

alliuris



ALLIURIS ACADEMY | SUMMER SCHOOL 2022

DIGITAL BASICS & LAW

VIRTUAL, 19 - 23 JULY 2022

ORGANISED BY HERFURTH & PARTNER, HANOVER

Alliuris Summer School

18 – 22 July 2022

Digital Economy & Law

Digital policy in Europe & USA, the new sale rules in Europe,
international employment, data protection law, the
new market rules in Europe, international supply chains

**ALLIURIS ACADEMY
SUMMER SCHOOL 2022**

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, Hanover

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

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

Editors & Lecturers:
Antonia Herfurth, LL.M., Rechtsanwältin,
Sara Nesler, LL.M.
Herfurth & Partner, Hanover / Brussels

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 Alliuris Academy was launched in 2006 as a three-pronged effort towards the training of young Alliuris lawyers via summer schools, foreign language training opportunities as well as exchange programmes. This year's Summer School took place from 18 to 22 July 2022. Because of Covid, it was held online for the third year in a row and was hosted by Herfurth & Partner in Hanover, Germany. Professor Dr. Christiane Trüe, who teaches at Bremen University of Applied Sciences, led the Summer School again this year.

This Summer School was a premiere because not only young lawyers from the Alliuris member firms were invited but also students from the University of Göttingen who do their Master in International IP and IT Law had the chance to attend. Alliuris could welcome attendants from i.a. China, Thailand, India, Bulgaria, Turkey, Italy, Spain, Germany, Netherlands, UK and Brazil.

The Academy focused on digital topics as they continue to be the driving factor of law and economy. The lectures were designed in a way that they had high practical use for the young lawyers' work in their firms. Beyond that, the days were shaped very interactively; the speakers had prepared surveys, quizzes and discussion rounds. Everyone enjoyed the interaction and the contributions, which came from so many and diverse countries that they lead to rich discussions.

Even though the social component was once again limited due to the pandemic, the participants had the opportunity to take a virtual tour through the new offices of FDL - Studio Legale Tributario in Milan, Italy, and, as it now became a tradition, to get together for a virtual toast on the last day of the Summer School

Hanover / Milan, July 2022

*Ulrich Herfurth
Chairman of the Board*

*Giuseppe Cattani
Academy Director*

*Prof. Dr. Christiane Trüe
Director Summer School 2022*

Overview

Digital Policy in Europe and USA

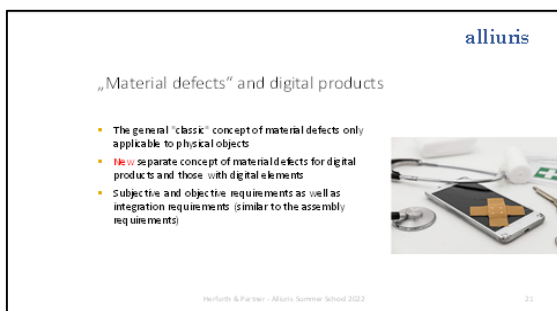


The first day of the Summer School focused on the digital policy in the EU and the USA. Ulrich Herfurth, Sara Nesler and Antonia Herfurth from Herfurth & Partner talked about fair play in digital markets.

In the last years, the European Commission and U.S. institutions such as the Federal Trade Commission have conducted numerous anti-

trust proceedings against the big tech companies – *Google (Alphabet)*, *Amazon*, *Facebook (Meta)*, *Apple* and *Microsoft*. They abuse their power and create an unfair competition on the digital market. Furthermore, the EU and the USA have drafted numerous legal acts to counter the current development. Examples are the EU's Digital Markets Act to control the market power of big platforms which act as gatekeepers, and the U.S.'s Ending Platform Monopolies Act. The speakers have briefly pointed out numerous other countries which have started to counter the current development such as Germany, the UK, South Korea and India.

The new Sales Rules in Europe & International Employment



On January 1, 2022, the Sales of Goods Directive (2019/771) and the Digital Content and Services Directive (2019/770) came into force. Therefore, on the second day, Sara Nesler gave an overview on the most significant changes, based on the German implementation of the Directives. She presented the new definition of "material defect" for tangible goods, digital goods and goods with digital elements. To test

their understanding of a "good with digital elements", the attendants took part in a survey. The survey showed the increasing relevance of the new rules due to the fast development of the Internet of Things. Afterwards, the young lawyers learned about new update obligations for digital goods and goods with digital elements and further changes in the B2C sector, such as information requirements and easier assertion of claims. Finally, Sara explained the main concerns about the novelties in the regulation of supplier recourse and the possibility and limits of a contractual deviation from the statutory provision for tangible and digital goods in the B2B and B2C sectors.

Social Security Law

Onboarding an employee from non-EU member state

- ✓ Territorial principle: Employees are subject to the social security law of the country in which they work.
- ✓ When there is no social security agreement between Germany and the two countries: problem of double insurance.
- ✓ On entry into Germany, (voluntary) health insurance is required
- ✓ With the start of employment, a change to German statutory health insurance is possible

Herfurth & Partner | Alliuris Summer School 2022

For the second part of the day, the floor was passed to Stephanie Reese from Herfurth & Partner. She talked about international employment and issues arising with it. First, Stephanie explained the legal framework and points which especially have to be regulated with international employment relationships, e.g. location of work and working time. She continued highlighting issues to pay attention to, such as tax law and social security law.

Data Protection Law and Europe

The third day was all about data protection. As at least half of the attendants came from non-EU countries, Professor Christiane Trüe started the day by giving an introduction to the General Data Protection Regulation (GDPR). She explained the applicability and presented the definitions provided by Art. 4 GDPR. Christiane Trüe continued by sensitising the young lawyers for conflicting basic rights and interests and legal consequences in case of infringement, that is liability and fines.

SPECIAL CATEGORIES OF DATA

Example of a special category of data

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

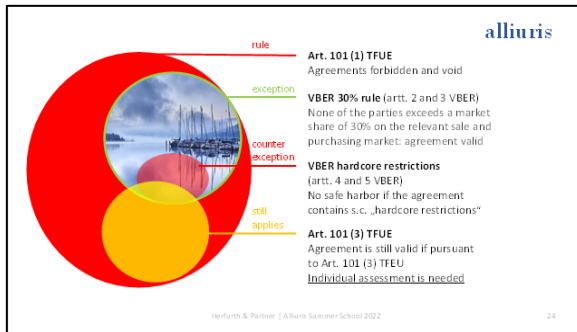
Third country transfer of personal data

Source: <https://www.eugdpr.de/en/eu-privacy-law/>

Herfurth & Partner | Alliuris Summer School 2022

Antonia Herfurth tied in here and presented the new Standard Contractual Clauses (SCCs) by the EU, published on June 4, 2021. SCCs are model contracts which are approved by the European Commission. They apply to the transfer of personal data to a non-EU country for which no adequacy decision exists, so-called *unsafe third countries*. The EU considers e.g. Brazil, China and – still – the USA as such.

The new Market Rules in Europe

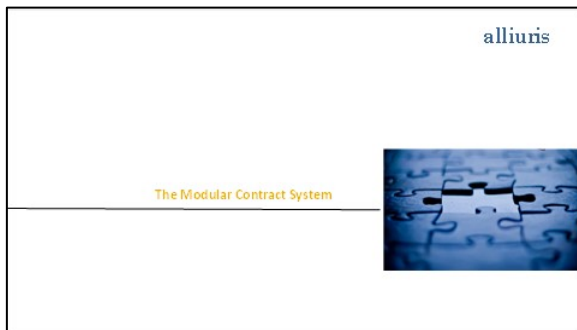


On the fourth day, it was the turn of another recent development in the European legislature: the new Vertical Block Exemption Regulation (VBER).

Ulrich Herfurth started by introducing the general functioning of competition law in the EU, the meaning of the prohibition of restrictive agreements depicted in Art. 101 (1) TFEU and the concept of vertical agreements. He

continued explaining how, in order to increase legal certainty, the European Commission issues block exemption regulations that specify the conditions under which certain types of agreements are exempted from the prohibition laid down in Art. 101 (1) TFEU. After a brief description of the structure of the new VBER, Ulrich Herfurth and Sara Nesler went on to describe the main contents and novelties of the VBER – from dual distribution, parity obligations and dual pricing agreements to exclusive and selective distribution, online sale restrictions and non-compete obligations. At the end of the day, the young lawyers took part in a quiz and discussed some critical points of the VBER.

International Supply Chains



The week ended with the topic “International Supply Chains”.

Ulrich Herfurth gave a detailed overview on the modular contract system used for agreements along the supply chains, such as framework purchasing agreements and framework supply agreements, as well as additional contracts, i.e., quality assurance agreements, warranty agreements, tool

transfer agreements, security agreements and confidentiality agreement. He also explained aspects of product liability and insurance conditions.



The second part of the day focused on current issues in the international supply chains, such as the Covid pandemic as an event of force majeure, the ongoing price increases, new rules regarding supplier recourse and recent developments in compliance requirements.

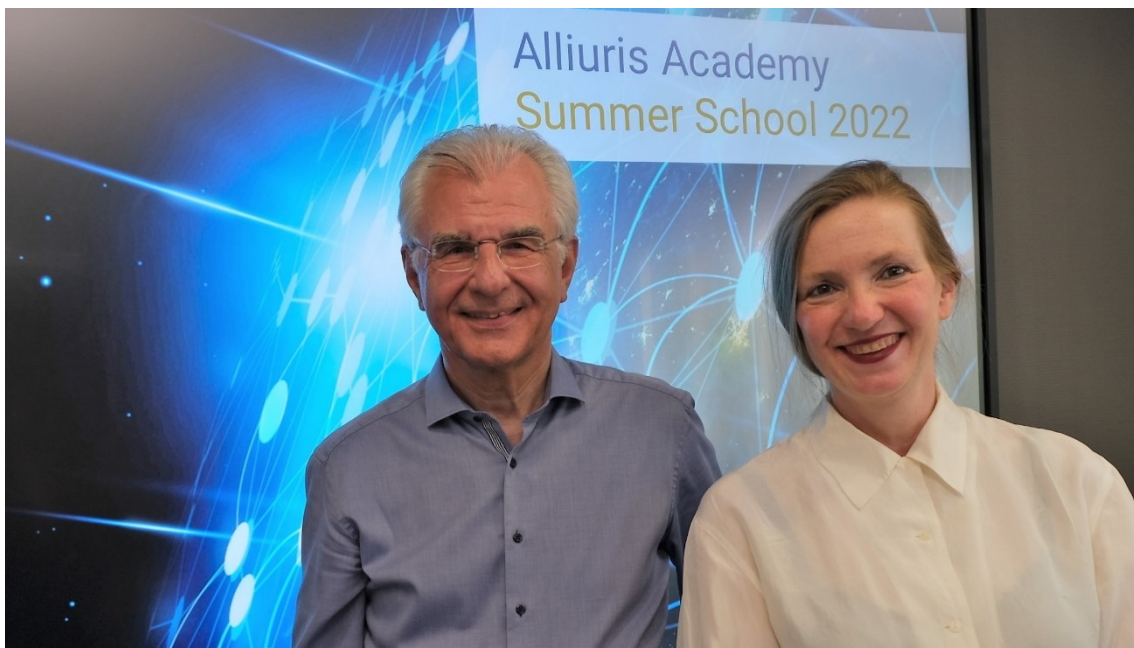


ALLIURIS ACADEMY

SUMMER SCHOOL 2022
18 - 22 JULY 2022

ORGANISED BY
HERFURTH & PARTNER, HANOVER

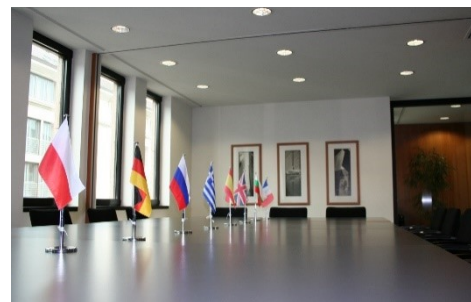
VIRTUAL

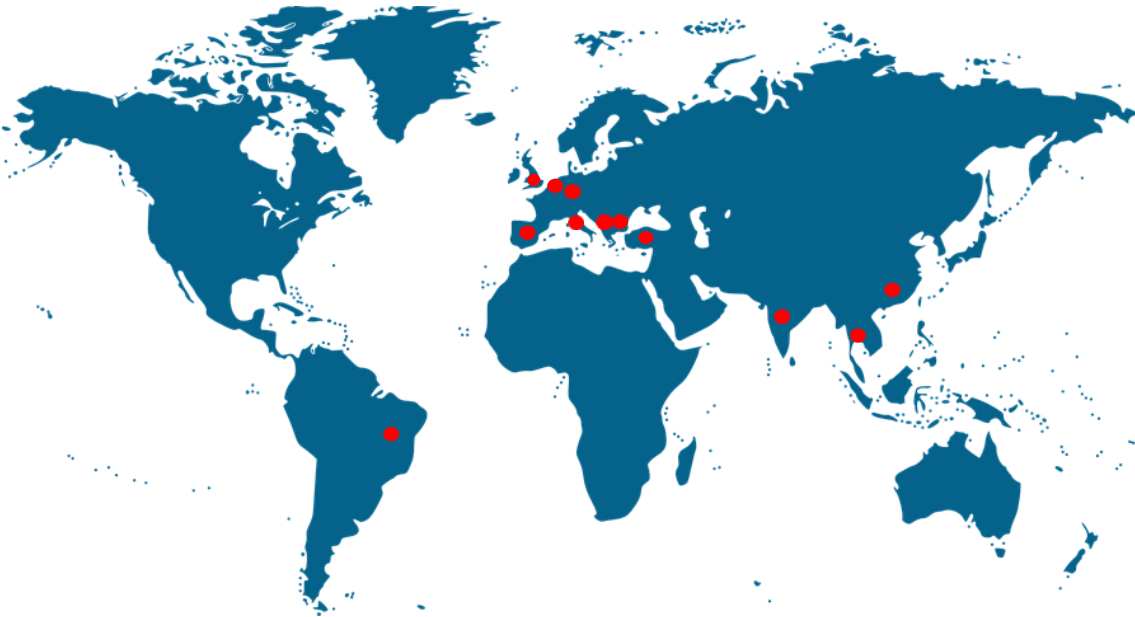




The speakers and organisers of the Summer School 2022

Herfurth & Partner in Hanover organised the Conference





Young lawyers from Brazil, China, India, Thailand, UK, Bulgaria, Kosovo, Turkey, Italy, Spain, Germany and the Netherlands participated in the Summer School





Some of the participants of
the Summer School



Reactions of the attendants

The virtual Alliuris Academy was much liked by the young lawyers:

"I think that Digital Policy in Europe and USA is a good topic of choice and a very interesting one. I like the idea that the focus of the summer school is at applicable law."

- Aurora Mullatahiri, Kosovo -

"The presentations on Digital Policy in Europe and USA were very interesting and useful! Thank you!"

