation mode to human development can be solved to the greatest extent, so that the economy and society can achieve exponential and leap-forward development, and a cooperative, shared, and prosperous the future of society can be expected.

Wenzhu Lan (China):

The of consciousness for information property protection

Ana Marija Đurić (Croatia):

I would say that human error is the greatest threat to data privacy and security. Employees that are ill-informed or clueless can use weak passwords, destroy data by accident, fall for phishing schemes, have privileged account access, and surf websites that are not permitted. Generally I would say that despite the fact that data has increased at an exponential rate over the last decade, poor security procedures continue to put businesses at danger of a data breach. The most serious threats in data privacy is Personal Identifiable Information where handling millions of data records becomes overwhelming in our technology-driven society due to the veracity and volume of data.

Tuncer (Netherlands):

Keeping up with technological developments and offer a secure data storage.

Zoë Jardim (Brazil):

Complexity of configuration and operation of protection systems, lack of data protection solutions for new technologies, and ensuring regulatory compliance.

Materials | Compact

The European Copyright Reform

Antonia Herfurth, attorney at law in Munich and Hanover

Hanover, April 2019

The copyright law in force in the EU is harmonized by various directives - but it dates back to 2001: at that time there was no Facebook, YouTube or Twitter. As a result, it no longer adequately serves its purpose "in this new digital environment." This was the view of the European Commission following an evaluation of copyright between the years 2013 and 2016, and as a result it initiated the reform.

On March 26, 2019, the European Parliament has now approved the copyright reform presented to it. The controversially discussed draft was adopted by a clear majority. If the Council of the European Union also confirms the draft, the legislative process would be completed, and the member states would have to implement the Copyright Directive within two years.

The aim is to adapt copyright law at EU level to the "new realities", as the development of digital technologies has led to changes in the creation, production, dissemination and exploitation of works and other protected subject matter. There are new forms of exploitation as well as new actors and business models. It also aims to better protect creators and rights holders by ensuring they receive fair remuneration for their content on the Internet. The EU also wants to promote the digital single market and prevent copyright fragmentation in the member states. Even though exceptions and limitations to copyrights are harmonized at the EU level, the emergence of new types of use in recent years means that it is not certain whether these exceptions will continue to be suitable for ensuring a fair balance between the rights and interests of authors on the one hand and those of users on the other. Moreover, these exceptions are only effective at the national level. Legal certainty for cross-border uses is not guaranteed.

The new EU directive

The current draft directive addresses measures in several new areas:

- Adaption of exceptions and limitations to the digital and cross-border environment;
- Improvement of licensing practices and ensuring wider access to content;
- Creation of a viable market for copyright protection.

There are four articles in the draft directive that stand out:

Text and data mining (Article 3)

From a network policy perspective, Article 3 is particularly interesting; it provides for a new, EU-wide mandatory barrier regulation in favor of text and data mining.

In the future, it will allow the automatic evaluation or analysis of already existing data for the purpose of non-commercial scientific research seeking to gain new knowledge (text and data mining).

In addition, Article 3 indirectly affects the framework conditions for the development and application of analysis methods - in the use of artificial intelligence, the question is who may access public data under which circumstances in order to develop, test or apply self-learning algorithms. However, since Article 3 only favors non-commercial scientific institutions, while the further development of artificial intelligence is largely driven by commercial data scientists and start-ups, the EU has created an opening clause in Article 4. This allows member states to provide further exceptions for their domestic industry, science, or the interested public.

Protection of press publications concerning online uses (Art. 15)

Article 15 is aimed at all services and Internet platforms that earn their money from third-party content, such as Google, YouTube, Facebook or even Instagram. The EU's intention is to no longer place publishers in the online sector in a worse position than other intermediaries of works, e.g. producers of sound recordings. After all, publishing services also cost time and money. In addition, the ancillary copyright is intended to secure the future of the press by creating a new source of income for European publishers.

Following the German and Spanish example, the EU therefore wants to introduce an ancillary copyright for press publishers. This grants press publishers the exclusive right to make the press product or parts thereof available to the public for commercial purposes, except in the case of individual words or very small text excerpts. The rule serves to protect against systematic access to the publishing service by the providers of search engines (whose business models rely heavily on the access to the publisher's work) and providers preparing content in accordance with a search engine.

Private or non-commercial uses of press publications by individual users are not covered by the provision.

Compensation claims by publishers (Article 16)

The EU wants publishers to participate again in statutory compensation claims.

To this end, Member States may now stipulate under Article 16 that where an author has transferred or licensed a right to a publisher, such transfer or licensing shall constitute a sufficient legal basis for the publisher's claim to a share of the compensation for the use of the work.

Licensing obligation and upload filters (Article 17)

Under current EU copyright law, Internet platforms are not liable for copyright-infringing content; instead, users are responsible for the images, videos, texts, or music they upload. With the copyright reform, platforms will now be responsible if content is uploaded for which they, the platforms, do not hold licenses.

To comply with Article 17, platforms must scan all content using software that uses an extensive database to check whether another person holds the copyright to the content; if so, the filter will prevent uploading (upload filter). Therefore, platform operators should acquire licenses for the content that is uploaded by users and thus also give the authors a share of the revenues.

A platform can escape liability if it has made timely efforts to obtain licenses from rights holders. In addition, platforms would be exempt from upload filters if they have been in existence for less than three years, have annual revenues of less than ten million euros, and have fewer than five million users per month.

Criticisms

While supporters see the current draft as strengthening the position of rights holders against platforms such as Google, YouTube or Facebook, critics warn of the consequences of the reform: The internet of the consumer would become much smaller. Critics fear a restriction of freedom of expression, art, and the press.

Text and data mining

As the Commission's initially restrictive proposal on text and data mining was extended to include a national opening clause, it earned approval. Soon, however, concerns arose about the timeframe commercial data scientists, start-ups and the like would have to wait in order for national governments to enact their own regulations, allowing them to develop and apply artificial intelligence, especially since the clause merely offered an exception to the rule. It was up to the member states to decide whether to accept it.

Ancillary copyright for press publishers

The motivations behind a stronger protection of press publishers as described above are entirely justified.

However, opponents of the ancillary copyright argue that the models taken as examples have already failed. The Spanish law is now known to have had a negative impact on the visibility of news and access to information in Spain and has been particularly damaging to smaller and independent media. The German ancillary copyright has only led to publishers in Germany making their content available again free of charge after a short time. Moreover, it is about to be declared null and void in court. The ancillary copyright has not generated any additional revenue for publishers.

It is also feared that, contrary to the original intention of covering only commercial users, also bloggers, small businesses or, for example, private users who collect, share and comment on other people's content on the web could be indirectly affected by Article 15.

In addition, the ancillary copyright would make the use of search engines and platforms more burdensome in everyday life. In the future, they would no longer be allowed to display titles or entire sentences if they had not acquired licenses from the rights holders. Under the EU reform, only individual words or short text excerpts may be displayed. Links are also allowed, but not link previews, which usually show the title and teaser of an article. The user would therefore hardly have a chance to find out what exactly the shared article is about before clicking.

Compensation claims for publishers

The introduction of compensation claims for publishers was declared illegal by the European Court of Justice back in 2015. The Court argued that this compensation, which at the time was up to 50% depending on the country and type of work, was intended to benefit authors alone.

Licensing obligation and upload filters

Opponents of the reform see the introduction of upload filters as a threat to the Internet culture. The fundamental problem is that upload filters, as automated computer programs, cannot recognize irony, satire or even sarcasm. In order to do so, they would need to put the contents in context.

Critics are also concerned that platforms will be cautious to delete too much content - including legal content – rather than too little (overblocking), given the risk of potential liability. Although the affected user could act against this by means of a complaint or lawsuit, many of them would be deterred from taking such steps.

Furthermore, there are concerns about the automated censorship of critical voices. The proponents, on the other hand, argue that the controls would be appropriate and transparent. Moreover, in most cases the platforms would acquire licenses for the copyrighted material anyway, so there would be no need for blocking. Yet it is argued that it is not clear how platforms should have sought licenses in good time if they only know at the moment of upload what kind of content is being uploaded.

The European Court of Justice has already ruled against upload filters at the beginning of 2012. They would violate the prohibition of a general monitoring obligation and undermine entrepreneurial freedom, as such a monitoring requires expensive and complicated IT systems. As a result, many fear a further growth of the market positions of already large platforms such as Google, Facebook or Amazon at the expense of smaller ones. This, in turn, could weaken the negotiating position of rights holders, as content could only be uploaded under the conditions dictated by these platforms or not at all.

Alternative proposals

The draft directive was adopted unchanged on March 26, 2019, despite the existence of alternative proposals.

More generous text and data mining

Although the introduction of the opening clause was praised by many experts, it was not considered sufficient. To avoid further difficulties the - already few - specialists and innovators in the IT sector, it was suggested that the opening clause should not be left at the national level but should be raised to the EU level.

To prevent a feared shift of commercial research to jurisdictions whose copyright laws are more generous than those of the EU, such as the U.S. or Asia, experts suggested exempting commercial mining and compensating rights holders in return.

Capturing only affected platforms

From the ranks of the European Parliament was suggested that the definition of "online content-sharing service providers" formulated in the Copyright Directive should be more narrowly defined. In this way, only those platforms that are affected by a particularly high number of copyright infringements could be required to introduce an upload filter. This would significantly reduce the conflict.

Introduction of flat-rate license fees

According to a proposal by the CDU for national implementation of the directive, the principle in Germany should be: "Pay instead of block." Accordingly, all content should be uploadable in principle without upload filters or risk of censorship. In a second step, platform operators would have to compensate authors for the use of their works. This would not apply if the use has already been allowed through the purchase of a license. In addition, uploads that are below a certain time limit should be free of license fees.

Outlook

Following the parliamentary approval of the copyright reform, the draft must be approved again by the member states. They had already done so - with a German yes - in February. The possible date for the new vote is April 9, 2019. The reform's opponents hope that the German government will refuse to give its approval this time. Especially since a German "no" vote would make the necessary majority among the member states uncertain. However, a German "no" is considered unlikely.

+ + +

Current Developments

Sara Nesler, Mag. iur (Torino), LL.M. (Münster)

Hanover, August 2021

Even if the deadline for the transposition of the directive passed on June 7, 2021, it remains problematic.

On the one hand, the Commission has initiated infringement proceedings against 23 member states. They are said to have not yet implemented the directive or to have done so inadequately. This does not include Germany, as the directive was transposed into national law on June 4.

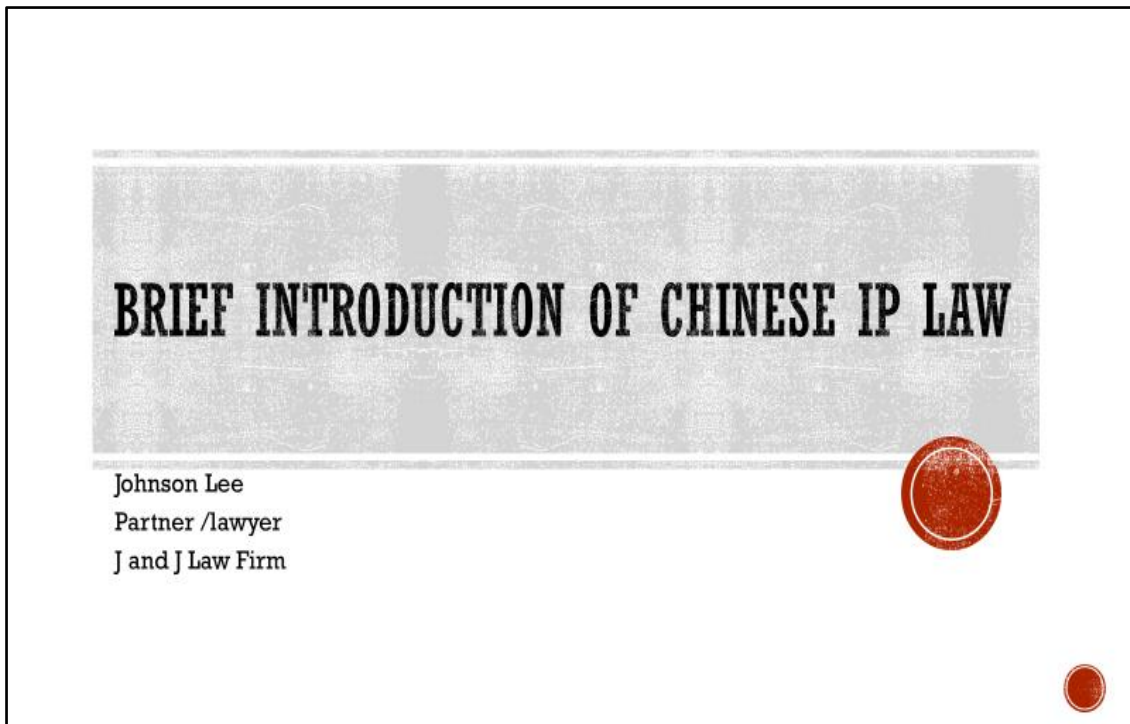
Secondly, the European Court of Justice is currently examining whether the directive violates the Charter of Fundamental Rights following a complaint by Poland. The Advocate General's Office has recommended that the case be dismissed. However, Article 17 must be interpreted in accordance with fundamental rights. Only clearly illegal content should be blocked automatically. Accordingly, service providers could not be required to carry out fully comprehensive preventive filtering.

The current situation is thus characterized by a high degree of legal and planning uncertainty, which puts companies and citizens in a state of limbo and endangers the internal market.

+ + +

Chapter Nine

Legal Basis of Intellectual Property Protection in China



1



2

OUTLINE

- Overview
- Patent Law
- Copyright Law
- Trademark Law
- Anti-unfair Competition Law



3

OVERVIEW

- While formulating domestic laws and regulations on IP, China has strengthened exchanges and cooperation with other countries in the field of intellectual property, and has acceded to more than ten international conventions on intellectual property protection.
- They mainly include: Trips Agreement, Paris Convention for the Protection of Industrial Property Rights, Berne Convention for the Protection of Literary and Artistic Works, World Copyright Convention, Madrid Agreement on International Trademark Registration, Patent Cooperation Treaty, etc.
- Among them, Trips Agreement in the WTO is considered to be an international convention in the field of IP protection, which involves a wide range of areas, has a high level of protection, has a strong degree of protection, and has a strong restrictive force. It plays an important role in the amendment of China's IP law.



4

OVERVIEW

- **Sorts of Law:** Patent Law , Copyright Law , Trademark Law, Anti-unfair Competition Law
- **Three protective methods:** Civil, Administrative, Criminal
- **Administrative authority's power:** inquire, investigate, carry out on-site inspection, consult and copy, seal up or seize, fine.



5

OVERVIEW

- **The damages :** For the infringement of IP rights, the obligee has the right to stop the infringement, eliminate the influence and compensate for the loss or claim the damages
- Determined according to the actual loss suffered by the right holder due to the infringement or the benefits obtained by the infringer from the infringement;
- or if it is difficult to determine the loss suffered by the right holder or the benefits obtained by the infringer, the damages shall be reasonably determined by reference to the multiple of the royalty.
- In the case of an intentional infringement with serious circumstances, the damages may be determined as not less than one nor more than five times the amount determined in the aforesaid method.
- Where it is difficult to determine the loss suffered by the right holder, the benefits obtained by the infringer, and the royalty, the people's court may, by taking into account factors such as the type of the IP right and the nature and circumstances of the infringement, determine the damages as not more than five million yuan.



6

PATENT

• The “Patent” means inventions, utility models and designs.

The term “**Invention**” refers to any new technical solution relating to a product, a process or an improvement thereof.

The term “**Design**” means a new design of the shape, pattern, or a combination thereof, as well as a combination of the color, shape and pattern, of the entirety or a portion of a product.

The term “**Utility model**” refers to any new technical solution relating to a product's shape, structure, or a combination thereof.

7

(19) 中华人民共和国国家知识产权局

(21) 发明专利申请

(22) 申请号 201810176909.9

(23) 申请日 2018.04.18

(71) 申请人 中投(惠州)新能源有限公司
地址 516069 广东省惠州市惠城区江北大道228号2号楼

(72) 发明人 王佩华 张炳松 薛上川 王润波 罗旭忠 肖光宇 赵俊杰 罗浩

(74) 专利代理机构 广州粤高专利商标代理有限公司
代理人 孔松迪 黄新如

(51) Int. Cl. H05D 27/02(2006.01)

(54) 发明名称 一种电力设备户外箱体环境实时监控装置及方法

(57) 摘要 本发明公开了一种电力设备户外箱体环境实时监控装置,在户外箱体内部安装温度传感器、湿度传感器、加热器和加热器控制电路,实时采集箱体内部温度、湿度数据并实时传输至外部服务器,服务器根据接收到的实时温度、湿度数据以及安装在户外箱体外部用于采集加热次数超过阈值以及低于阈值时进行报警的报警指示灯(7)的输入端连接到温度控制器(3)与加热器(4)之间的连接线上,所述报警指示灯(7)的输入端与报警装置(6)的输出端相连,所述电源(5)还为报警装置(6)供电。

权利要求书

1. 一种电力设备户外箱体环境实时监控装置,所述户外箱体(1)为户外端子箱或机构箱,在所述户外箱体(1)内安装有温度传感器(2)、湿度传感器(3)、加热器(4)和电源(5),所述温度传感器(2)通过温度控制器(3)与加热器(4)相连,所述电源(5)为温度控制器(3)供电,其特征在于,所述实时监控装置包括安装在户外箱体(1)内用于实时采集加热器的加热次数的监控装置(6)以及安装在户外箱体(1)外侧面用于在所述加热次数超过阈值上限以及低于阈值下限时进行报警的报警指示灯(7),其中,所述监控装置(6)的输入端连接到温度控制器(3)与加热器(4)之间的连接线上,所述报警指示灯(7)的输入端与报警装置(6)的输出端相连,所述电源(5)还为报警装置(6)供电。

2. 根据权利要求1所述的电力设备户外箱体环境实时监控装置,其特征在于,所述监控装置(6)包括微处理器(61)和第一显示屏(62),所述微处理器(61)的输入端连接到温度控制器(3)与加热器(4)之间的连接线上,所述第一显示屏(62)和报警指示灯(7)的输入端均连接到微处理器(61)的输出端,电源(5)与微处理器(61)的电源端相连。

3. 根据权利要求2所述的电力设备户外箱体环境实时监控装置,其特征在于,所述监控装置(6)进一步包括一监控箱体(60),所述微处理器(61)安装于该监控箱体(60)的内部或者背面,所述第一显示屏(62)设置于该监控箱体(60)的正表面上,在所述监控箱体(60)的正表面上还设有一与微处理器(61)输入端相连的输入单元(63)和复位按钮(611)。

4. 根据权利要求2所述的电力设备户外箱体环境实时监控装置,其特征在于,所述微处理器(61)的输出端与加热器(4)的输入端相连,以在微处理器(61)采集的加热次数小于阈值下限或大于阈值上限时控制加热器(4)工作。

5. 根据权利要求1所述的电力设备户外箱体环境实时监控装置,其特征在于,所述监控装置(6)包括计数器(65)和第二显示屏(66),所述计数器(65)的输入端连接到温度控制器(3)与加热器(4)之间的连接线上,所述第二显示屏(66)和报警指示灯(7)的输入端均连接到计数器(65)的输出端,电源(5)与计数器(65)的电源端相连。

6. 根据权利要求5所述的电力设备户外箱体环境实时监控装置,其特征在于,所述计数器(65)的输出端与加热器(4)的输入端相连,以在计数器(65)采集的加热次数小于阈值下限或大于阈值上限时控制加热器(4)工作。

7. 根据权利要求1-6任一项所述的电力设备户外箱体环境实时监控装置进行监控的方法,其特征在于,其包括以下步骤:

步骤1,温度传感器监测户外箱体内部的温度信息,所述温度信息包括温度信息和湿度信息,当所述温度信息小于温度控制器给定的温度条件以及湿度信息大于湿度控制器给定的湿度条件时,温度控制器启动加热器工作;