- Sophia Yordanova, Bulgaria -

"Thank you all for your preparation. I am quite interested in the international labour law and company laws and learned a lot from today's session. I also learned a lot from the session on the new Market Rules in Europe. It's difficult for a country outside the EU to understand but it's quite interesting. I love the questions and discussions because it's very useful for understanding and all the friends and teachers are very nice. Thank you."

- Zhengmin (Corrine) Wu, China -

"It was very nice to meet you all and I hope we can meet in person someday. Thanks for all the effort and well organised presentations."

- Judith Guillén Cantero, Spain -

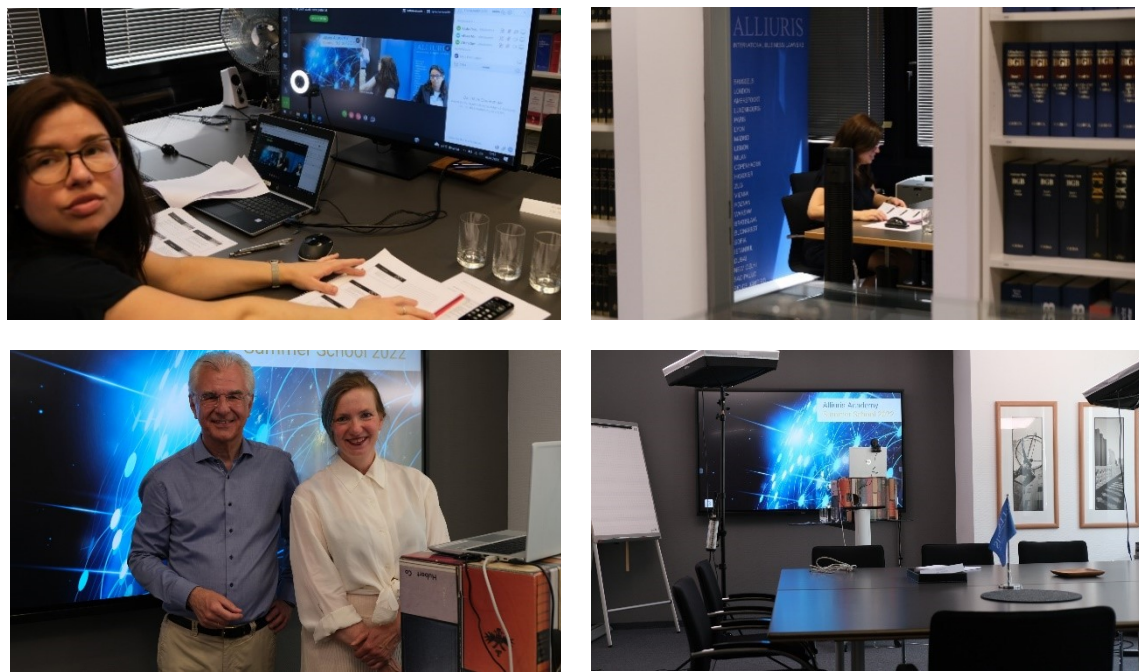
"Thank you and hope to see you in person in the future."

- Shuangying (Helen) Yu, China -

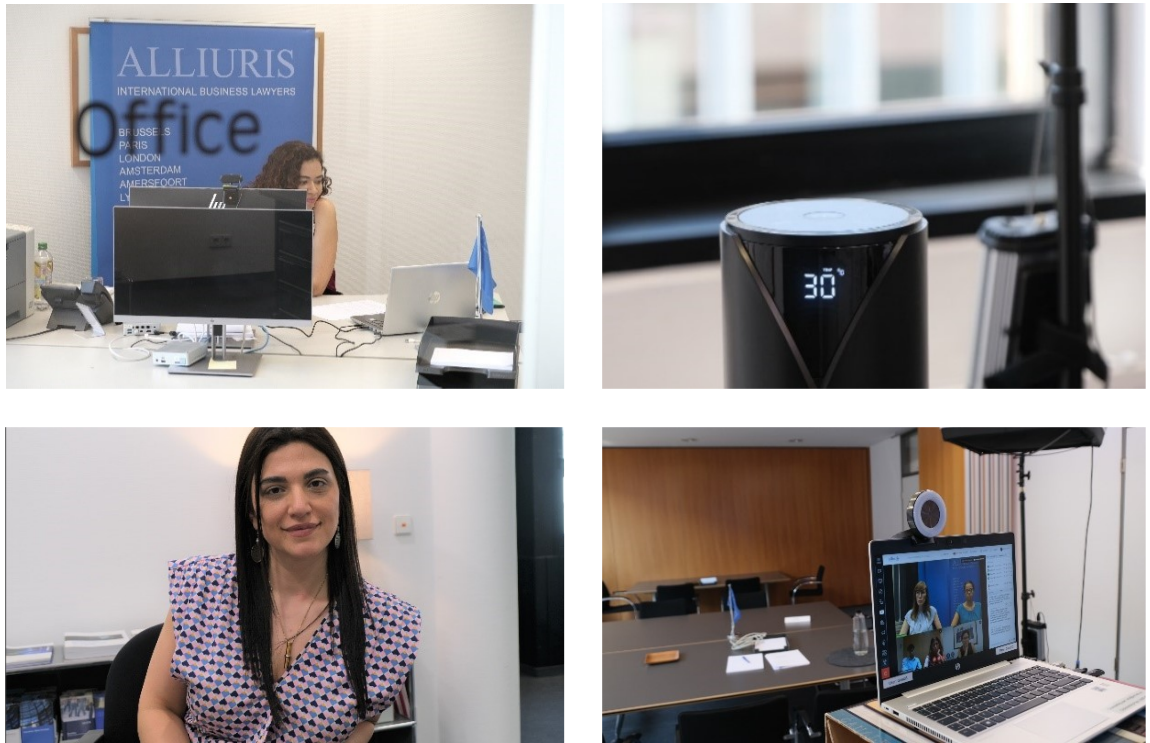
"Thank for the great week and the well prepared speeches."

- Antje Katharina Liedtke, Germany -





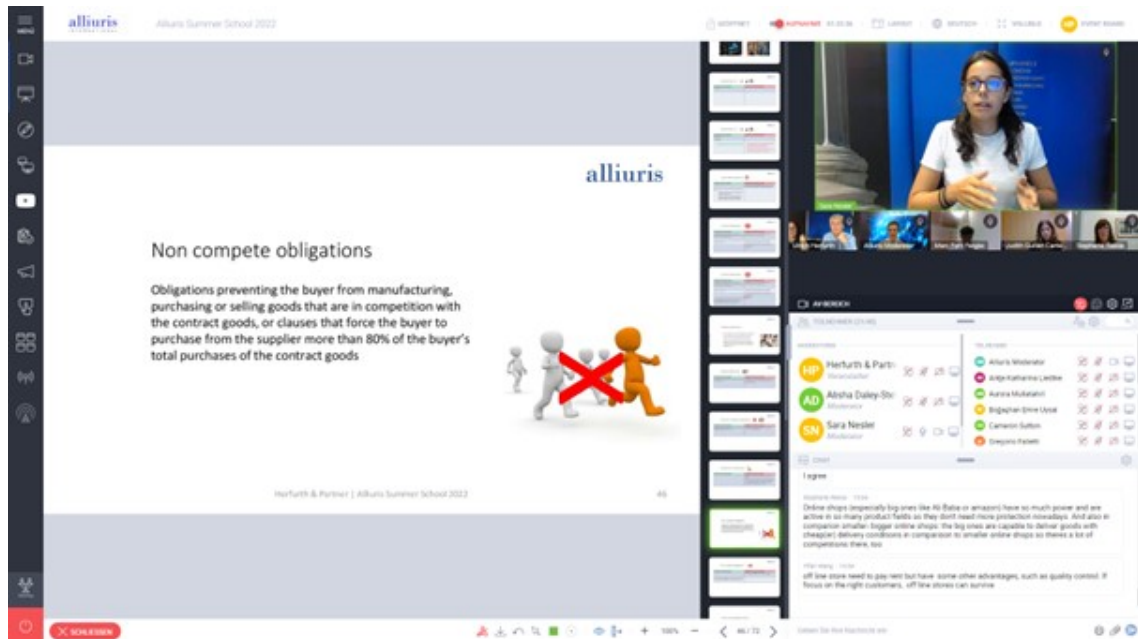
Behind the scenes of the Summer School





The team at work

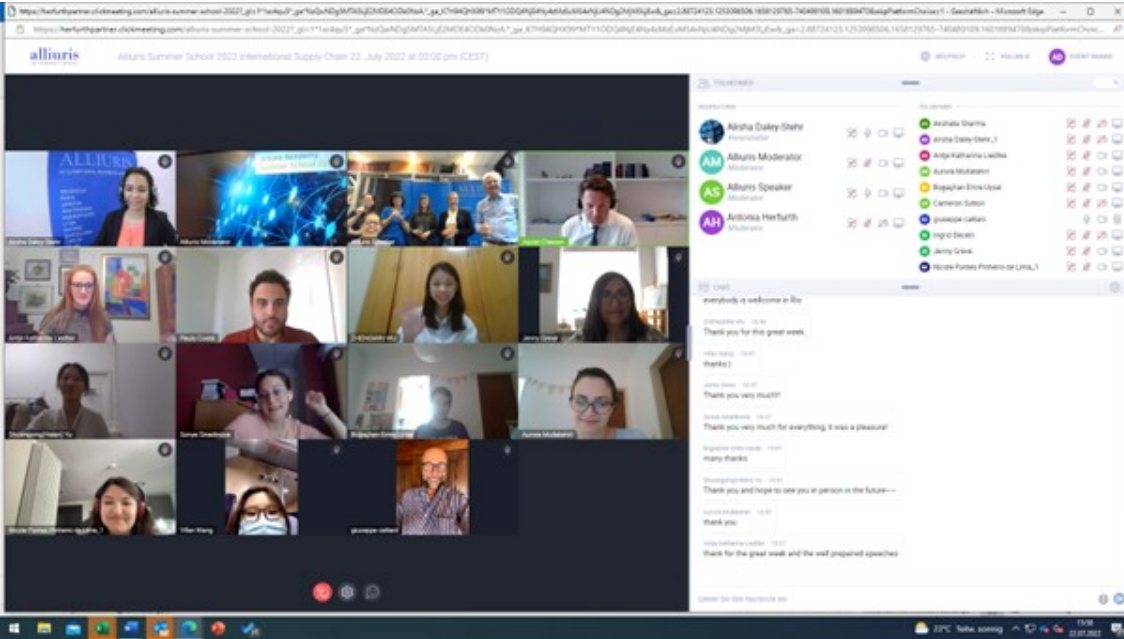




Focus on the presentations

Afterwards: time for an ice cream





Virtual Toast at the end of the Summer School

And our real one



Report

Contents

	<i>page</i>
I. Chapter One – Digital Policy in Europe and USA	19
1. Presentation	20
<i>(Ulrich Herfurth, Antonia Herfurth, Sara Nesler Herfurth & Partner)</i>	
2. Materials	46
2.1. The EU Digital Services Act	46
Compact, August 2021 <i>(Antonia Herfurth & Sara Nesler Herfurth & Partner)</i>	
2.2. The EU Digital Markets Act	51
Compact, December 2020 <i>(Ulrich Herfurth Herfurth & Partner)</i>	
2.3. Trading Platforms and Competition	56
Compact, April 2021 <i>(Sara Nesler Herfurth & Partner)</i>	
2.4. The European Data Act	61
Compact, April 2022 <i>(Antonia Herfurth Herfurth & Partner)</i>	
2.5. The Data Governance Act and the Data Act of the EU	65
Compact, December 2021 <i>(Sara Nesler Herfurth & Partner)</i>	
2.6. Artificial intelligence in Europe	70
Compact, September 2021 <i>(Ulrich Herfurth & Sara Nesler Herfurth & Partner)</i>	
II. Chapter Two – The New Sales Rules in Europe	75
1. Presentation	76
<i>(Sara Nesler Herfurth & Partner)</i>	
2. Materials	106
2.1. The new law on the sale of goods	106
Compact, January 2022 <i>(Aline-Kristin Pehle Herfurth & Partner)</i>	

III.	Chapter Three – International Employment	113
1.	Presentation <i>(Stephanie Reese Herfurth & Partner)</i>	114
2.	Materials	122
2.1.	Onboarding - bringing foreign employees on board Compact, April 2022 <i>(Stephanie Reese Herfurth & Partner)</i>	122
IV.	Chapter Four – The General Data Protection Regulation	127
1.	Presentation <i>(Prof. Dr. Christiane Trüe Herfurth & Partner)</i>	128
V.	Chapter Five – Data Protection and international business: Standard Contractual Clauses for trade with third countries	147
1.	Presentation <i>(Antonia Herfurth Herfurth & Partner)</i>	148
2.	Materials	178
2.1.	The new Standard Contractual Clauses of the EU Compact, May 2022 <i>(Antonia Herfurth Herfurth & Partner)</i>	178

VI.	Chapter Six – The new EU Regulation on competition restrictions in vertical markets (VBER)	183
1.	Presentation <i>(Ulrich Herfurth, Sara Nesler Herfurth & Partner)</i>	184
2.	Materials	220
2.1	Restrictions on Competition in Distribution <i>Compact, October 2022 (Ulrich Herfurth & Sara Nesler Herfurth & Partner)</i>	220
VII.	Chapter Seven – Quality and Security in the Supply Chain	225
1.	Presentation <i>(Ulrich Herfurth Herfurth & Partner)</i>	226
VIII	Chapter Eight – Supply Chain Problems	247
1.	Presentation <i>(Ulrich Herfurth, Sara Nesler Herfurth & Partner)</i>	248
2.	Materials	264
2.1	Contractual disruptions and Russia <i>Compact, April 2022 (Ulrich Herfurth & Aline-Kristin Pehle Herfurth & Partner)</i>	264
2.2	The EU's Sanctions against Russia <i>Compact, March 2022 (Steffen Töhte Herfurth & Partner)</i>	269
2.3	Business related sanctions in Russia <i>Compact, April 2022 (Thomas Brand Brand & Partner)</i>	274
2.4	The EU Approach to Supply Chains <i>Compact, February 2022 (Steffen Töhte Herfurth & Partner)</i>	279

Chapter One

Digital Policy in Europe and USA

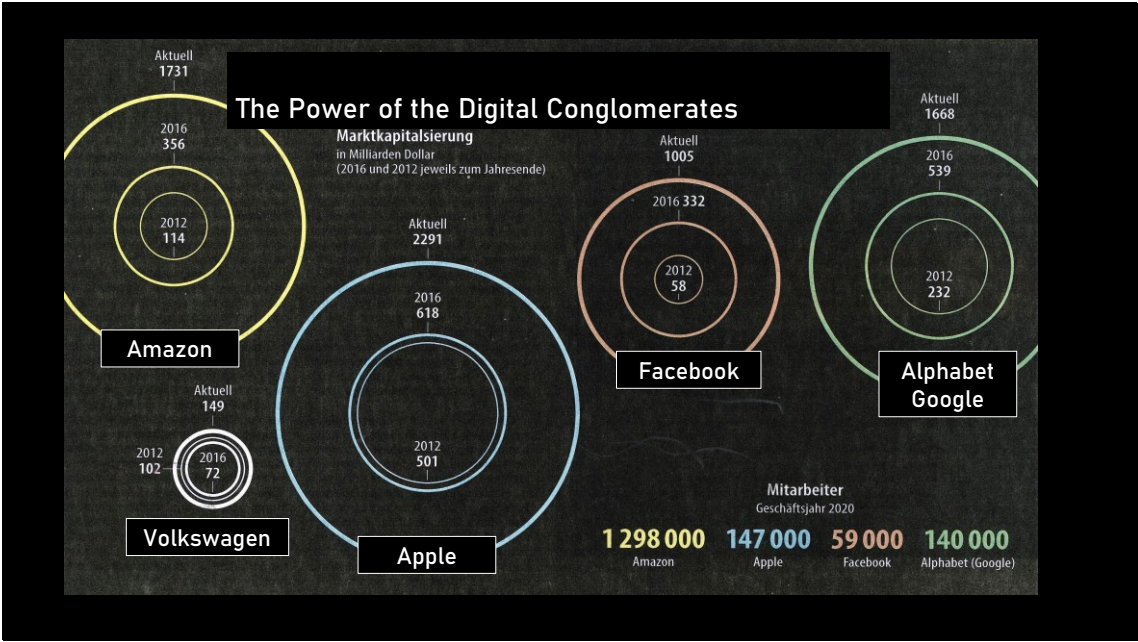
DIGITAL MARKETS

1

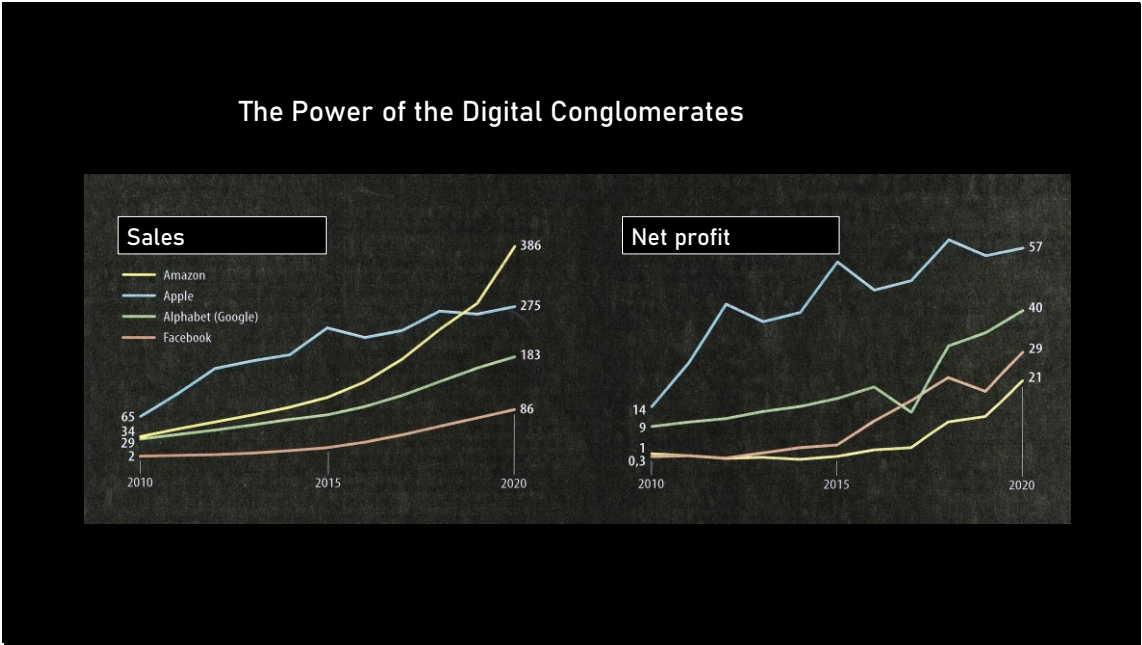
FAIR PLAY IN DIGITAL MARKETS

ALLIURIS SUMMER SCHOOL | JULY 2022

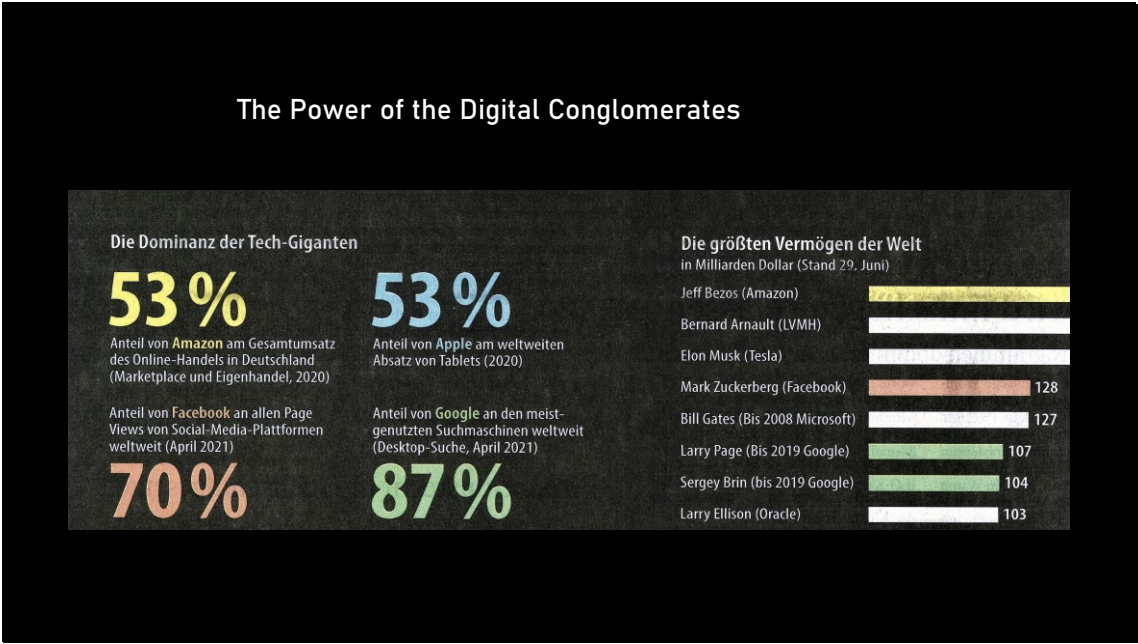
2



3



4



5



6

The Power of Law.



Lisa Khan | US Federal Trade Commission

7

The Power of Law.



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

8

The Power of Law.



European Commission vs GAFAM

- Google, price comparison system EGC confirmed fine of € 2,42 billion. Appeal ECJ
- Google, Android system Fine of € 4,3 billion, appeal EGC
- Google, AdSense advertising Fine of € 1,49 billion
- Apple, music streaming Pending
- Apple, E-Books, audiobooks Pending
- Apple, Apple Pay Pending
- Amazon, Buy Box Pending
- Amazon, Marketplace Pending
- Google & Meta (Facebook), online display advertising New, 2022
- Facebook, Marketplace New, 2022

...

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.



European Commission vs GAFAM

Amazon, Marketplace, pending

- Amazon is both a platform operator and a merchant
- Collection of data on the activity of the merchants. This data may be used to affect competition
- Possibly also plays a role in the selection of the „Buy Box“ merchant
- Investigation by the German Federal Cartel Office, terms and conditions changed
- The BKA's and the EU Commission's main concerns are likely to be covered for the most part by the new Digital Markets Act

11

The Power of Law.



European Commission vs GAFAM

Google & Meta (Facebook), online display advertising New, 2022

Google provides intermediation services between advertisers and publishers by real time auctioning of online display advertising space	Meta, through its 'Meta Audience Network', participates in auctions for third party publishers' advertising space using Google's and rivals' advertising technology services.
--	---

“Jedi Blue” agreement: allegedly gave Facebook an illegal advantage in Google's ad auctions in exchange for Facebook's word that it would end its own ad service plans

12

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 Services Act | draft act
- Data Governance Act | draft act
- Data Act | draft act
- White Paper on AI | published
- AI Regulation | draft act
- Fairness & Transparency Regulation | in force

13

The Power of Law.



Digital Market Policy of the EU

- E-Commerce Regulation | in force
- E-Privacy Regulation | draft act
- Algorithms
- Software Product Liability | proposal
- Chips Act | proposal
- Adapting liability rules to the Digital Age and AI | initiative

14

The Power of Law.



Digital Market Policy of the EU

- **General Data Protection Regulation (GDPR)**
in force, had to be implemented until May 2018, market principle:
applicable to any controller or processor who is active in the EU territory,
processing of personal data prohibited except for specific reasons, inter alia (Art. 6 para. 1 GDPR):
 - fulfilment of legal / contractual obligations
 - written consent of the individual
 - specific interest of the controller, prevailing interest of the individual

15

The Power of Law.



Digital Market Policy of the EU

EU Copyright Directive
in force and had 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

16

The Power of Law.



Digital Market Policy of the EU

Digital Markets Act
draft act of January 2021, Council and Parliament reached agreement on draft in March 2022; 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)

17

The Power of Law.



Digital Market Policy of the EU

Digital Services 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

18

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

19

The Power of Law.



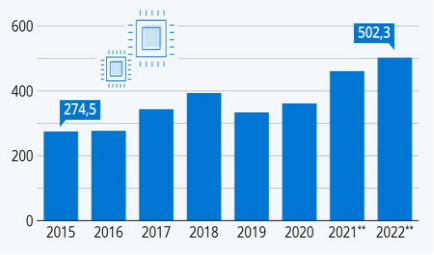
Digital Market Policy of the EU

Data Act
draft act of February 2022, intended to ensuring fairness in the allocation of data value among actors of the data economy

- main idea is to break up data monopolies by giving rights and more control to data creators (users of a product or service) and by increasing the sharing of data
- however, avoids topic of whether original right in data exists and who is entitled to it (data ownership)

20

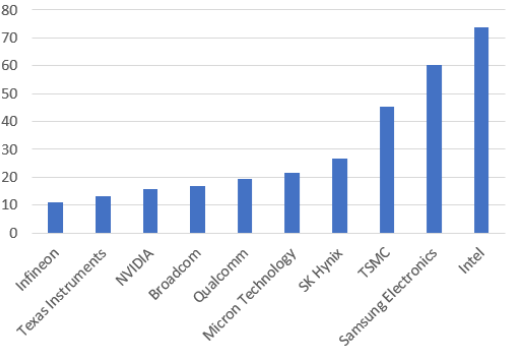
Worldwide Sales of Microchips / Semiconductors ,
in USD, 2022 estimated



21

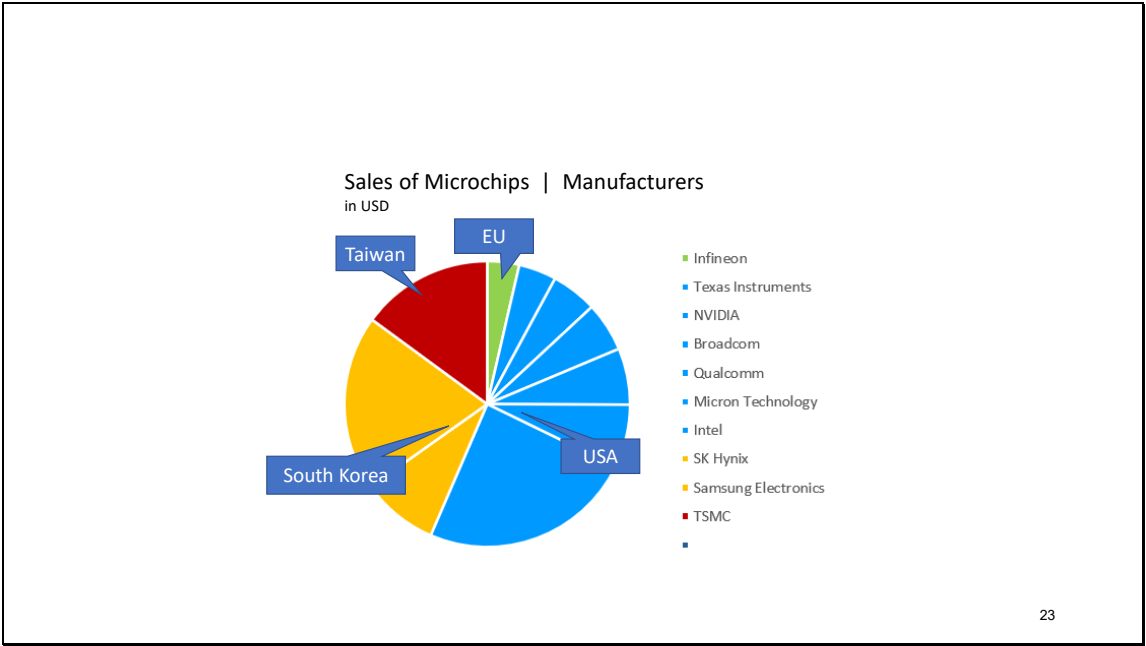
21

Sales of Microchips | Manufacturers
in USD



22

22



23

The Power of Law.




Digital Market Policy of the EU

Chips Act
proposal, first introduced in September 2021, intended to address semiconductor shortages and strengthen Europe's technological leadership

- main aims are to push innovation capacity of state-of-the-art chips, to combat skills shortage and to attract and train skilled workforce, and to gain comprehensive understanding of global semiconductor supply chains

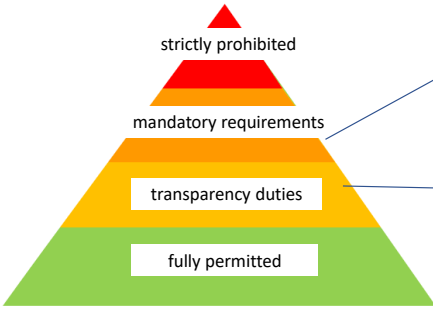
24

The Power of Law.



Digital Market Policy of the EU

Artificial Intelligence



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

25

The Power of Law.



Digital Market Policy of the EU

Adapting liability rules to the Digital Age and AI

initiative, first introduced in June 2021, intends to modernise liability rules and reduce obstacles to get compensation for damage

- Product Liability Directive from 1985, today, security of many products and services depends on digital content (e.g. software updates)
- Questions: Can digital, intangible products be classified “products”?
 New technologies bring new risks – are cyber vulnerabilities covered?
 Who is responsible if complex digital technologies are defect?

26

The Power of Law.



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

27

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

28

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

29

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

30

The Power of Law.



Federal Cartel Office vs GAFAM

Procedures under section 19a GWB
In 2021, the Federal Cartel Office has 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.

As per Mai 2022, the Federal Cartel Office has concluded the first step of the procedures against Alphabet (Google) and Meta (Facebook) affirming their cross market importance under section

31

The Power of Law.