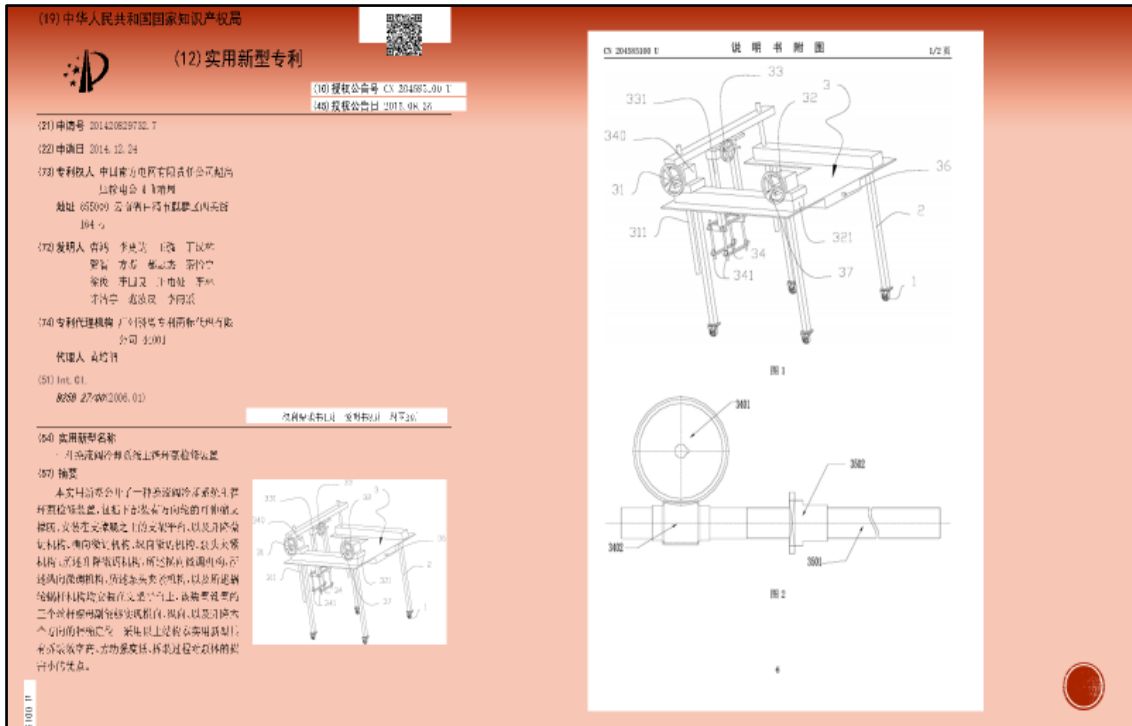
步骤2,启动加热器时,温度控制器与加热器之间的连接线上产生一电流脉冲,该电流脉冲触发监控装置计数;

步骤3,统计一段时间内监控装置的计数次数,并与该监控装置内设置的该段时间内加热次数阈值上限和加热次数阈值下限进行比较;

步骤4,当所述计数次数不在加热次数阈值下限和加热次数阈值上限之间时,监控装置驱动报警指示灯和加热器工作;

步骤5,显示屏存储所述监控装置驱动报警指示灯和加热器工作的事件报告。

8



9



10

PROTECTION SCOPE

- The scope of protection of the patent right for an invention or utility model shall be determined by the terms of **the claims**. **The description and the appended drawings** may be used to interpret the claims.
- The scope of protection of the patent right for design shall be determined by the product incorporating **the patented design as shown in the drawings or photographs**.



11

INFRINGEMENT ACT

- For an invention or utility model, no entity or individual is entitled, without permission of the patentee, **to make, use, promise to sell, sell or import** the patented product, or **to use the patented process and to use, promise to sell, sell or import** the product directly obtained from the patented process, for production or business purposes.
- For a design, no entity or individual is entitled, without permission of the patentee, **to make, promise to sell, sell, or import** the design product, for production and business purposes. *(to use ?)*



12

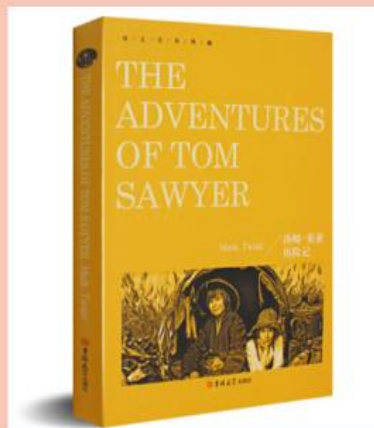
WORKS

- **“Works” is Copyright Law’s headstone.**
- **“works”** shall refer to **original** intellectual achievements in the fields of literature, art and science that can be **expressed** in a certain form:
 1. written works;
 2. oral works;
 3. musical, dramatic, quyi, choreographic and acrobatic art works;
 4. works of fine art and architecture
 5. photographic works;
 6. audiovisual works
 7. drawings of engineering designs and product designs, maps, sketches and other graphic works as well as model works;
 8. computer software;
 9. other intellectual achievements that meet the characteristics of works.



13

WRITTEN WORK



14

MUSICAL WORK



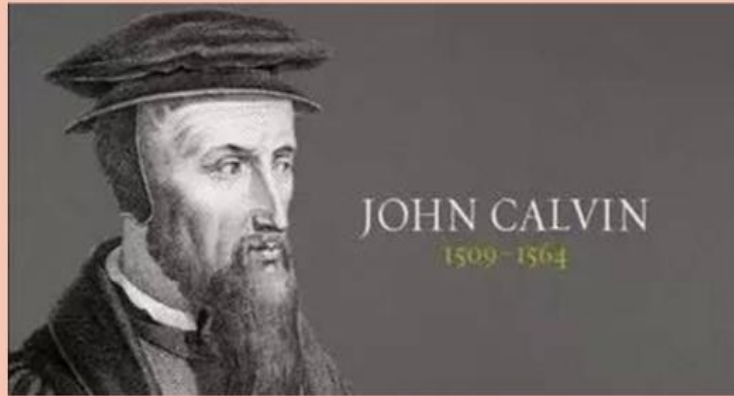
15

ACROBATIC ART WORK



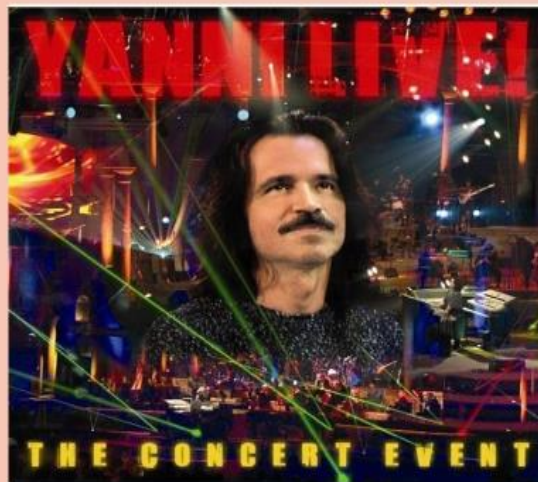
16

WORK OF FINE ART



17

AUDIOVISUAL WORK



18

CHOREOGRAPHIC WORK



19

PHOTOGRAPHIC WORK



20

ARCHITECTURE



21

MAP



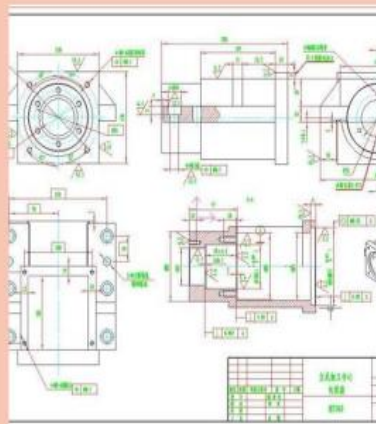
22

SKETCH



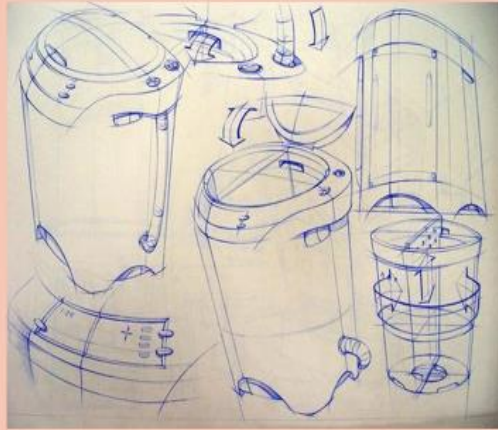
23

DRAWING OF ENGINEERING DESIGNS



24

DRAWING OF PRODUCT DESIGNS



25

COMPUTER SOFTWARE

```
public partial class Sys_Admin
{
    public int Id { get; set; }
    public string LoginName { get; set; }
    public string Pwd { get; set; }
    public string DisplayName { get; set; }
    public Nullable<int> LoginCount { get; set; }
    public Nullable<System.DateTime> LastLoginDate { get; set; }
    public string LastLoginIP { get; set; }
    public string Remark { get; set; }
    public Nullable<bool> Active { get; set; }
    public Nullable<int> CreateBy { get; set; }
    public Nullable<System.DateTime> CreateOn { get; set; }
    public Nullable<int> UpdateBy { get; set; }
    public Nullable<System.DateTime> UpdateOn { get; set; }
}
```

云教程中心

26

COPYRIGHT

- **“Copyright”** shall include the following **personal rights and property rights**:
 1. **the right of publication**, that is, the right to decide whether to make a work available to the public;
 2. **the right of authorship**, that is, the right to claim authorship and to have the author's name mentioned in connection with the work;
 3. **the right of alteration**, that is, the right to alter or authorize others to alter one's work;
 4. **the right of integrity**, that is, the right to protect one's work against distortion and mutilation;
 5. **the right of reproduction**, that is, the right to produce one or more copies of the work by means of printing, Xeroxing, rubbing, sound recording, video recording, duplicating, re-shooting, or digital way etc.;
 6. **the right of distribution**, that is, the right to provide the public with original copies or reproduced copies of works by means of selling or donating;

27

COPYRIGHT

7. **the right of lease**, that is, the right to non-gratuitously permit others to temporarily use the original or copy of audiovisual works and computer software, unless the computer software is not the main object of lease;
8. **the right of exhibition**, that is, the right to publicly display the original copies or reproduced copies of works of fine art and cinematographic works;
9. **the right of performance**, that is, the right to publicly perform works, and to publicly transmit the performance of works by various means;
10. **the right of projection**, that is, the right to make, by such technical equipment as projector, episcopes, etc., the works of fine art, photographic works, audiovisual works, etc. reappear publicly;
11. **the right of broadcasting**, that is, the right to publicly broadcast or disseminate works by wired or wireless means, and to disseminate broadcast works to the public by audio amplifier or other similar instruments for transmission of signs, sounds or images, excluding the right as prescribed in item (12) of this paragraph;

28

COPYRIGHT

12. **the right of dissemination via information networks**, that is, the right to provide works that may be obtained by the public at the time and place selected by the public by wired or wireless means;
13. **the right of production**, that is, the right to fix works on the carrier audiovisual works;
14. **the right of adaptation**, that is, the right to modify a work for the purpose of creating a new work of original creation;
15. **the right of translation**, that is, the right to transform the language of a work into another language;
16. **the right of compilation**, that is, the right to choose or edit some works or fragments of works so as to form a new work;
17. other rights which shall be enjoyed by the copyright owners.



29

COPYRIGHT-RELATED RIGHTS

- **Publisher's Right** : A publisher shall be entitled to permit others to exploit the format design of a published book or periodical of his or prohibit others from doing so.
- **Performer's Right**: A performer shall, in relation to his performance, enjoy the rights:
 1. to show his/her identity;
 2. to protect the character in his performance from distortion;
 3. to authorize others to make live broadcasts or to publicly transmit his live performance, and to receive remuneration for it;
 4. to authorize others to make sound recordings and video recordings, and to receive remuneration for it.
 5. to permit others to reproduce, distribute and lease the sound recordings or video recordings which record his performance, and to receive remuneration for it;
 6. to permit others to disseminate his performance to the public through information network, and to receive remuneration for it.



30

COPYRIGHT-RELATED RIGHTS

- **Producer of Sound Recordings or Video Recordings' Right:** A producer of sound recordings or video recordings shall have the right to permit others to reproduce, distribute, lease and disseminate to the public through information network such sound recordings or video recordings and shall have the right to receive remuneration for it.
- **Broadcasting Station or Television Station's Right:** A broadcasting station or television station shall have the right to prohibit the following acts conducted without its permission:
 1. Rebroadcasting a radio or television program broadcast by it by wired or wireless means.
 2. Recording and reproducing a radio or television program broadcast by it.
 3. Disseminating a radio and television broadcast by it to the public via information networks.



31

INFRINGEMENT ACT

- Any acts, without permission of the obligee, unless otherwise provided in Copyright Law, such as: to alter, or to publish, to reproduce, to distribute, to perform, to lease, to exhibit, to broadcast, to translate, to project, to adapt, to compile the works, are illegal. That is to say, they all are infringement acts upon the copyright of works.



32

TRADEMARK

- **Trademark:** Any sign including *word, design, letter, numeral, three-dimensional symbol, combination of colors, and sound, as well as a combination of the above* may serve as a registered trademark .
- The trademark for registration shall be **distinctive** for easy identification, and may not be in conflict with any **prior legal rights** acquired by others.



33

TRADEMARKS



34

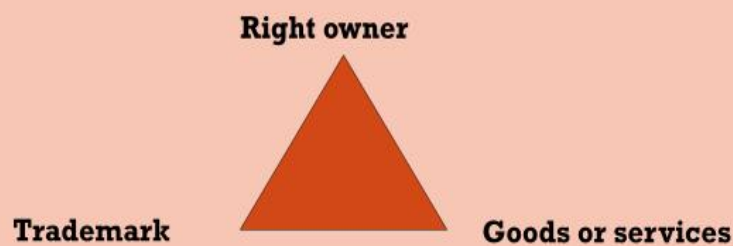
PROTECTION SCOPE

- **The exclusive right of registered trademark** shall be limited to the trademark *approved for registration* and the goods or services on which the trademark is *approved to be used*.



35

THE EXCLUSIVE RIGHT



36

INFRINGEMENT ACT

- Any of the following conduct shall be an infringement upon the right to exclusively use a registered trademark:
 1. Using a trademark **identical with** a registered trademark on **identical goods or services** without being licensed by the trademark registrant.
 2. Using a trademark **similar to** a registered trademark on **identical goods or services**, or using a trademark **identical with** or **similar to** a registered trademark on **similar goods or services**, without being licensed by the trademark registrant, which may **easily cause confusion**.
 3. **Selling goods or services** which infringe upon the right to exclusively use a registered trademark.



37

ACTS OF UNFAIR COMPETITION

- **Business Confusion:** business operators shall not commit the following acts of confusion to mislead a person into believing that **a commodity belongs to another person or has a particular connection with another person:**
 1. Using without permission **a label identical or similar to** the name, packaging or decoration of another person's commodity with certain influence.
 2. Using without permission **another person's name** with certain influence, such as the name of an enterprise, the name of a social organization, or the name of an individual.
 3. Using without permission **the principal part of a domain name, the name of a website, or a web page** with certain influence of another person.



38

ACTS OF UNFAIR COMPETITION

▪ Trade Secrets

Trade secret refers to the technical information and business information that is **unknown to the public**, has **commercial value**, and for which the obligee **adopts certain security measures**.



39

ACTS OF UNFAIR COMPETITION

▪ Business operators shall not commit the following **acts of infringing upon trade secrets**

1. **Acquiring** a trade secret from the right holder by theft, bribery, fraud, coercion, electronic intrusion, or any other illicit means.
2. **Disclosing, using, or allowing another person to use** a trade secret acquired from the right holder by any means as theft, bribery, fraud, coercion, electronic intrusion, or any other illicit means.
3. **Disclosing, using, or allowing another person to use** a trade secret in violation of his or her confidentiality obligation with the right holder
4. **Abetting, or tempting, or aiding a person to disclose, use, or to allow another person to use** a trade secret in violation of his or her non-disclosure obligation with the right holder.



40



Materials | Compact

Data Protection in China

Jennifer Feng, attorney at law in Guangzhou

Guangzhou, December 2021

With the rapid development of information technology, more and more service or products providers collect, store, process, analyze and/or use all kinds of data to find business opportunities. Through big data technology, these providers can easily learn our name, gender, address, hobbies, or even our family information, income level, health status, etc. In order to pursuit of profits, some companies began to improperly collect, process, or resell people's personal information, even violate the privacy of individuals. The big-data mining and personal information resale have opened the door for criminals, especially fraudsters. Those companies that have acquired the personal data of millions or even billions of individuals actually gain super power. They are able to easily manipulate people's behavior. For example, a UK data consultancy firm, Cambridge Analytica, was alleged that it misused the data of millions of Facebook users for Donald Trump's presidential campaign in 2016. Thus, the PRC government is more and more concerned about the misuse of big data.

On the other hand, the rapid development of information technology is leading our life and society to be more efficient and transparent. In today's China, people rarely use cash in their daily life, in contrast, they finish their payment via the app WeChat and/or AliPay on their mobile phone. In recent years, the majority of buying and selling activities happen online. The extensive use of e-application system and biometric identification enable people to deal with things at home by just clicking buttons on their phones, which cut short the application time from months or days to minutes. Presetting the nationwide e-application systems also makes the application procedure more predictable and transparent.

Thus, it becomes a big issue for the PRC government to balance the benefit and negative impact of big data technology. In this article, we will try to give our readers an overview of laws and regulations related to data protection in China.

For data security, China's legislation has been enacted separately in the areas of civil, criminal and administrative Law.

1. Civil Law System

Civil law mainly deals with the relationship between natural persons, or the relationship between a natural person and a legal person. Therefore, the main concern under the civil law system is the protection of personal information. Before the popularity of information technology, China's civil law legislation related to data protection mainly focus on personal rights such as life, health, portrait, privacy, reputation, etc. An individual whose rights is infringed can seek judicial relief under General Principles of Civil Law (The predecessor of the Civil Code), and Tort Liability Law, which is a secondary legislation of civil law.

After entering the information era, some personal information that didn't seem important before, such as name, address, email, track of a person's movement, if combined with other information, may be used to deduce the valuable or private information of a person, e.g., a person's consumption habits, hobbies, interpersonal relationship. Thus, a more specific and comprehensive secondary law was introduced, i.e., Personal Information Protection Law (Effective on November 1, 2021).

Under the civil law system, personal information is classified as three levels according to their importance and sensitivity. Please refer to the below chart.

Personal Information Protection Law mainly stipulates the rules of processing personal information and sensitive personal information, the rights and obligations of individuals in the processing of personal information. The law also provides guidelines on handling the personal information by state organs, as well as rules for cross-border transmission of personal information. According to the law, processing of personal information includes collection, storage, use, transmission, providing, publicizing, deletion, etc. The activities involving in processing personal information of natural persons within the border of China are also subject to this law, such as the activities aimed to provide product or service to domestic people, analyze and evaluate the behavior of natural persons in China, or another stipulated situation.

The law stipulates four basic principles for natural person's data processing:

- **Lawfulness.** Any organization or individual must not illegally collect, use, process or transmit other person's personal information. It is prohibited to illegally trade, provide or publicize personal information. It is prohibited to process personal information that may cause harm to national security or public benefit. The processors are obliged to take necessary measures to ensure safety of personal information.
- **Justification.** This principle requires that the purpose of processing personal information must be specific, clear and reasonable. The processors shall follow the principle of openness and transparency. They are required to disclose their rules of processing personal information, and express the purposes, methods and scope of processing.
- **Necessity.** The collection of personal information should be limited to the minimum extent for fulfillment of the process purpose.

- Good Faith. Any organization or individual shall obtain informed consent from natural persons before they process personal information except several stipulated situations (Emergency Avoidance). Misleading, intentional omission or obscure language may cause the consent being void. The processing shall not exceed the scope of consent.

Processing sensitive personal data is prohibited unless a personal data processor aims to a specific purpose with sufficient necessity and takes strict protective measures. In addition, the individual's informed consent shall be obtained in advance unless the law stipulated otherwise. Under some circumstances, a written consent is required.

It is worth to know that when it is necessary for personal information processors to provide personal information to outside the territory of the People's Republic of China, the processors must meet one of the following conditions: 1) passing safety assessment organized by the competent government authority; 2) obtaining Personal Information Protection Certification issued by authorized professional institutions; 3) adopting the template contract formulated by competent government authority ; or 4) other conditions stipulated by law or regulation.

2. Criminal Law

To prevent and fight against crime of infringe data safety, Criminal Law stipulates several crimes.

- Crime of infringing upon citizens' personal information. Any organization or individual violates the relevant laws and regulations to sell personal information of citizens to a third party shall be imposed a fine, and/or sentenced to criminal detention or fixed-term imprisonment, which can be as long as no more than 7 years.
- Crime of refusing to perform the obligation to manage information network security. The object of this crime is internet service providers, which provide information to the public or provide services to the people who intend to obtain internet information. The providers may be imposed a fine, and/or sentenced to criminal detention or no more than 3 years fixed-term imprisonment if they refused to correct their security measures under the requirement of the competent supervision authority so as to cause 1) widespread of illegal information; 2) serious harm by disclosure of users' information; 3) serious harm due to the loss of evidence in a criminal case; or 4) other serious circumstances.

3. Administrative Law System

From the perspective of strengthening the administration of data by the government, China has also introduced a series of laws, the most important of which are Cybersecurity Law (effective on 1st June, 2017) and Data Security Law (effective on 1st September, 2021).