- Antitrust vs GAFAM
- Digital Market Policy of the USA

32

The Power of Law.



Antitrust vs GAFAM

- Antitrust Division vs Alphabet (Google)
- Up to 38 State Attorneys General vs Google
- Federal Trade Commission and 48 States vs Facebook
- Epic Games vs Apple
- Epic Games vs Google
- District of Columbia vs Amazon

33

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.

34

The Power of Law.



Antitrust vs GAFAM

Alphabet (Google)


16.12.2020 10 SAGs: monopolizing online advertising

17.12.2020 38 SAGs: monopolizing search

07.07.2021 38 SAGs: monopolizing mobile app distribution and in-app payment

35

The Power of Law.



Antitrust vs GAFAM

Facebook

Facebook is accused by the FTC and 48 US states of buying up competitors, especially WhatsApp and Instagram, in order to avoid competition in the social media industry. The FTC's antitrust lawsuit aims to force Facebook to reverse these two major acquisitions.

FTC refiled its lawsuit after a judge dismissed an earlier version in June 2021, the 48 states are appealing

36

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.

Ruling in September 2021 mostly in favor of Apple, Epic Games appealed supported by 35 states and Microsoft.

37

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.

38

The Power of Law.



Digital Market Policy of the USA

- CLOUD Act
- 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)

39

The Power of Law.



Digital Market Policy of the USA

CLOUD Act
enacted in March 2018

Allows U.S. authorities to access (personal) data held by U.S.-based data and communication companies on any server they own. Data must be critical for investigations of serious crime.

Controversial, invasion of privacy and restriction of fundamental rights.

40

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 that:

- Use 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. (e.g., Fulfillment by Amazon + Amazon prime model)

41

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.

42

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.

43

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.

44

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.

45


The Power of Law.



- Worldwide procedures VS GAFAM

46

The Power of Law.



Competition and Markets Authority vs GAFAM


Apple
Ongoing investigation, monopolization of mobile app distribution

Facebook
The CMA ordered Facebook to sell Giphy, an online database and search machine for GIF files. Facebook is appealing

Ongoing investigations (Facebook Marketplace, Facebook Dating)

47

The Power of Law.




Korea Fair Trade Commission vs GAFAM

In September 2021, Google was fined \$177 million for monopolization of mobile operating systems. Google is appealing.

48

The Power of Law.



Competition Commission of India vs GAFAM

Investigation vs. Google, monopolization of mobile operation systems
Started in April 2019, it has been concluded in Sept. 2021. A final ruling is awaited

Investigation vs Google , monopolization of mobile payments
Started in November 2020, ongoing

49

The Power of Law.

What about your country?



50

Thank you for listening to

FAIR PLAY IN DIGITAL MARKETS

by
Sara Nesler
Antonia Herfurth
Ulrich Herfurth
www.herfurth.de



ALLIURIS SUMMER SCHOOL | JULY 2022

51

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 its 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.

+ + +

The European Data Act

Antonia Herfurth, attorney at law in Hanover and Munich

April 2022

On February 23, 2022, the European Commission published the draft legislation for the Data Act. Together with the Data Governance Act, the Data Act forms a legislative package under the European Data Strategy. So far, only personal data has been in the focus of discussions, non-personal data is hardly regulated in the EU. The two new draft laws now regulate personal and non-personal data. Special about the Data Act is that it gives individuals and companies control over the non-personal data they generate.

Aim of the Data Act

Data are one of the most important economic goods of our time. In the absence of existing regulations for non-personal data, there is a lot of confusion about when data is generated, what data are generated and who holds the generated data. In addition, existing data are in the hands of a few powerful companies. Such concentration leads to a market imbalance that restricts competition and hinders data access and use by third parties.

The aim of the Data Act is to ensure a fair distribution of data value among the players in the data economy. To this end, it prescribes fair access and use of data, as well as data portability and interoperability between different service providers. In this way, data monopolies and lock-in effects are to be dissolved. Users should have more control over the data they generate, and the public sector should have access to data needed to address political and societal challenges, such as the Corona pandemic.

Data users and data holders

The Data Act defines a “user” as a natural or legal person who owns, rents or leases a product or uses a service. The status of “data user” is linked to the contractual relationship with the device. “Data holder” is the legal or natural person who is legally entitled or obliged to provide certain data, or in the case of non-personal data and through control of the technical design of the product and related services, is able to do so. Phrased simply: The data holder is the one who has de facto technical control over the data.

The Data Act thus assumes that data is not in the hands of the user, i.e. in the hands of the data generator, but in the hands of the data-processing company.

Data access and data use

For this reason, the draft law creates a right to data access and use in favour of data-generating users.

Products and services should be designed in such a way that users have access to the data they generate, easily, securely and, where necessary and appropriate, directly. If the user does not have direct access, the data holder must grant him access on request without delay, free of charge and, if necessary, continuously and in real time.

In addition, the Data Act provides for information obligations towards the user before the user buys, rents or leases the data-generating product or service. For example, the user must be informed about:

- the nature and extent of the data generated by the product,
- whether data is generated continuously and in real time,
- how the user can access the data,
- whether the manufacturer or service provider intends to use the data itself or to allow a third party to do so, and if so, for what purposes,
- the identity and contact details of the data holder.

At the request of the data user, the data holder must share his data with third parties. These so-called data recipients may only process the data for the purposes and under the conditions agreed with the user. Data must be deleted when it is no longer needed for the agreed purpose. If the data holder is obliged to make data available to a data recipient, he must do so under fair, reasonable and non-discriminatory conditions and in a transparent manner. Any remuneration must be reasonable. If the data holder and the data recipient cannot agree on a fair data use contract, the Data Act provides for dispute resolution bodies.

The right to data access shall not be enforced against small and micro enterprises.

Prohibition of unfair contractual terms

The Data Act stipulates that unfair terms in data use agreements that are unilaterally imposed on a medium, small or micro enterprise are not binding on them. Such clauses are usually not the result of balanced contractual negotiations, but the consequence of take-it-or-leave-it situations. In Article 13 of the Data Act, the EU has introduced an *unfairness test*. According to this, a contractual term is unfair if it deviates grossly from good commercial practice and is thus contrary to good faith and morality. This general rule is supplemented by a list of terms which are always unfair and a list of terms which are presumed to be unfair, i.e. which are deemed to be unfair. In addition, the European Commission is to develop non-binding model contract clauses which the parties can use, similar to the standard contractual clauses under the General Data Protection Regulation.

Data portability

It is common for providers of data processing services to hinder customers from switching to a competing service provider by, for example, imposing long notice periods or making data portability difficult. By making the switch as cumbersome as possible, customers are tied to the existing provider, so-called lock-in effect. The Data Act provides that customers can switch from one data processing service to another data processing service covering the same type of service without being hindered by commercial, technical, contractual and organisational measures.

The rights of the customer must be specified in a written contract. As a minimum, the contract must state that the customer has the right to change provider within 30 days. The provider must support the customer in switching and continue to provide unrestricted services. The provider must also provide a full specification of all data that will be exported during the switching process. This includes all data imported by the customer at the beginning of the service contract and all data generated by the customer and by the use of the service during the contract period. This includes, in particular, security settings, access rights and access logs to the service. If the service provider states that a change within 30 days is technically not possible, he must inform the customer within seven days. The provider bears the burden of proof. The switch must be completed within six months of the customer's request at the latest.

The service provider may not charge the user for the change. This applies after a transitional period of three years after the Data Act comes into force.

Interoperability

In addition, the Data Act lays down basic interoperability requirements for operators of data rooms and providers of data processing services. Here, the draft law refers in particular to cloud

computing and edge computing providers. Uniform standards will enable data to be exchanged more effectively and mechanisms for data sharing to work better together. The Data Act also sets out basic requirements for smart contracts. These help the contracting parties to guarantee that the agreed data use conditions are adhered to.

For cloud and edge computing providers, the rules of data portability also apply; in particular, a change of service provider must be possible within 30 days and must not be artificially impeded by legacy providers.

Data access due to exceptional circumstances

Data holders must make data available to the public sector due to exceptional circumstances. Exceptional circumstances are, for example, public emergencies or if the lack of data prevents a public institution from fulfilling a task in the public interest and the data cannot be obtained in any other way. If the data holder has incurred technical or organisational costs as a result of the provision of the data, these costs shall be reimbursable.

The public institution may use the data only for the purpose stated by it. If the data is personal data, it must take technical and organisational measures to protect the data subject and destroy the data as soon as it is no longer necessary for the fulfilment of the purpose. In the case of trade secrets, the public institution should only request them as a last resort and only to a limited extent. In doing so, it must take reasonable measures to ensure the confidentiality of the trade secret.

The right to access data should not be asserted against data holders who are small or micro enterprises.

Safeguards for non-personal data in international contexts

Data processing services shall not disclose or provide access to non-personal data to third countries if this would create a conflict with Union law or the national law of the Member State concerned. If the request is based on the decision of a court or an authority and on an international treaty, the decision shall be recognised and enforced. If it is not based on an international treaty, the request should only be complied with in exceptional cases, for example for the purposes of criminal prosecution.

Conclusion

With the Data Act, the European legislator has introduced a further measure that weakens the de facto control of monopolistic data holders and strengthens the position of data-generating

users. The regulatory measures of recent years show that the EU wants to break up the current one-sided structures of the data market and thus create opportunities for innovation and competition in the data economy. In the context of rights in data, there have been discussions about the introduction of data ownership, which the EU has not followed up on in the Data Act. Rather, a shift towards data sharing seems to be taking place, i.e. the EU is more concerned with data sovereignty.

It remains to be seen how the Data Act will develop and establish itself in practice. For example, there are no rules on how to deal with overlapping rights to use data. It is conceivable that everyone should be able to use the data they need to fulfil their services, for example, a garage should be able to use the data it needs to repair a vehicle.

The Data Act will presumably not come into force before 2023.

+ + +

The Data Governance Act and the Data Act of the EU

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

December 2021

The exchange and use of data are of great importance for the competitiveness of European companies and for a smooth administration. The EU Commission has recognized this and has presented its Data Strategy on February 19, 2020. In doing so, it hopes to combine efficient data access with an effective competition policy and a high level of data protection. The Data Governance Act and the Data Act form the regulatory pillar of the European Data Strategy and could bring significant benefits but also new challenges for companies and citizens.

Data Governance Act

The draft regulation on data governance (Data Governance Act) was already published by the EU Commission in November 2020. It aims to promote the availability of data for use by strengthening data sharing mechanisms across the EU and improving trust in data intermediaries. To do this, it focuses mainly on three measures.

Making public sector data available

Data held by the public sector will be made increasingly accessible. To achieve this, agreements that restrict the reuse of data held by public sector bodies will be prohibited, even beyond the "Open Data" Directive. This includes, for example, data that is protected because of the intellectual property rights of third parties or because of its sensitivity. An exception is provided for, among others, when such an agreement is necessary for the provision of a service or product in the general interest.

The competent public sector bodies designated by the Member States must make the conditions for the re-use of the data publicly available. They may also impose obligations, such as that only processed data may be used (through anonymization, pseudonymization, and deletion of confidential information), or that the reuse must take place in a controlled processing environment. Fees may be charged for permission to reuse this data.

Data sharing services

In order to increase trust in the data intermediaries, in the future, the provision of certain data sharing services will be subject to notification. The new regulation also imposes a series of

requirements on providers regarding their own use of data, the access process, the interoperability of data, and the prevention of abusive and unlawful behavior.

Those providing services to data subjects must act in their best interests under the Data Governance Act and facilitate the exercise of their rights under the GDPR. In particular, they must provide advice on the possible types of data use and customary terms and on the conditions for such uses.

The competent authorities will supervise and enforce compliance with these rules. For this purpose, they will be able to impose fines and penalty payments and/or order the suspension of the data sharing service.

Data altruism

New regulations are also foreseen for data altruistic organizations. These are organizations established for the pursuit of general interest and perform data altruistic activity through a structure which is legally independent and separate from other activities. Recognized data altruistic organizations subject to special transparency requirements will be entered in a register attesting to their credibility.

Other measures

The draft also provides for the establishment of a Data Innovation Council in the form of a group of experts to advise and assist the EU Commission. In addition, to reduce the risk of data leakage, access by foreign courts and authorities to the data collected will be restricted.

Criticisms

The draft has been well received for the most part. Nevertheless, there has been criticism that it lacks a clear systematic demarcation from other regulations, in particular the General Data

Protection Regulation, the planned ePrivacy Regulation and the Directive on the Protection of Business Secrets. Concerns were also expressed about the bureaucratic burden.

Outlook

The EU Commission announced on November 30, 2021 that the EU Parliament and Council had reached political agreement on the proposed Data Governance Act. The regulation now needs final approval from the EU Parliament and Council. Businesses and citizens interested in using the data made available, as well as affected service providers and organizations, should prepare accordingly.

Data Act

The second measure presented by the EU Commission as part of its communication on data strategy in 2020 is called “Data Act” and appears somewhat more controversial. It is intended to promote the exchange of data by and between companies in order to advance the development of the EU data economy. A first draft of the regulation is expected soon. Nevertheless, it is already partly foreseeable in which direction the Commission's proposals will go. It can be gleaned from the impact assessment published by the Commission on 28/05/2021 and from the results of the public consultation conducted from June 3 to September 3, 2021.

Several problem areas have been identified that inhibit or prevent data sharing between and by companies. These include general factors such as the lack of fairness in digital markets or low legal certainty, but also more specific issues such as the lack of portability when using cloud services and the need for harmonized standards for smart contracts.

To address these issues, different measures could be introduced. They play out in both B2G and B2B relationships.

Data sharing B2B

- Data access plays a major role in the digital economy. For startups and small companies it is often difficult to gain it, due to their weak bargaining power. This creates an imbalance in the market and prevents innovation. The Commission therefore proposes to introduce data access and usage rights. Unfair contract terms are to be prevented by a fairness test.

Part of the business community has objected that the exchange of data can also lead to a restriction of competition, especially if it includes sensitive, competition-relevant

information. For this reason, the exchange of data should take place on a voluntary basis. Only where a market distortion has been identified should access be regulated on a sector-specific basis. In order to make it easier to ensure data protection, guidance for companies should also be made available.

- Access to machine-generated data is to be expanded. This could require a reform of the database directive.
- The market for cloud computing services is also to become more competitive. Organizations and companies are increasingly dependent on cloud services for processing data, and these
- services often already have a great deal of market power. In order to avoid lock-in effects, portability between cloud services shall be secured by a portability right.

In its statement on the Data Act, the DIHK (Association of German Chambers of Commerce and Industry) called for the negotiating position of cloud users to be strengthened by standard contractual clauses. This requires that the right to data portability is extended to the commercial users of cloud services. Currently, this is only incompletely regulated in Article 20 of the GDPR, and the technical implementation of the transfer has not yet been standardized. The Data Act is intended to concretize the general right to data portability. For example, the Commission is considering obliging providers of smart devices to enable real-time data transfer via interfaces. This is also intended to promote competition.