1) *The purpose of the two laws*

We can see the common purposes of the two laws: both aim to the safeguard of national security (Data Security Law adds sovereignty security), and the protection of the legal rights of individuals and organizations. On the other hand, the two laws aim to the protection of network and data, as well as to promote the development and utilization of data and information technology.

This is a good example shows the effort by the PRC government to balance the benefit and negative impact arising from the development of new technology.

2) *Cybersecurity Law*

All the organizations or individuals that construct, operate, maintain and use the network within the People's Republic of China, as well as the supervision and management of network security are subject to this law.

The PRC government implements network security level protection rules. Network operators should fulfill their security protection obligations in accordance with the rules to protect the network from interference, sabotage, or unauthorized access, and to protect network data from being leaked, stolen or tampered.

The PRC government implements the key protection for those important industries and fields, such as public communications, information services, energy, transportation, water conservancy, finance, public service, and e-government, as well as the key information infrastructure, which could seriously endanger national security, national economy, and the people's livelihood and public interests if it is destructed, loss of functionality or data leakage.

It is required that the operators of key information infrastructure must store any and all personal data collected and generated during its operating in the People's Republic of China. The State Council is authorized by the law to formulate the specific scope and security protection measures for critical information and infrastructure. By now, we have not seen any specific measures by the State Council. There is a similar stipulation (Art. 40) in the Personal Information Protection Law, which mentioned that the key information infrastructure operators and personal information processors shall store the data domestically collected and generated within the People's Republic of China when the processed amount of personal information reaches a certain amount. We have not found out how much "the certain amount" is yet but it is believed that the government will classify according to the importance and sensitivity of the data, not just amount of data. For example, Apple and Tesla are both required to store the data in China, although the number of customers of these two companies are far apart.

3) *Data Security Law*

The law advocates Big Data Strategy. The government will promote the construction of data infrastructure, encourage and support the innovative application of data in various industries and fields. The state will support the development and utilization of data to improve the

intelligent level of public services. This strategy will lead to innovative and profitable business in this field.

This law stipulates that the state protects data based on different types and levels of data classified according to the importance in social and economic development, and to the extent of harm that may be caused to national security, public interests or legal rights of organizations and individuals.

The law also stipulates the obligations of data processors. It is required that any process of data or development of new data technology must be aimed to promote economic and social development, improve people's common wealth and accord with social morality and ethics.

+ + +

Chapter Ten

Dispute Resolution in China, Litigation and Arbitration



1



2



Part I - Ways for Settlement of International Trade Disputes

1. Conciliation 和解

Conciliation refers to a process where parties resolve their dispute by direct negotiation on a voluntary basis without the assistance of a third party.

和解即由双方自行协商解决争议，无第三方介入。

3



Part I - Ways for Settlement of International Trade Disputes

Advantages 优点	Disadvantages 劣势
a. simple procedure 程序简单、非正式	a. often fails to reach a mutually satisfactory solution 常无法达成谅解
b. low cost 低成本	b. conciliation agreement lacks the legal binding effect 和解协议无法获得强制执行
c. possibility of maintaining the cooperative relationship 可能维持合作关系	

4




Part I - Ways for Settlement of International Trade Disputes

2. Mediation 调解

Mediation is a process where the parties involved in a dispute resolve their dispute with the assistance of a third party (the Mediator).

调解为争议各方在第三方（调解人）斡旋调解之下解决争议的方式。

5



Part I - Ways for Settlement of International Trade Disputes

- a. based on the respect for the free will of the parties and an informal negotiating atmosphere
尊重各方的意愿，气氛相对轻松
- b. the process of reaching an agreement will be accelerated due to the participation of the third party
基于第三方的斡旋，达成和解共识的可能性增加
- c. when the mediator is an arbitration body, it can make an award upon the parties' agreement, the award will have a legal binding effect
调解人为仲裁机构时，可要求仲裁机构就达成的协议作出确认
- d. less cost and simpler process compared with litigation and arbitration
与仲裁与诉讼比较，程序简单、成本较低

6




Part I - Ways for Settlement of International Trade Disputes

3. Litigation and Arbitration 诉讼和仲裁

- **Litigation 诉讼** - law suit by competent public court
(到法院打官司)
- **Arbitration 仲裁** - dispute settlement process where the parties submit their dispute to an arbitration institute to decide their dispute
- 仲裁指当事人将争议交由仲裁机构，由其按事实和法律进行裁决
- Litigation and Arbitration are currently the most popularly applied forms of dispute settlement in international transaction
- 诉讼和仲裁为国际贸易争端最为常用的解决方式


7



Part II - China's Law Court System and Arbitration System

第二部分 中国的诉讼与仲裁制度

8




Part II - China's Law Court System and Arbitration System

China's law court system is formed by 4 levels

- (1) Supreme People's Court—highest judicial organ of the State
最高人民法院—最高司法机关
- (2) Higher People's Courts—Each province has a higher people's court
高级人民法院—在各省、市、自治区设立
- (3) Intermediate People's Courts—located in a municipality
中级人民法院
- (4) Local People's Courts—located in rural counties or municipal districts
基层人民法院

9




Part II - China's Law Court System and Arbitration System

Two-final Trial System

- (1) Every case can be tried by the court of first instance, and can be appealed to a court of higher level.
每一个案件都可以发生一审及二审。
- (2) After the second trial, the case will have legal effect.
案件经过二审，即发生法律效力。
- (3) However, any party of the case can apply for a retrial after the second instance, but the application will not stopped the case from being enforced.
不服生效判决的当事人可以申请再审，但不停止案件执行。

10




Part II - China's Law Court System and Arbitration System

China's Arbitration Law

- (1) Arbitration by Institution 机构仲裁
 - China International Economic and Trade Arbitration Commission (CEITAC)
 - 中国国际经济贸易仲裁委员会
- (2) Ad hoc Arbitration 临时仲裁

11



Part II - China's Law Court System and Arbitration System

China's Arbitration Law

- (1) AL 1994 provides that an arbitration agreement must contain a declaration of intention to submit to arbitration, specify the scope of the matters subject to arbitration and designate the name of the arbitration body selected to conduct the arbitration.
 - 仲裁条款。
- (2) Enforcement of Arbitration Award
 - 仲裁裁决的执行

12



**Part III - Litigation and arbitration in
China: Which is better?**

**第三部分
中国的诉讼与仲裁，哪个更好？**

13



**Part III - Litigation and arbitration in
China: Which is better?**

1.Key differences between litigation and arbitration (区别)

Arbitration 仲裁	Litigation 诉讼
Arbitrators are appointed by the parties 仲裁员由当事人指定	judges are appointed by the state 法官由国家指定
arbitration body, arbitration rules, arbitration location can be chosen by the parties 仲裁机构、适用的程序规则、仲裁地 点可由当事人协商选定	procedure must be strictly in accordance with the law and the regulations 程序法定，当事人无法变更
hearing not open, decisions/judgments not made public 程序不公开，裁决不公布，私密性强	be generally heard publicly, judgments be publicly pronounced 原则上公开审理，判决公示
the award is final 一裁终局	judgments of any court of first instance can be appealed 实行两审终审制

14



Part III - Litigation and arbitration in China: Which is better?

2. Which is better: litigation or arbitration? 哪个更好?

Arbitration 仲裁

Advantages 优势	Disadvantages 劣势
<ul style="list-style-type: none"> •Parties can keep their disputes and business secret 保持争议事项的私密性 •Likely to be treated by the professionals with more expertise 通常由较为专业的人士审理 •The award can be far easier to be enforced in foreign countries 比较容易在外国获得执行 	<ul style="list-style-type: none"> •Arbitration bodies lack powers of granting of interim remedies 仲裁机构缺乏采取临时保护措施的权利 •International arbitration has become very expensive 国际仲裁成本高昂

15




Part III - Litigation and arbitration in China: Which is better?

2. Which is better: litigation or arbitration? 哪个更好?

Litigation 诉讼

Advantages 优势	Disadvantages 劣势
<ul style="list-style-type: none"> •much cheaper and faster than arbitration 程序比仲裁快捷、成本较低 •much quicker than many foreign courts 中国法院裁决比许多外国法院快 •put even more pressure on business partner 可以给争议对方施加更大的压力 	<ul style="list-style-type: none"> •quality of process and decision making vary across courts 各地法官素质差异较大 •susceptible to local protectionism and improper interferences 容易受地方保护主义和不正当干预影响 •more obstacles for judgment enforcement in foreign country 判决在国外较难获得执行

16



Part III - Litigation and arbitration in China: Which is better?

How to decide?

Chose of litigation or arbitration should be fact specific and dependent on the nature of the dispute.

选择使用诉讼还是仲裁解决争议，没有固定模式，因案而异。

17




Part III - Litigation and arbitration in China: Which is better?

Arbitration 仲裁:

- large cases (over 5 million RMB, for example)
争议数额较大的案件（例如500万元）
- cases likely to be heard in small city in China's interior, especially with powerful company owner as adversary
如果诉讼会在内地小城市进行，特别是对手在当地较有权势的话，则建议预设仲裁条款

18



Part III - Litigation and arbitration in China: Which is better?

Litigation 诉讼:

- Relatively small cases
相对较小的案件
- Cases need specific remedies such as an IP injunction, or a seizure of certain assets
如果案件可能涉及财产保全、知识产权保护等措施，建议以诉讼方式解决

19



Part IV - How to write a China contract, arbitration versus litigation?

第四部分
如何在合同中选择仲裁或是诉讼?

20



Part IV - How to write a China contract, arbitration versus litigation?

1. the benefits of a good contract with your business partner
一份完善合同的好处
2. ask this question: if there is a dispute under this agreement, am I most likely to be a plaintiff or a defendant
给自己提问：如果发生合同争议，我会是原告还是被告？
3. draft contract to maximize the chance to get good result
精心制作条款，确保获得最佳效果

21



Part IV - How to write a China contract, arbitration versus litigation?