Data sharing B2G

The public sector could benefit from the use of data processed by private companies. However, access is limited, partly because of the lack of clarity in the legal framework, and partly because companies have no incentive to share their data with the state.

The Data Act aims to introduce mandatory data sharing for certain public interest purposes. In addition, the agreement on rights of use and their remuneration shall be facilitated by requirements for data sharing and transparency, through protective measures and through the creation of intermediary structures.

In the interest of companies, a clear demarcation between the mandatory and voluntary transfer of data, which is to be preferred for them, would be desirable. An appropriate incentive system (for example, through tax advantages) should take into account the costs of data transfer and the increased risk of disclosing trade secrets. Strict protection of confidential business

information and transparency regarding the use of the data could also increase the trust and willingness of companies.

Smart contracts

"Smart contracts," are automated binding agreements written in codes and blockchains. They could play an important role in facilitating the agreement on rights of use in both B2G and B2B relationships. However, the EU currently lacks harmonized standards for these types of contracts, making international use difficult even within the EU. The Data Act is intended to provide the necessary regulatory framework and technical standards.

International data protection

The problem of international data protection also arises in the context of the Data Act. One particular issue is the international handling of non-personal data (for example, at the request of foreign authorities), which has not been regulated to date. One solution could be to oblige service providers to inform users of such a request and not to grant it if it is prohibited under EU law or the law of the Member States.

Outlook

Only the draft legislation will be able to better clarify what specific benefits and challenges will arise from the Data Act and allow for preparation. Its publication was originally planned for the end of 2021 and is expected shortly.

+ + +

Artificial intelligence in Europe

Ulrich Herfurth, Lawyer in Hanover and Brussels
Sara Nesler, Mag. iur. (Torino), LL.M. (Münster)

September 2021

The term "artificial intelligence" includes self-learning systems that are used in a variety of fast-developing technologies. For example, AI can be used to increase the efficiency of production plants and improve the prevention of diseases. With the progress of digitalisation, AI will play an important role in the economy and society. However, in addition to the benefits, the use of AI systems also creates challenges and risks that should be kept under control with regulation. A company's future strategy should therefore take into account the development of the legal framework for AI.

Development within the EU

The European Union published a White Paper in 2020 that expands the AI strategy presented in 2018 in two main directions. First, it will push AI development and research by making resources available and increase AI competences within the EU thanks to greater cooperation between member states. In addition, the EU wants to promote citizens' confidence in the new technologies and also ensure access to AI for small and medium-sized enterprises. On the other hand, the need for global regulation at the European level has been recognised.

As a result, on 21.04.2021, the EU Commission presented a proposal for a regulation to establish harmonised rules for artificial intelligence (AI Regulation). The main target of the draft is to regulate the use of AI systems in the EU in such a way that the risks of the technology are minimised without complicating or limiting its development.

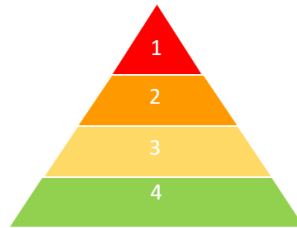
Scope of the Regulation

The AI Regulation provides for a broad definition of AI. This makes the regulation applicable not only to modern *machine-learning* systems, but also to traditional *hard-coded* software based on logic and statistics. The entire value chain of AI systems is affected, both in the private and the public sector. The planned AI regulation is therefore aimed at providers, developers and manufacturers of AI systems, but also at importers, traders and users (excluding consumers).

Measures by risk level

In order to fully regulate different AI systems and applications without setting unnecessary limits to the development and use of the new technologies, the regulation follows a risk-based approach.

The draft defines four levels of risk, which will be modified or extended as needed in the future.



(1) Unacceptable risk

AI systems that create an unacceptable risk will be banned. These include systems that manipulate people's behaviour or exploit physical and psychological weaknesses, which can cause physical or psychological harm. Examples include toys that cause young children to behave dangerously, so called “*social scoring systems*” that can lead to discrimination by authorities, and systems that use biometric identification (exceptions include identification and tracking of a criminal offender or suspect).

(2) High risk

This risk level covers two main groups of applications: firstly, security systems and components (e.g. robotic surgery applications or automotive security components), and secondly, systems used in sensitive areas that may cause fundamental rights violations. This also includes critical infrastructures, access to schooling or education, professional recruitment procedures, law enforcement, the administration of justice, as well as important private and public services, such as credit rating.

For high-risk AI systems, the regulation contains strict requirements, including on the risk assessment of systems, quality of data sets, traceability of operations and adequate human oversight. To ensure compliance, placing a high-risk AI system on the market will require a positive (internal or external) conformity assessment, registration in a European database established for this purpose and the use of a CE conformity symbol.

In addition to the obligations for suppliers and product manufacturers, the planned AI Regulation also provides for supervisory, reporting and warranty obligations for importers and distributors.

(3) Low risk

AI systems that require special transparency obligations are rated as low risk. For example, the use of chatbots and exposure to so called *deep fakes* (manipulated or generated content that is perceived as authentic people, facts or objects) should be made public in the future. The same applies to systems that detect emotions or make biometric categorisations.

(4) Minimal risk

The majority of AI systems, such as video games or spam filters, pose only minimal risk according to the AI Regulation and should accordingly be free to use within the framework of the law already in force.

Recent issues for discussion

However, it is questionable whether the Commission will succeed with the draft regulation in creating a clear legal framework that fully protects fundamental rights without making the development and use of AI systems excessively difficult.

Uncertainty in the law

Terms such as "psychological damage" and "psychological weakness" are not defined in detail. This is important both for business and for the effective protection of citizens: it is not clear how far the use of nudging can go without being regarded as unacceptable.

Extensive requirements

Suppliers and product manufacturers are criticising the requirements for high-risk systems and their verification as too complicated. At the same time, specialists complain that the draft takes too much economic interests into account. High-risk systems can cause serious negative consequences, and it is therefore not sufficient that an internal conformity assessment should be sufficient for most high-risk systems. On the other hand, suppliers appreciate this approach, as it better protects intellectual property and trade secrets.

Practicability in practice

It is also unclear how some regulations can be implemented in practice. Human supervision for automated assessments and decisions, for example, is much more broadly regulated than in the GDPR. According to the AI Regulation, the formal involvement of a human in the decision is not sufficient. Instead, humans with an understanding of the system and aware of the possible effects of bias in the automation should be able to decide independently whether to use the AI system or to disregard the result.

Currently, this is often not the case when assessing the credit rating of a customer. It is true that a human assessment is carried out alongside the algorithmic assessment, and the final decision on whether to grant a loan is usually made by a human being. Nevertheless, the algorithmic assessment plays a central role in the calculation of the interest rate. The clerk is bound to the "system" there, and also cannot fully comprehend which criteria have gone into the assessment. For reasons of data protection, not all criteria that have gone into the score are disclosed to the bank.

Automated assessments and decisions play a growing role in many areas of the economy and society. Greater transparency of processes is therefore desirable for AI to serve and gain the trust of humans - as desired by the Commission. Nevertheless, it must be considered how and to what extent the rules can be applied in practice without suppressing the supposed advantages of AI, such as time savings and objectivity, by extensive human control and correction. If no balance is found, the role of the human decision-maker will remain largely on paper, as with the General Data Protection Regulation. Finally, the decision to bypass algorithmic assessment could become a liability issue. In practice, many human decision-makers would not want to take on the responsibility for this.

Liability and enforcement

Who should be liable for damage caused by AI-controlled machines and systems that are not covered by contractual liability is left open in the proposed regulation. An example of this is damage caused by a malfunction of an autonomously driving vehicle. Thus, the draft lacks the necessary systematics at this point. (More on this in the Compact "*Artificial Intelligence and Law*", Ulrich Herfurth, January 2019).

The regulation does not yet provide any special rights for those who are assessed by AI systems or whose behaviour is controlled. Enforcing the law in the field of artificial intelligence is particularly difficult because the processes are often not transparent. However, the draft does not

address reversals of the burden of proof or alleviations of causality.

Implementation of the Regulation

For the implementation of the regulation, the establishment of a European AI Committee with mainly advisory functions is planned. The new authority is to consist of the competent authorities of the member states and the European Data Protection Supervisor, following the model of the European Data Protection Committee. Compliance with the requirements for high-risk systems is to be checked by the market surveillance authorities.

Violations of the AI Regulation are punishable by heavy fines. These can reach up to 30 million euros or 6 % of the worldwide annual turnover. It is therefore very important for companies to observe legal developments and to plan strategically accordingly.

Outlook

The draft is still at the beginning of the legislative process. It is still unclear whether possible changes will favour the development of AI and the associated economic interests or the protection of citizens' fundamental rights. Both interest groups are lobbying intensively.

The AI regulation is expected to come into force in 2024.

+ + +

Chapter Two

The New Sales Rules in Europe



1



2

Summary

- Introduction
- Material defects: tangible goods
- Material defects: digital goods
 - B2B
 - B2C
- Further changes: (B2C)
- Supply chain: tangible goods
 - B2B
 - B2C
- Supply chain: digital goods
 - B2B
 - B2C



3

Introduction

4

The new EU Directives

- Two new EU Directives, the Sales of Goods Directive (2019/771) and Digital Content and Services Directive (2019/770) came into force on 01.01.2022
- EU Directives are not directly applicable. They must be transposed into national law by all Member States
- The following slides are based on the German transposition of the directives, but similar laws apply in the other Member States



Herfurth & Partner - Alliuris Summer School 2022

5

5

Material Defect: Tangible Goods

Herfurth & Partner - Alliuris Summer School 2022

6

6

Extended definition of “material defect”

Both for B2C and B2B contracts - **new**:

- ✓ a purchased item is only free of defects if it meets both **subjective and objective** quality requirements and any necessary **assembly** requirements
- ✓ It is **no longer** sufficient for the item to comply with an agreed quality **or** the quality that would normally be expected



Herfurth & Partner - Alliuris Summer School 2022

7

7

Contractual deviations

- The objective quality requirements may be deviated from by contract
- For B2C contracts, it is required that the consumers have been expressly informed of a deviation of the goods from the regular objective requirements and the deviation has also been explicitly contractually agreed



Herfurth & Partner - Alliuris Summer School 2022

8

8

Material Defect: Digital Goods

Herfurth & Partner - Alliuris Summer School 2022

9

9

New rules for digital products and products with digital elements (B2C only)

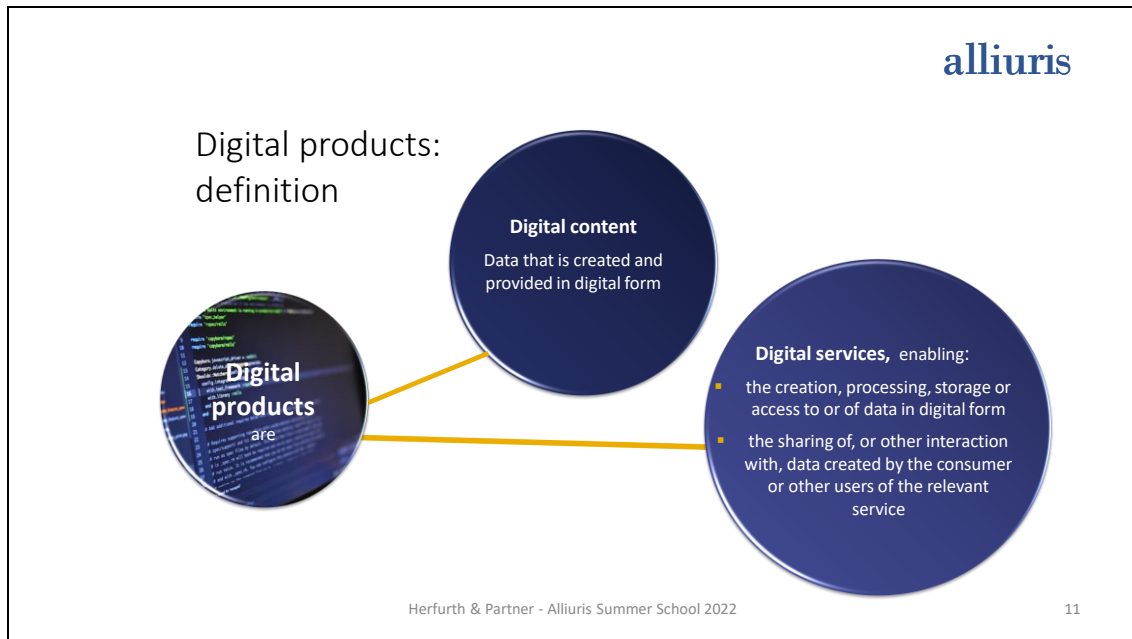
- Special regulations for B2C contracts for the provision of **digital products** and **products with digital elements**
- Purpose: to extend the life cycle of the products and strengthen security for users (data protection and cyber security)



Herfurth & Partner - Alliuris Summer School 2022

10

10



11

alliuris

Products with digital elements

- Definition: "item that contains or is connected to digital content or digital services in such a way that **it cannot fulfill its functions without this digital content or digital services**"
- The digital content or service must be essential for a functional use of the sold goods
- Assumption that obligation of the entrepreneur includes the provision of digital content or digital services

Herfurth & Partner - Alliuris Summer School 2022

12

12

alliuris

Is it a product with digital elements?



smartphone

Herfurth & Partner | Alliuris Summer School 2022

13

13

alliuris

Is it a product with digital elements?



car with navigation system

Herfurth & Partner | Alliuris Summer School 2022

14

14

alliuris

Is it a product with digital elements?



mowing robot

Herfurth & Partner | Alliuris Summer School 2022

15

15

alliuris

Is it a product with digital elements?



shoes

Herfurth & Partner | Alliuris Summer School 2022

16

16

alliuris

Is it a product with digital elements?



Herfurth & Partner | Alliuris Summer School 2022

17

17

alliuris

Is it a product with digital elements?



Herfurth & Partner | Alliuris Summer School 2022

18

18

alliuris

Is it a product with digital elements?



Herfurth & Partner | Alliuris Summer School 2022

19

19

alliuris

Is it a product with digital elements?



for now...

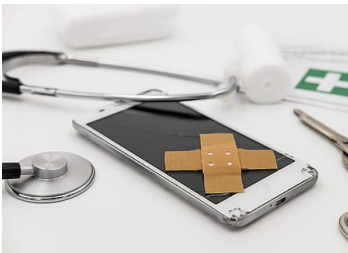
Herfurth & Partner | Alliuris Summer School 2022

20

20

„Material defects“ and digital products

- The general "classic" concept of material defects only applicable to physical objects
- **New** separate concept of material defects for digital products and those with digital elements
- Subjective and objective requirements as well as integration requirements (similar to the assembly requirements)



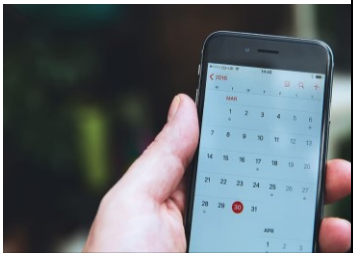
21

Subjective prerequisites	Objective prerequisites	Integration prerequisites
1. Agreed quality 2. Suitability for intended use 3. Provision as agreed in the contract 4. Provision of updates	1. Suitability for usual use 2. Usual and expected condition 3. Condition corresponds to test version or advance notice 4. Provision with accessories and instructions 5. Provision of updates and information about them 6. Provision of the latest available version	Proper implementation of integration Alternatively, at least proper integration by contractor or proper instruction.
For No.1: agreed quantity, functionality, its compatibility, interoperability	For No.2: (conscious and justified) public statements, quantity, functionality, compatibility, accessibility, continuity, security	"Integration" means the connection and integration into the digital environment of the consumer

22

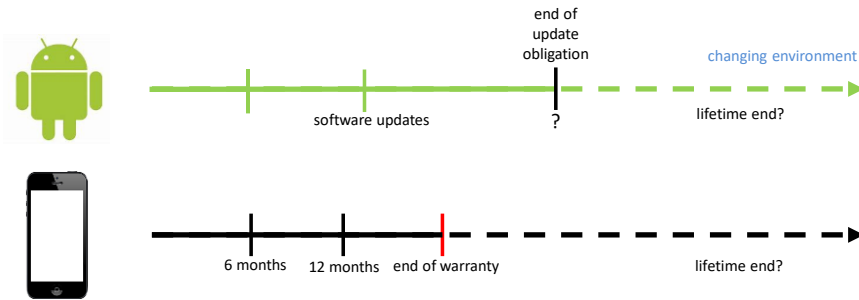
Update obligations (B2C)

- For goods with digital elements, updates must be provided at regular intervals if this is necessary and expected to maintain the contractual functional and usage status
- Duration of the obligation depends on the product or the contractual agreement. If the updates are not provided, the product is defective
- Statute of limitation: 12 months after the end of the period of the obligation to update

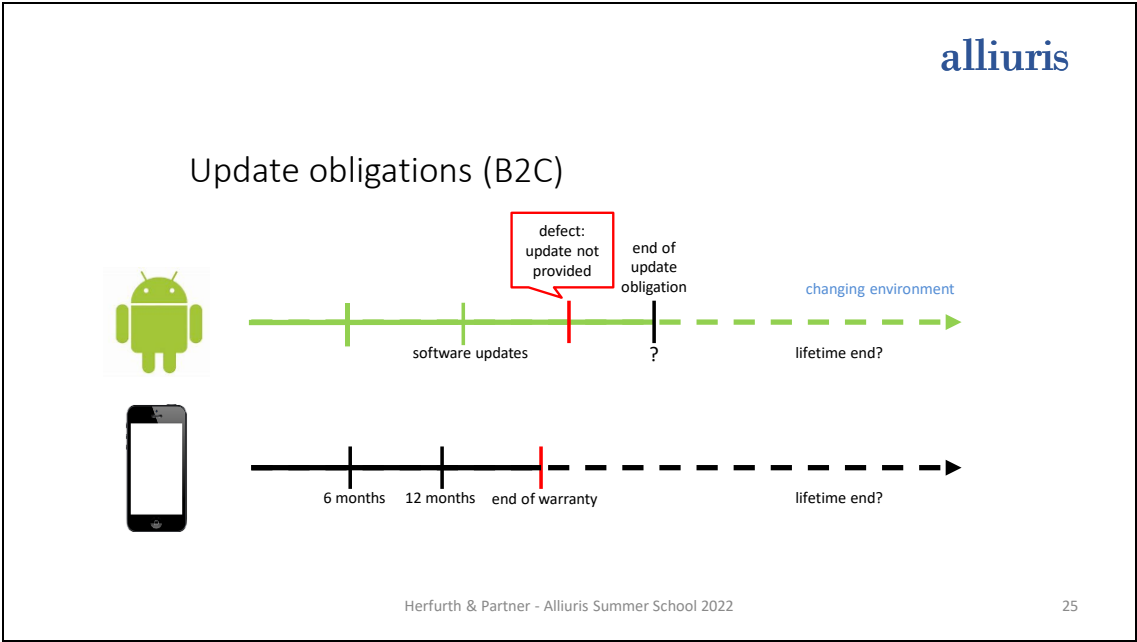


23

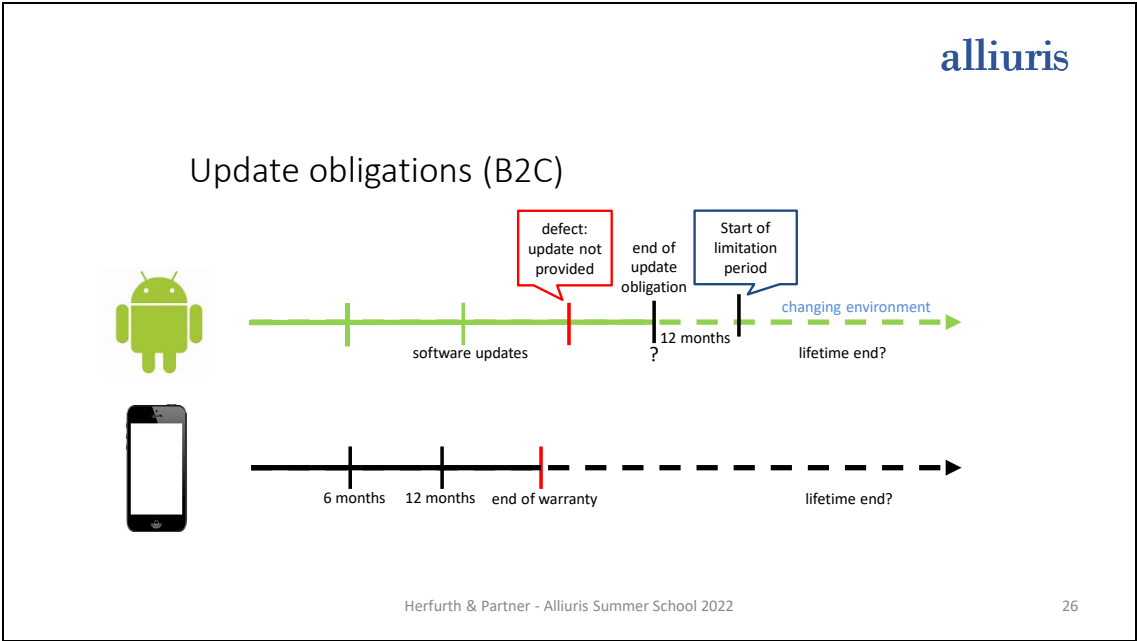
Update obligations (B2C)



24



25



26

Digital goods in B2B business

- Adoption of individual statutory regulations for digital goods via individual agreements. Advantage: better "fitting"
- Adoption of individual regulations in the company's own purchasing terms and conditions: consider carefully



Herfurth & Partner - Alliuris Summer School 2022

27

27

Further Changes (B2C)

Herfurth & Partner - Alliuris Summer School 2022

28

28

Information requirements (B2C)

- Used goods, exhibition goods and B-goods:
 - ✓ **Separate, specific** information about reductions in quality
 - ✓ General information in the product description, the general terms and conditions or descriptions is no longer sufficient.
- Information about upcoming changes and updates to digital products



Herfurth & Partner - Alliuris Summer School 2022

29

29

Easier assertion of claims (B2C)

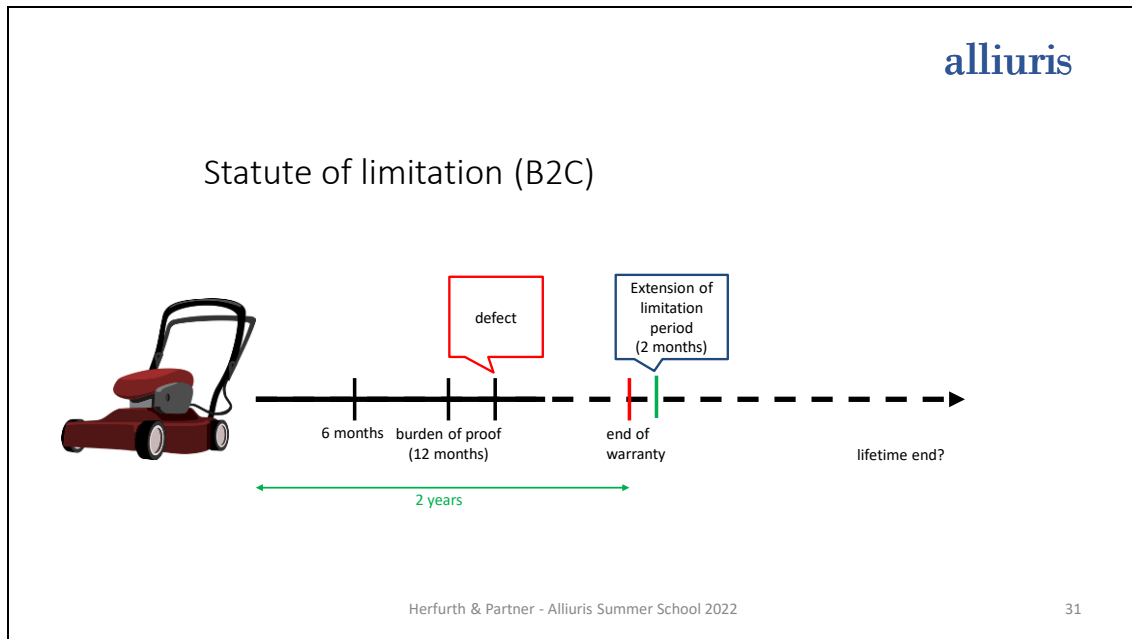
- Easier withdrawal (setting of explicit deadline no longer necessary)
- Extension of the reversal of the burden of proof from 6 to 12 months
- Suspension of the statute of limitations: the consumer has at least 2 months to report the defect, even if the defect is discovered shortly before the expiration of the (normally 2-year) warranty period



Herfurth & Partner - Alliuris Summer School 2022

30

30



31

alliuris

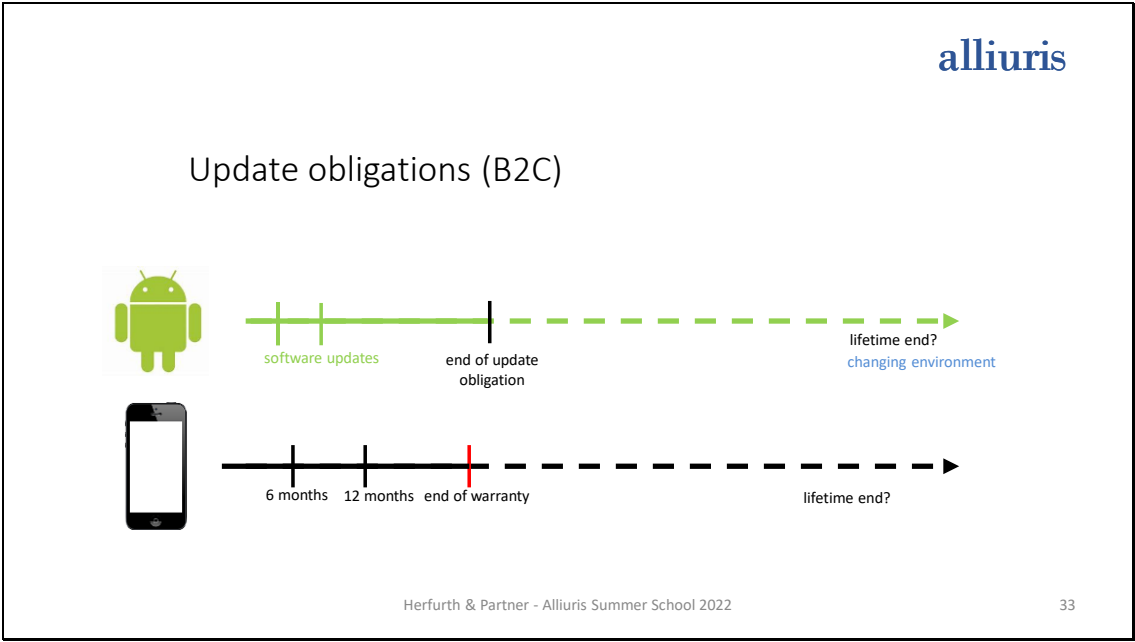
Specifically for **digital goods**:

- If a defect is discovered within the limitation period, the limitation period may be extended by 4 months
- If the digital goods are provided for a lasting period of time, the limitation period starts only 12 months after the end of the provision period
- In the case of updates, the limitation period begins 12 months after the end of the corresponding provision period
- In case of agreed permanent provision of the digital goods, the liability period lasts at least 2 years from the provision of the goods.