Avoid unenforceable clause in China

在中国履行的合同应避免以下陷阱：

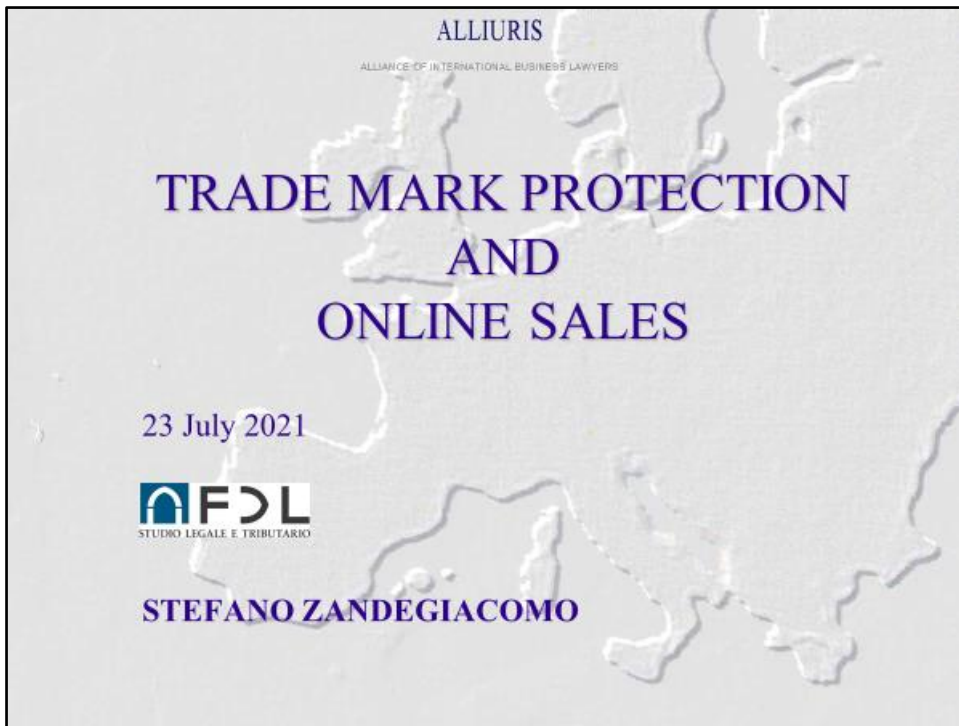
- contract governed by laws of a foreign country
适用外国法律作为准据法
- litigation in a law court of a foreign country
选择外国法院作为争议解决机构
- use languages other than Chinese
使用中文之外的其他语言作为合同语言

22

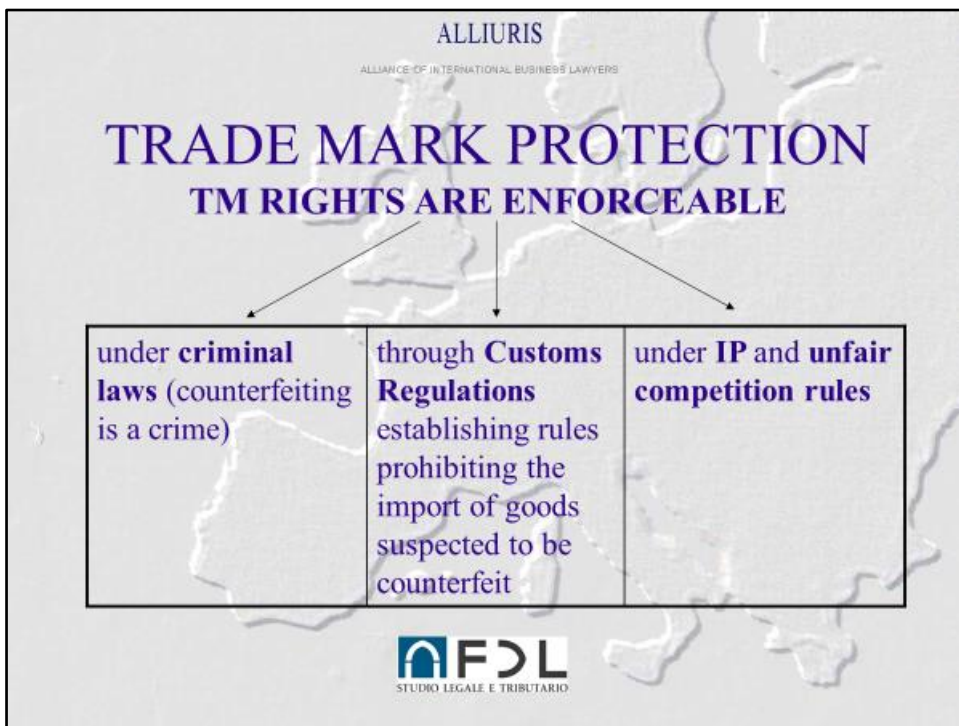


Chapter Eleven

Trade Mark Protection and Online Sales



1



2

ALLIURIS
ALLIANCE OF INTERNATIONAL BUSINESS LAWYERS

Actions based on IP rights infringements

- Protection of TM rights against counterfeit products («**fake products**»)
- Protection of TM rights against **original products sourced from outside the EU / EEA (European Economic Area) based on the «TM territoriality» principle**


STUDIO LEGALE E TRIBUTARIO

3


ALLIURIS
ALLIANCE OF INTERNATIONAL BUSINESS LAWYERS

PRINCIPLE OF «TRADE MARK TERRITORIALITY»

RIGHTS CONFERRED BY AN EU REGISTERED TRADE MARK

The proprietor of an EU trade mark shall be entitled to prevent all third parties not having his consent from using in the course of trade, in relation to goods or services, any sign where:
(...)
**«the following, in particular, may be prohibited:
c) importing or exporting goods under the sign»**

Art. 9 of Regulation (EU) No. 1001/2017 on the European Union TM


STUDIO LEGALE E TRIBUTARIO

4

ALLIURIS
ALLIANCE OF INTERNATIONAL BUSINESS LAWYERS

GREY MARKET

In case of goods manufactured outside of the European Economic Area (EEA) and **imported in the EEA without the consent of the TM owner**, the IP right holder has the right to oppose to the **parallel import** and subsequent resale on the EU market of such (original) products that were first put on the market outside of the EU.

 FDL
STUDIO LEGALE E TRIBUTARIO


5

ALLIURIS
ALLIANCE OF INTERNATIONAL BUSINESS LAWYERS

“EXHAUSTION OF THE RIGHTS CONFERRED BY AN EU TRADE MARK”

“An EU trade mark shall not entitle the proprietor to prohibit its use in relation to goods which have been put on the market in the European Economic Area under that trade mark by the proprietor or with his consent”

Art. 15 § 1 of Regulation (EU) No. 1001/2017

 FDL
STUDIO LEGALE E TRIBUTARIO

6

ALLIURIS
ALLIANCE OF INTERNATIONAL BUSINESS LAWYERS

The above «exhaustion» principle does not apply when there exist

“legitimate reasons for the proprietor to oppose further commercialisation of the goods, especially where the condition of the goods is changed or impaired after they have been put on the market”

Art. 15 § 2 of Regulation (EU) No. 1001/2017


 FDL
STUDIO LEGALE E TRIBUTARIO

7

ALLIURIS
ALLIANCE OF INTERNATIONAL BUSINESS LAWYERS

The European case-law has included the existence of a Selective Distribution System (SDS) among the «legitimate reasons» preventing the exhaustion of TM rights.

«damage done to the reputation of a trade mark may, in principle, be a *legitimate reason* within the meaning of [Article 7(2) of the Directive 89/104/EEC], allowing the proprietor of the mark to oppose further commercialisation of luxury goods which have been put on the market in the EEA by him or with his consent» (ECJ Copad / Dior, C-59/2008).

 FDL
STUDIO LEGALE E TRIBUTARIO

8

ALLIURIS
ALLIANCE OF INTERNATIONAL BUSINESS LAWYERS

For this reason, in order to protect the image and brand reputation of the so called «luxury goods», a crucial aspect is the **distribution system** adopted by TM owners to distribute their goods in the EU.


STUDIO LEGALE E TRIBUTARIO

9

ALLIURIS
ALLIANCE OF INTERNATIONAL BUSINESS LAWYERS

“SELECTIVE DISTRIBUTION SYSTEM” (SDS)

SDS means 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».

Art. 1, letter e) of Commission Regulation (EU) No. 330/2010


STUDIO LEGALE E TRIBUTARIO

10

ALLIURIS
ALLIANCE OF INTERNATIONAL BUSINESS LAWYERS

SDS: A «PROTECTED» NETWORK

- SDS is compatible with Article 101 (1) of the TFEU
- SDS is very important in order to:
 - i) **ensure consistent standards and quality of service in terms of how the products are sold, with the goal of preserving the luxury nature of the products;**
 - ii) **build brand equity through particular brand positioning;**
 - iii) **take legal actions against grey marketers and/or stop sales which are made in an inappropriate manner or in inappropriate/unauthorised sales outlets.**

 **FDL**
STUDIO LEGALE E TRIBUTARIO

11

ALLIURIS
ALLIANCE OF INTERNATIONAL BUSINESS LAWYERS

LEGAL CONTEXT OF «ONLINE SALES»

- VBER - REGULATION (EU) No. 330/2010**
- GUIDELINES ON VERTICAL RESTRAINTS – EU COMMISSION NOTICE (2010/C 130/01)**
- E-COMMERCE SECTOR INQUIRY (EU Commission – May 6, 2015)**

 **FDL**
STUDIO LEGALE E TRIBUTARIO


12

ALLIURIS
ALLIANCE OF INTERNATIONAL BUSINESS LAWYERS

VBER - Vertical Block Exemption Regulation
(Commission Regulation (EU) No. 330/2010)

Restrictions that remove the benefit of the block exemption – so called «**hardcore restrictions**»:

- Art. 4 (b)** the restrictionof the customers to whom a buyer to the agreement ... may sell the contract goods or services ...
- Art. 4 (c)** the restriction of active or passive sales to end users by members of a selective distribution system operating at the retail level of trade.



STUDIO LEGALE E TRIBUTARIO

13

ALLIURIS
ALLIANCE OF INTERNATIONAL BUSINESS LAWYERS

• **(52) Guidelines on Vertical Restraint**
«The **internet is a powerful tool to reach a greater number and variety of customers** than by more traditional sales methods ... wich explains why **certain restrictions on the use of the internet are dealt with as (re)sales restrictions**».

IN PRINCIPLE, EVERY DISTRIBUTOR MUST BE ALLOWED TO USE THE INTERNET TO SELL PRODUCTS


STUDIO LEGALE E TRIBUTARIO

14

ALLIURIS
ALLIANCE OF INTERNATIONAL BUSINESS LAWYERS

- **(54) Guidelines on Vertical Restraint**

Under the Block Exemption **the supplier may require quality standards for the use of the internet site to resell its goods** ...this may be relevant in particular for selective distribution.