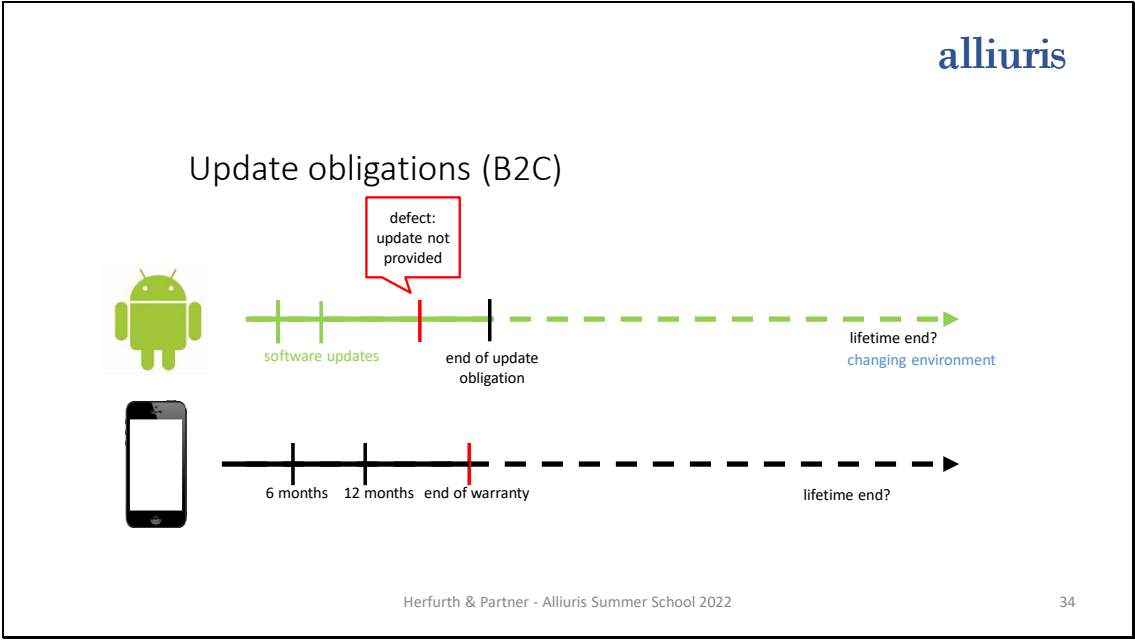
Herfurth & Partner - Alliuris Summer School 2022

32

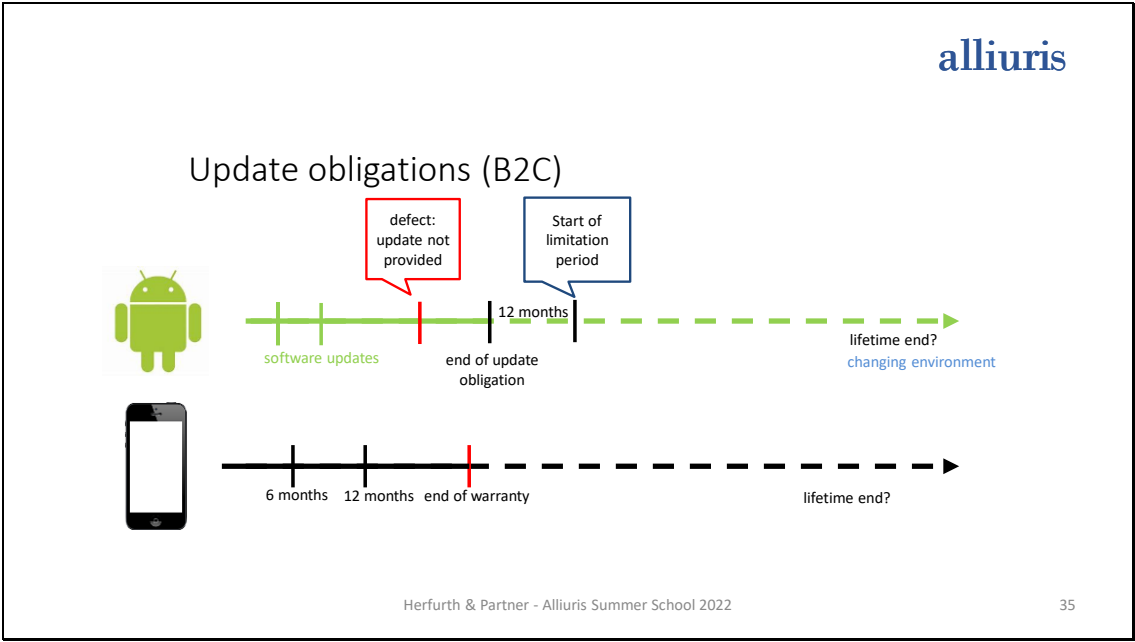
32



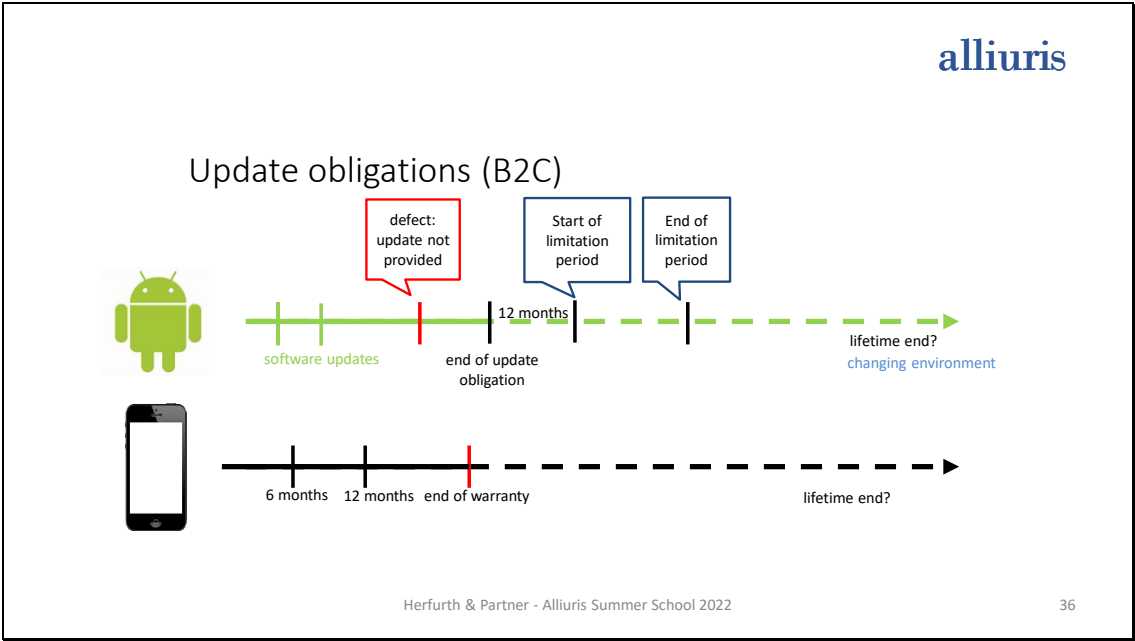
33



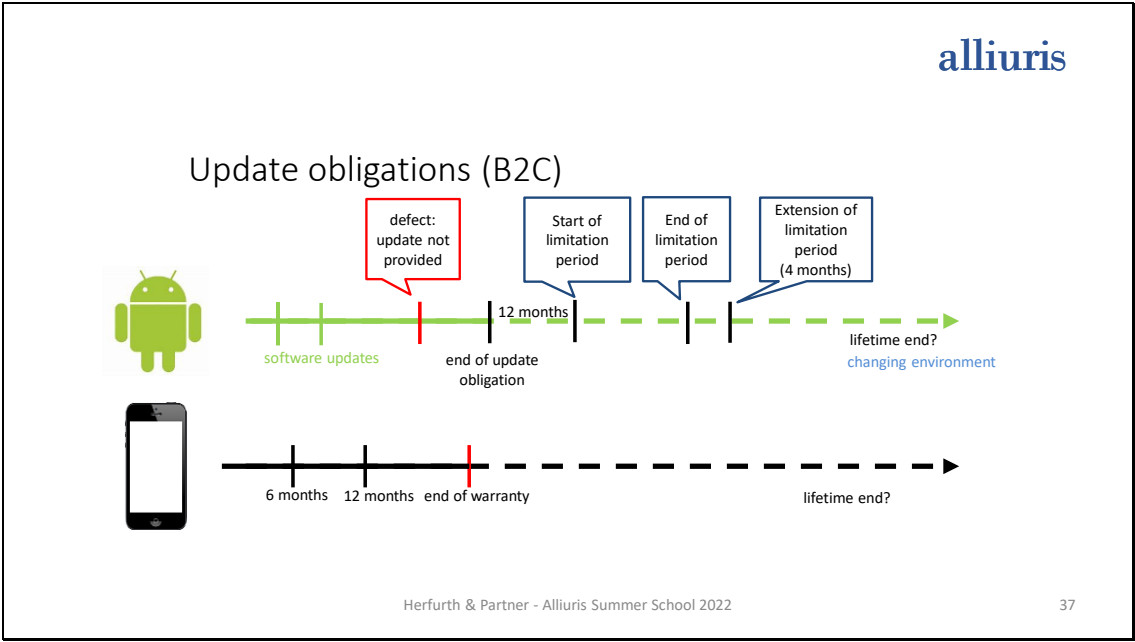
34



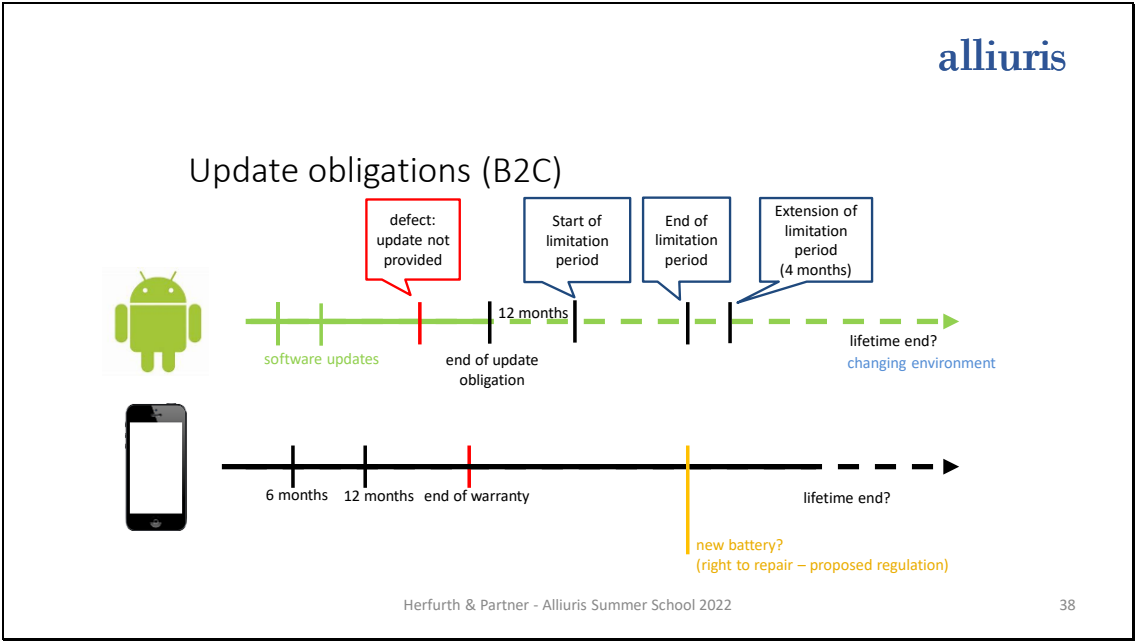
35



36



37



38

Stricter requirements for warranty declarations and agreements (B2C)

Warranty declarations and agreements must:

- Be understandable and transparent
- refer to the legal warranty rights which continue to exist in their entirety
- be made available at the latest at the time of delivery on a "permanent data carrier" (paper or e-mail)



Supply Chain: Tangible Goods

Suspension of expiry in supplier recourse

- Possibility of taking recourse against suppliers
- Limitation period of 2 years
- Suspension: if the item has been sold to the consumer before the 2 years have expired, the seller can assert his rights of recourse up to 2 months after he himself had to fulfill subsequent performance claims
- Previous time limit of 5 years from the date of handover (supplier-seller) ceased to apply on 01.01.2022