«a supplier may require that its distributors use third party platforms to distribute the contract products only in accordance with the standards and conditions agreed between the supplier and its distributors for the distributors' use of the internet»


STUDIO LEGALE E TRIBUTARIO

15

ALLIURIS
ALLIANCE OF INTERNATIONAL BUSINESS LAWYERS

- **(54) «For instance, where the distributor's website is hosted by a third party platform, the supplier may require that customers do not visit the distributor's website through a site carrying the name or logo of the third party platform»**


STUDIO LEGALE E TRIBUTARIO

16

ALLIURIS
ALLIANCE OF INTERNATIONAL BUSINESS LAWYERS

**Coty Germany GmbH - Parfümerie Akzente GmbH
(ECJ – case C-230/16 of 6 December 2017)**

This is a key ruling for the protection of luxury brands' image and to determine how luxury goods are placed on digital platforms.

It has stated that the supplier of luxury goods can impose on its authorised distributors to sell such goods on the Internet «**solely through their own online shops**» and «**not using a different business name**» or «**third-party platforms in a discernible manner**».



17

ALLIURIS
ALLIANCE OF INTERNATIONAL BUSINESS LAWYERS


Ruling

In particular EJC in Coty's case has stated that:

«**the prohibition imposed on the members of a selective distribution system for luxury goods, which operate as distributors at the retail level of trade, of making use, in a discernible manner, of third-party undertakings for internet sales**

does not constitute

a restriction of customers, within the meaning of **Article 4(b)** of that regulation, or a **restriction of passive sales to end users**, within the meaning of **Article 4(c)** of that regulation».



18

ALLIURIS
ALLIANCE OF INTERNATIONAL BUSINESS LAWYERS

**OTHER «LEGITIMATE REASONS»
FOR A TM OWNER TO OPPOSE FURTHER
COMMERCIALIZATION OF GOODS:**

- (i) **Re-packaging:** opening and closing afterwards again the *cellophane* protecting the products (in case of pharmaceuticals: ECJ Bristol-Myers Squibb C- 427/93);
- (ii) **Re-labelling** (in case of beverages: ECJ Ballantine C-349/95);
- (iii) **Manipulations/decoding of batch codes and products' identification codes** (ECJ Loendersloot/Ballantines C-349/95; ECJ Hoffmann-La Roche/Centrafarm C-102/77; ECJ Pfizer/Eurim-Pharm C-1/81).



19

ALLIURIS
ALLIANCE OF INTERNATIONAL BUSINESS LAWYERS

Manufacturers/suppliers normally put manufacturing codes on their products in order to identify the **production batch**.

Batch codes are mandatory for certain categories of products, like for example:

«cosmetic products shall be made available on the market only where the container and packaging of cosmetic products bear (...) the batch number of manufacture or the reference for identifying the cosmetic product»

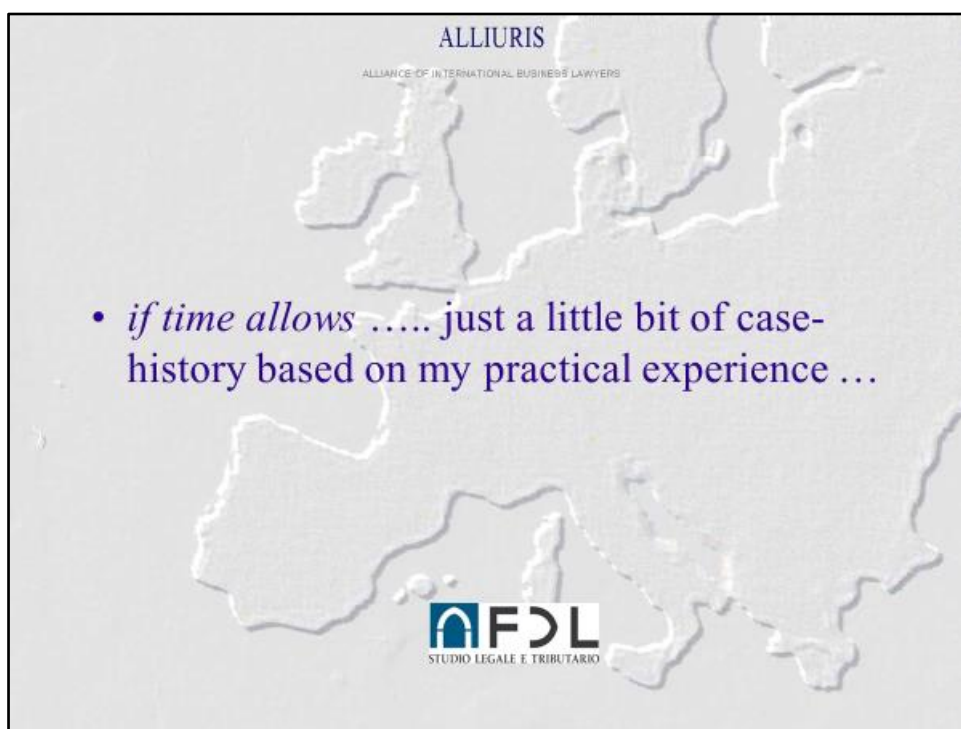
Art. 19, lett. e) of Regulation EC No. 1223/2009 on cosmetic products



20



21



22



23

 A black and white portrait of a man with short dark hair and glasses, wearing a dark suit jacket, a white shirt, and a patterned tie. He is smiling slightly and looking directly at the camera.	<p>Stefano Zandegiacomo De Zorzi Avvocato</p> <p>FDL Studio legale e tributario P.zza Borromeo, 12 - 20123 Milano T +39 02.72.14.921 F +39 02.80.52.565 info@fdl-lex.it</p>
--	---

Materials | Compact

International Trade Mark Protection

Aline Kristin Pehle, Trainee lawyer

Hanover, February 2021

New awareness through online marketing: What problems arise in trade mark protection?

Today, most companies that want to increase their national or international profile rely on online marketing, as for many this is the easiest and - supposedly - most cost-effective way. It is no longer just traditional web domains or ad windows that are used, but also social media channels. Even many small and medium-sized companies now maintain their presence in social networks as a matter of course. In addition, the cooperation with so-called Influencers or celebrities is becoming increasingly popular.

The possibilities to increase one's reach are therefore becoming more and more diverse. Appropriate and clever marketing can even be used to specifically trigger or exploit real "Internet hype". A company or its brand can thereby achieve a high profile in the desired target group within a few days or weeks - and sometimes worldwide. However, the attempt to establish or expand in new markets through the rapid prominence of brands should also prompt entrepreneurs to take a proactive approach to the relevant property rights.

How protected is one's own brand in a suddenly newly opening market? And how protected is one's own brand in the regular sales territory if an unexpected competitor enters (perhaps even overnight)?

National, European, and global trade mark protection

In the trade mark protection system, a fundamental distinction must be made between the national, European, and global levels.

As a starting point, when a trade mark is to be used for the first time in a particular country, it is a matter of national trade mark law.

In Germany, a trade mark can be applied for at the German Patent and Trade Mark Office (headquarters in Munich). The protection extends geographically to the entire territory of Germany, temporally for an initial period of ten years, with the possibility of extension for a fee shortly before the expiry of the term.

If a trade mark is to be protected within the borders of the EU, it can be registered as an EU trade mark. The legal basis is an EU regulation^[1]. The European Union Intellectual Property Office (EUIPO), which is based in Alicante, Spain, is responsible for this. After the expiration of ten years, the trade mark protection can be extended again for another ten years.

The great advantage of the EU trade mark is the uniform legal protection throughout the EU. The trade mark does not have to be applied for individually in each member state in which it is to be used and enjoys the same standard of protection everywhere.

However, this advantage is at the same time its major disadvantage: obstacles to registration in only one member state (e.g. the opposition of the owner of an earlier trade mark) usually prevent the creation of the EU trade mark. If it turns out after registration that there were grounds for refusal in only one state, the EU trade mark may lose its protection in all other member states as well. Whether this is a disadvantage or not, depends on the perspective. Therefore, as soon as an entrepreneur intends to have his trade mark protected throughout the European Union due to an intended expansion, he should not only look for possibly earlier or prioritized Community trade marks, but also for earlier trade marks in each of the 27 member states within the scope of a trademark search.

Efforts by states to establish trade mark protection at the international level through treaties under international law have existed since the end of the 19th century. Even if there is still no uniform, globally valid trade mark protection law, the international community has at least been able to agree on certain minimum standards and has in the meantime created the WIPO in Geneva, the World Intellectual Property Organization. Based on the Madrid Trade Mark Protection System, the Paris Convention for the Protection of Industrial Property and most recently the TRIPS[2] Agreement of the WTO, it is possible to obtain protection of a trade mark in over 190 different countries through WIPO.

The advantage of using the WIPO system as opposed to going through the respective national patent offices of the individual states is first of all that the trade mark owner is ultimately entitled to registration in the desired additional states. Once registered in a contracting state, registration in other states can only be denied in exceptional cases. In addition, foreign trade mark owners may not be treated worse than domestic trade mark owners since there is an equal treatment requirement.

It should be emphasized, however, that no universal trade mark is created here; rather, the territoriality principle has an effect: A one-time registration and thus automatic protection in all contracting states cannot be obtained. Instead, it must be specifically stated in which states the trade mark is to obtain protection. The legal consequence is that the loss of trade mark protection in one of the contracting states does not at the same time mean the loss of protection in another state. The main problem for the competitor is that he must enforce his trade mark protection in each of the states concerned individually, always with the uncertainty that it is not clear whether his action will be successful in each case.

Trade mark protection in new markets

New market - new registration

The principles of territoriality, registration and priority are common in all three systems. A trade mark can only be protected where it has been entered in a trade mark register and thus officially

granted protection rights. In addition, older trade marks have priority over younger trade marks, they are prioritized.

If a company's brand gains sudden recognition/popularity in other countries as a result of successful social media campaigns, but is not registered there, any competitor can first make use of this brand - i.e. use it or, in the worst case, register it themselves. The seemingly promising appearance on the new market can therefore quickly turn into a failure without registration.

If the company unexpectedly encounters a new competitor on its traditional market whose trade mark is more or less identical to its own trade mark, the first thing to consider is which of the two is already registered. Only if its own trade mark is already registered can the company take action against the competitor. However, it should not succumb to the temptation to make use of a competing trade mark itself, as this could possibly give rise to liability under competition law. If neither of the two trade marks has yet been registered, the priority principle also applies: the trade mark that is registered first prevails and is protected against the other trade mark. This sometimes leads to a race against time.

A company that intends to sell its products under a particular trade mark in a particular market or even just to advertise them there is therefore strongly advised to register the trade mark with the relevant authority - be it the national trade mark office, the EUIPO or the WIPO. In addition, a thorough trade mark search should be carried out in advance to rule out the possibility that the trade mark is already protected in favor of another rights holder. Nowadays, this has become relatively easy by means of registers that can be viewed online.[3] Nevertheless, in individual cases it can be difficult to assess whether one's own trade mark differs strongly enough from an already registered trade mark, e.g. in the case of figurative trade marks. If necessary, it is advisable to seek the advice of a specialist attorney in order to avoid the unnecessary waste of time and expense that can result from a refusal to register.

The principle of "well-known" trade marks

No rule without exception. An outgrowth of the priority principle which is generally accepted is the principle that no new trade mark may be registered which is identical (probably including imitation or translation) with a trade mark which is generally known or popular. In English, these trade marks are referred to as "well-known trade marks", in German as "notoriously well-known trade marks". Following this principle, a domestic, unregistered trade mark may well claim protection against a new foreign trade mark. Conversely, a foreign trade mark that is not registered in Germany may also be granted protection against a new domestic trade mark.

The "well-known trade marks" have been legally regulated in the WTO/WIPO system, in the USA, the EU and in German trade mark law.

It seems only logical to now apply this concept to a trade mark that has achieved great recognition or prominence in a state or region through clever online marketing, even before the company has had the opportunity to distribute as well as register it: imitators who want to profit from any hype could be prohibited from using/registering an identical trade mark.

Here, the first question that arises is whether the trade mark must already be used or whether mere awareness is sufficient. Is it possible to protect a trade mark that has neither been registered nor used? The argument against this could be that its protection should possibly not be more extensive than the protection of properly registered trade marks. The TRIPS Agreement allows the contracting states to make the registration of a trade mark dependent on whether the trade mark is actually used. Three years are mentioned as a time frame for orientation. The EU even assumes an actual period of use of five years, but the act of affixing the trade mark to export goods is sufficient for the assumption of use.

However, the wording of the TRIPS Agreement deems the awareness of the trade mark through advertising in the respective contracting state to be sufficient. Over the years, there have also been several rulings in which actual use was not deemed necessary and which allowed the notoriety of "well-known trade marks" to be sufficient to fall under trademark protection.[4] This means that the protection of an unregistered trade mark not used domestically against use by third parties is thoroughly recognized.

There is no uniform definition of well-known or the "well-known" criterion. WIPO initially leaves the assessment of whether a trade mark is sufficiently well-known or whether there is a likelihood of confusion with a new trade mark to the respective national authorities. Therefore, minimum requirements have been developed through national practice and case law, all of which have in common that the trade mark must have a high degree of recognition in the target group: The TRIPS Agreement, for example, focuses on the public's knowledge of the relevant area ("sector"). The European Court of Justice (ECJ) requires the awareness in a "significant part" of the relevant "professional milieu." [5] The Court of Justice of the European Union (CFI, subordinate to the ECJ) even makes a spatial limitation: a corresponding awareness in the region instead of in the whole Member State, is sufficient.[6]

"Notoriously well known" implies that for a well-known mark to be protected, it must have been known for a certain period of time. In 1999, WIPO's Interpretative Recommendations to the TRIPS Agreement required, among other things, a certain length of time in which a mark has been known, used, or advertised for it to be considered "well-known."

But why should older well-known trade marks, which have had more time to be registered, necessarily be more worthy of protection than equally well-known younger trade marks that are "fresh" on the market? At least the English wording, which is likely to be the decisive one in an interpretation, allows for a certain opening.

Especially in times of digitalization, in which sufficient awareness in the target group, as is generally required, is achieved more and more quickly worldwide through targeted marketing abroad, triggering of Internet hype, etc., and in which competitive situations arise more quickly through exchange via international platforms, expansion through online trade, etc., it would appear that the term "fresh" is not a suitable term. Since competition situations arise more quickly, it seems only justified not to apply overly strict criteria to the duration of awareness. After all, the competitor who registers his trade mark first has the decisive advantage.

To assume as a ground for refusal only the existence of trade marks with a long reputation, but not that of more recent trade marks with a reputation, seems unreasonable and no longer up with the times.

Conclusion

Ultimately, of course, it depends on the further development of national practice. The safest way for entrepreneurs is still the registration.

Entrepreneurs should not miss the moment when a registrable trade mark is created, lest competitors who want to take advantage of a possible sudden popularity of the trade mark beat them to it by registering it. Nevertheless, it may be worthwhile to look ahead and have the protection concept of the "well-known trade mark" in mind for emergencies. After all, the significance and reach of a trade mark on the market does not always depend on its "notoriety" or age.

The concept of "well-known trade marks" raises yet another aspect that companies should keep in mind when conducting trade mark searches: In case of doubt, it is not sufficient to rely only on the trade mark registers. It should also be checked whether one's own trade mark collides with a "well-known trade mark" or "notoriously well-known trade mark". Otherwise, there may be unwanted surprises.

[1] EU VO 2017/1001

[2] Agreement on Trade-Related Aspects of Intellectual Property Rights

[3] DPMA Register: <https://register.dpma.de>

EU-Register: eSearch plus: <https://euipo.europa.eu/eSearch/>

WIPO-Register: Madrid Monitor: www.wipo.int/madrid/monitor/en/index.jsp

[4] McDonald's Fall (Südafrika) 1995; WHIRLPOOL Fall (Indien) 1986; TRIPP TRAPP Fall (Schweiz) 2004; EUG 2018: J-M.-E.V. e hijos, SRL vs EUIPO

[5] EuGH, General Motors-Fall, 1999

[6] EUG 2018: J-M.-E.V. e hijos, SRL vs EUIPO

+ + +

Chapter Twelve

Trade Mark Quiz

1. Presentations



1

EU Trade Mark Quiz

1


A gold Lindt bunny chocolate with a red ribbon and the text "Lindt GOLDHASE".

Lindt bunny ("Goldhase")

23 July 2021 | Alluris Summer School 2021

EU Trade Mark Quiz

2



"Libro" for books

23 July 2021 | Alluris Summer School 2021

The image shows a slide from a quiz. At the top right, it says "EU Trade Mark Quiz". In the top left corner, the number "2" is enclosed in a blue circle. The main content is the word "LIBRO" in a bold, sans-serif font. The letters "LI" are yellow, "BR" are orange, and "O" is red. Below the logo, the text "'Libro' for books" is centered. At the bottom, there is a small footer: "23 July 2021 | Alluris Summer School 2021".

3

EU Trade Mark Quiz

3

SWITZERLAND

"Switzerland" for cheese

23 July 2021 | Alluris Summer School 2021

The image shows a slide from a quiz. At the top right, it says "EU Trade Mark Quiz". In the top left corner, the number "3" is enclosed in a blue circle. The main content is the word "SWITZERLAND" in a bold, black, sans-serif font. Below the word, the text "'Switzerland' for cheese" is centered. At the bottom, there is a small footer: "23 July 2021 | Alluris Summer School 2021".

4

EU Trade Mark Quiz

4

ALASKA

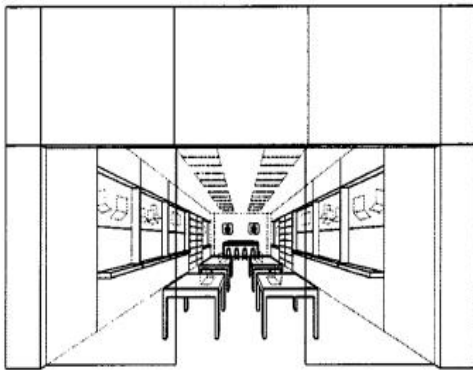
"Alaska" for mineral water

23 July 2021 | Alluris Summer School 2021

5

EU Trade Mark Quiz

5



Apple store

23 July 2021 | Alluris Summer School 2021

6

EU Trade Mark Quiz

6



Tennis ball smelling like freshly cut grass

23 July 2021 | Alluris Summer School 2021

7

EU Trade Mark Quiz

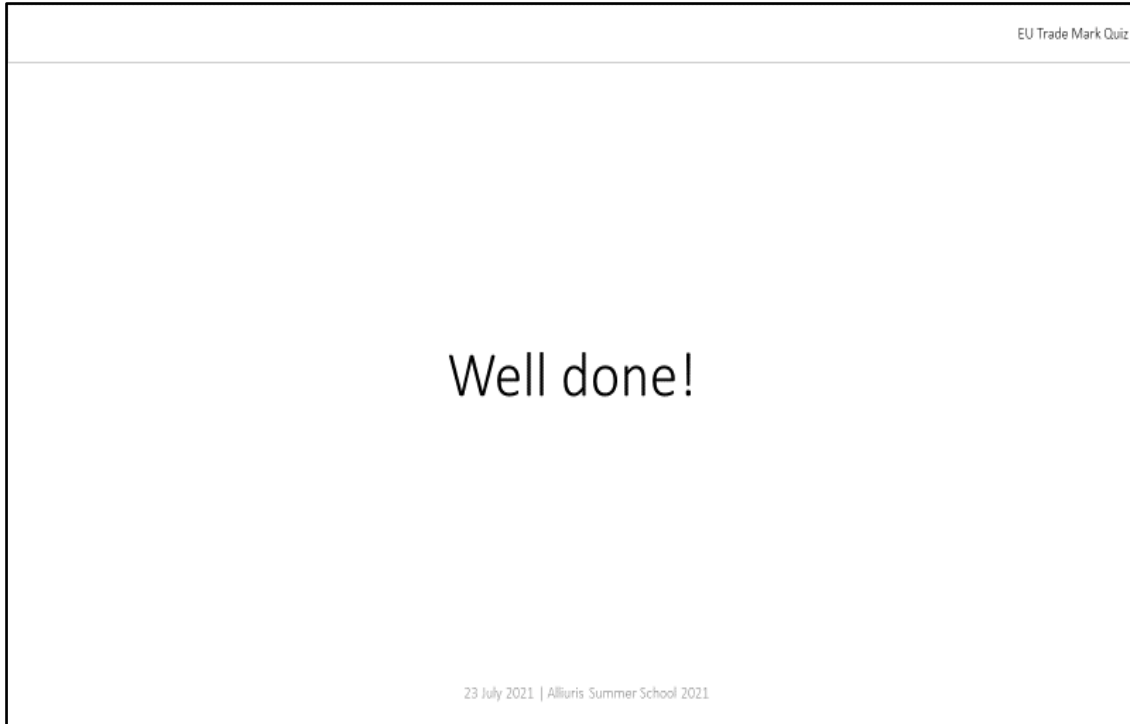
7



"Fucking Hell" for beer from the Austrian village Fucking

23 July 2021 | Alluris Summer School 2021

8



9



Antonia Herfurth
Rechtsanwältin (D) ,

herfurth_antonia@herfurth.de