41

NSO



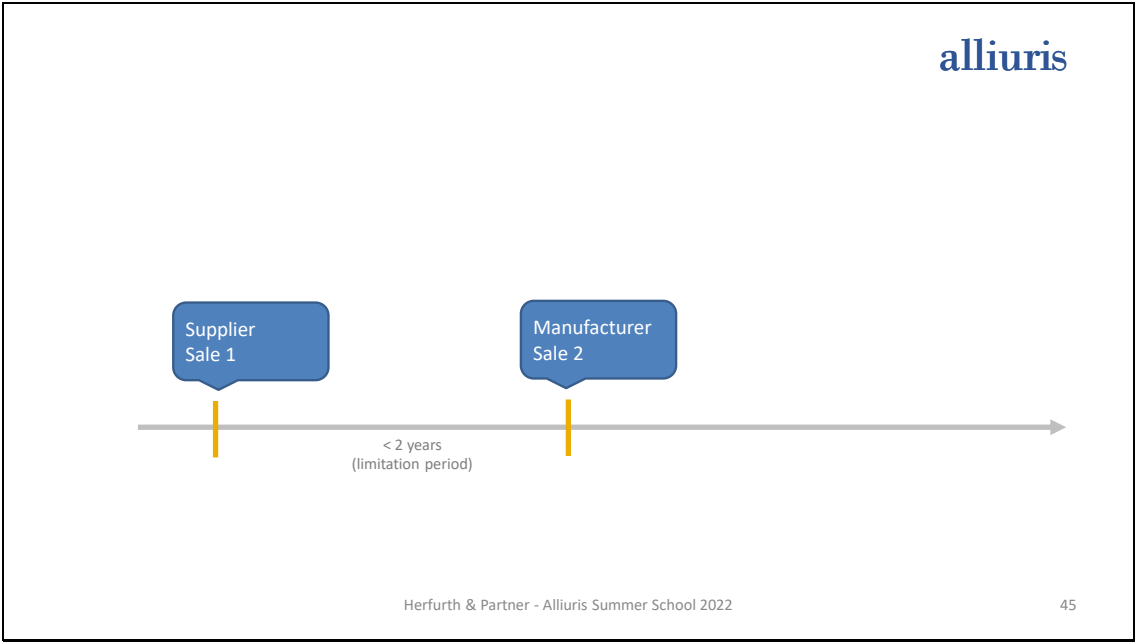
42



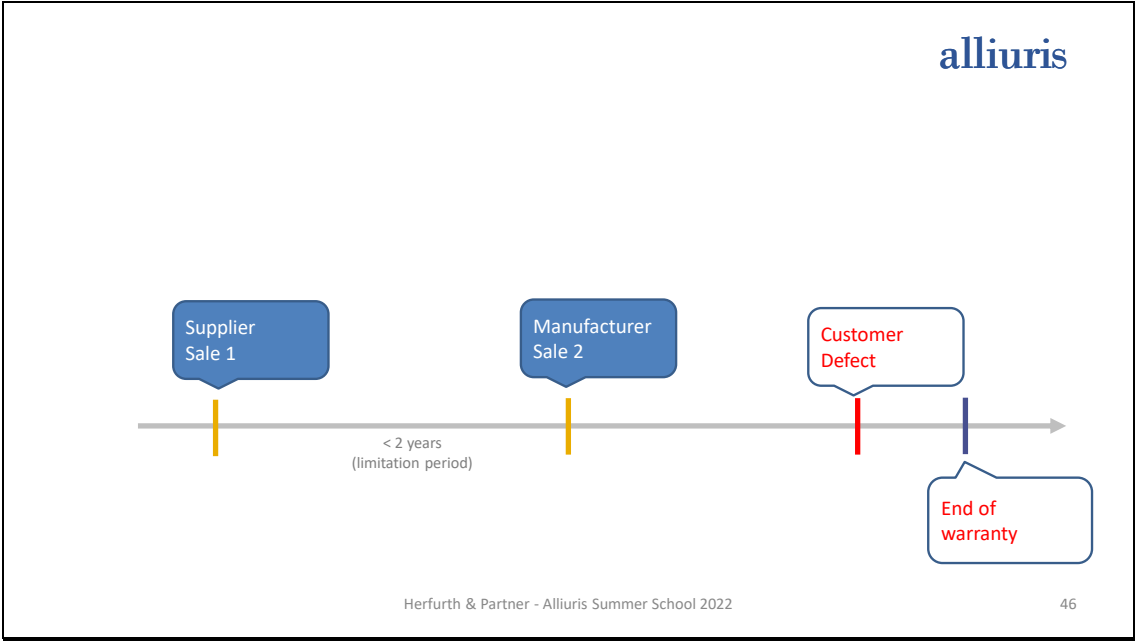
43



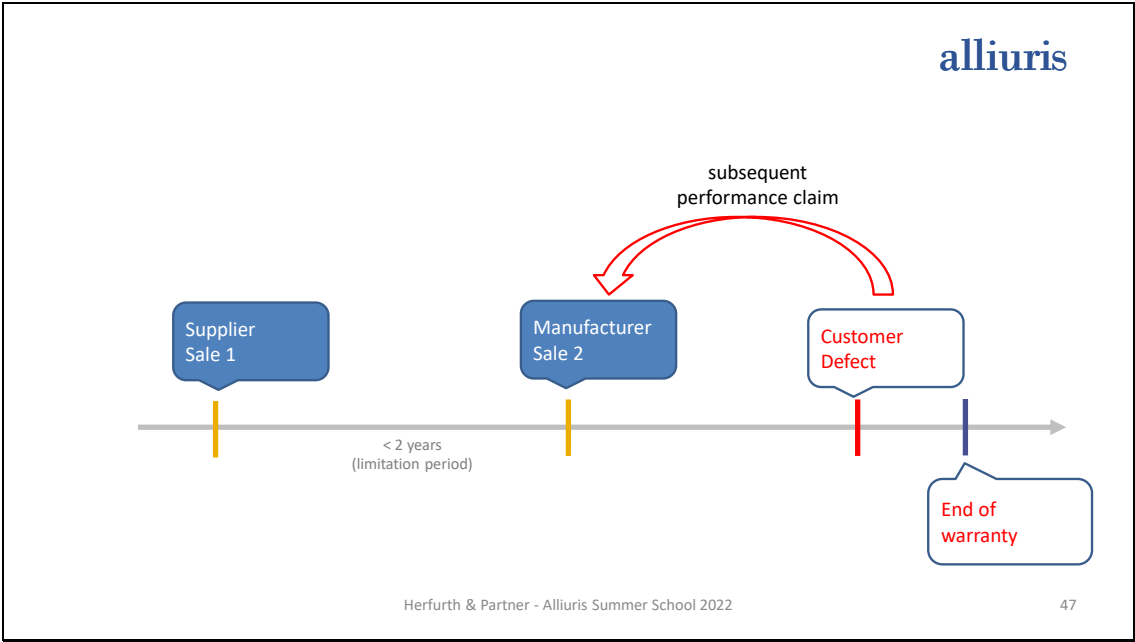
44



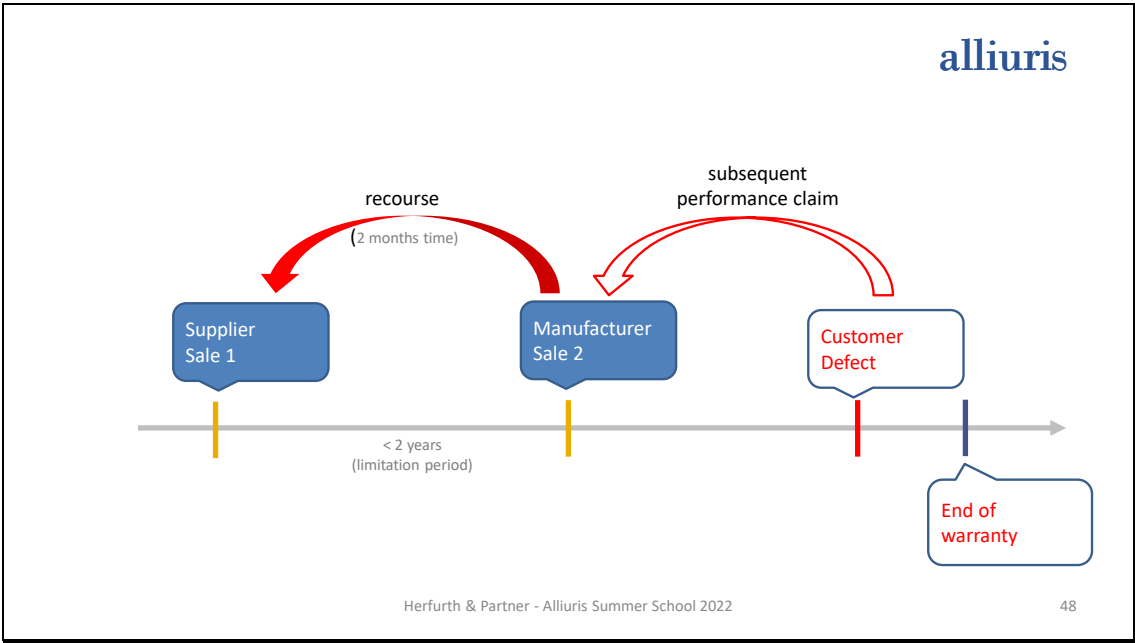
45



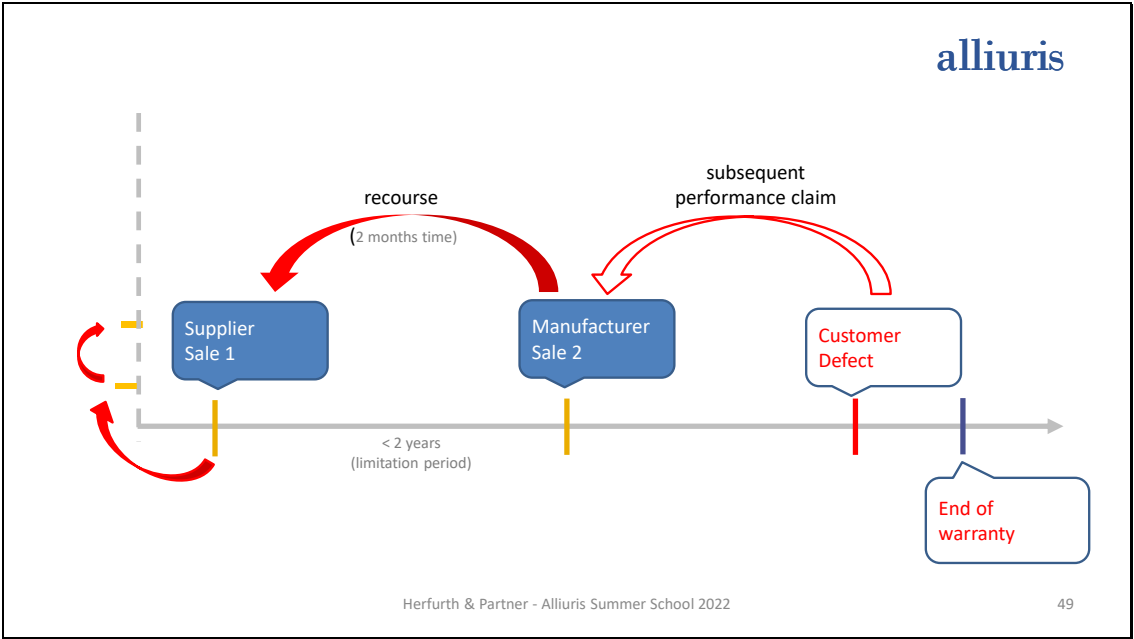
46



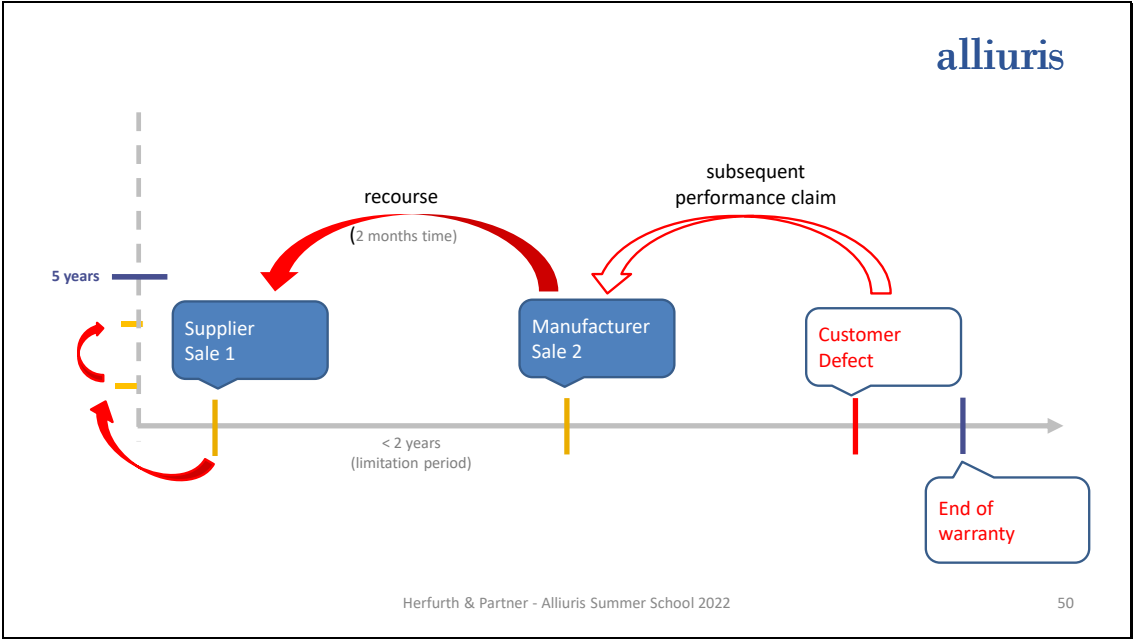
47



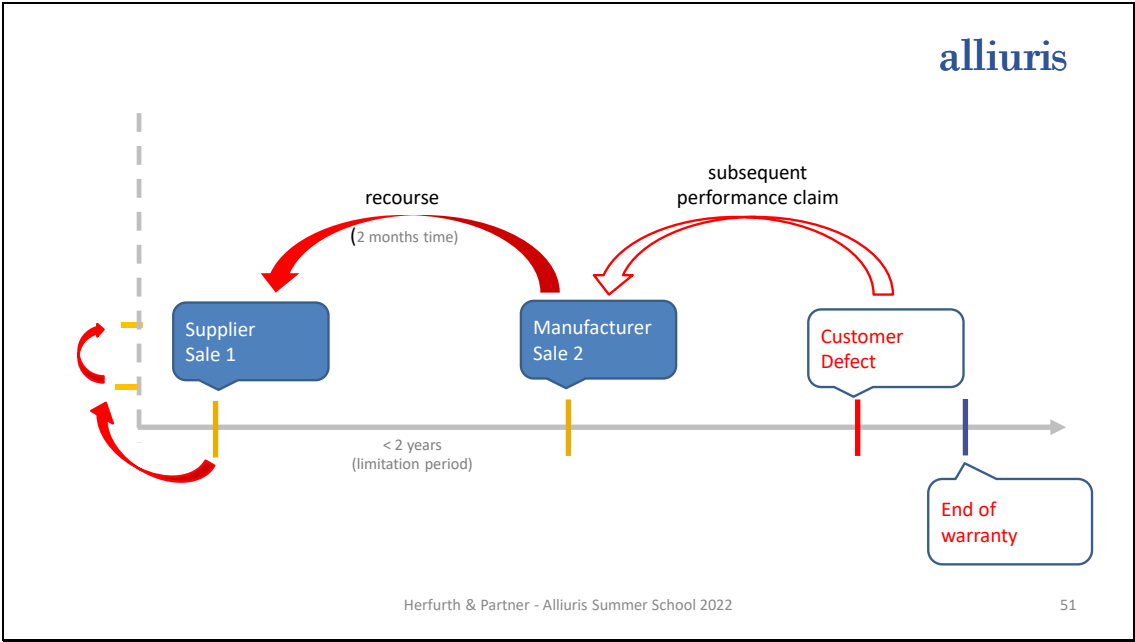
48



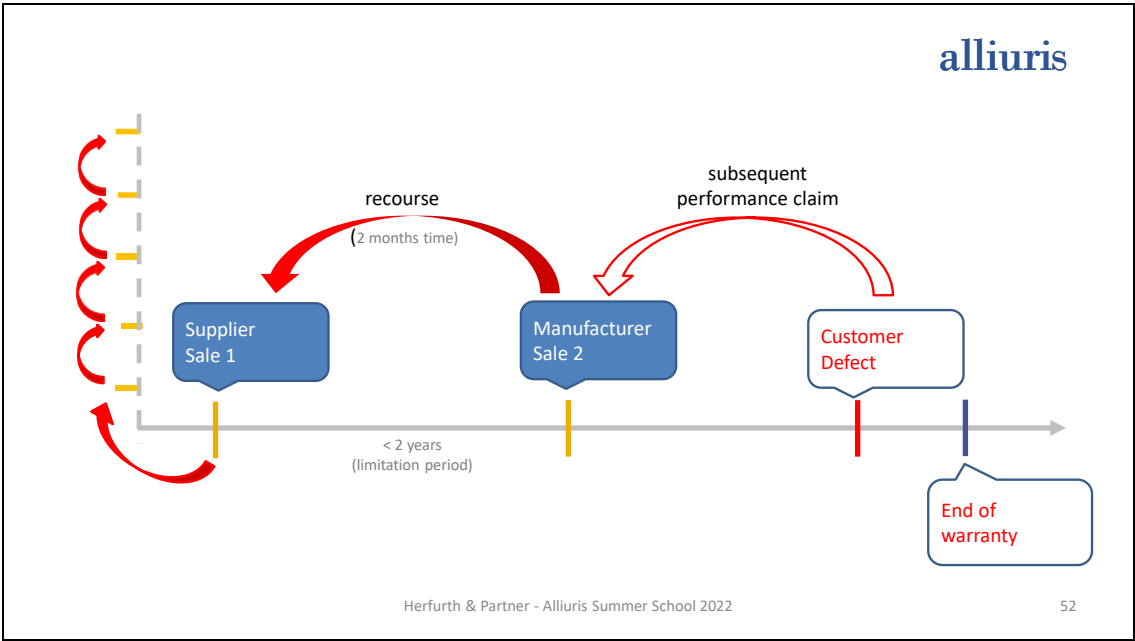
49



50



51



52

Contractual deviation (B2B)

- §§ 445a, 445b BGB: a supplier can exclude the recourse claims of its B-customer by means of a GTC clause or through an individual contractual agreement.
- A limitation of the right of recourse to an appropriate maximum amount is permissible.



Herfurth & Partner - Alliuris Summer School 2022

53

53

Contractual deviation (B2C)

- In principle, a supplier can exclude the recourse claims of its customer by means of a GTC clause or through an individual contractual agreement.
- However, if the last customer of the chain is a consumer, § 478 II BGB applies: Deviation from statutory provision allowed only if the respective customer receives an “adequate compensation” for the exclusion of the recourse claims, i.e.
 - ✓ Lump sum settlement
 - ✓ Lump sum claim for compensation for expenses in warranty cases



Herfurth & Partner - Alliuris Summer School 2022

54

54

Supply Chain: Digital Goods

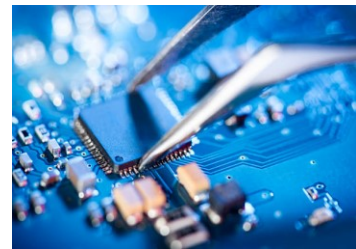
Herfurth & Partner - Alliuris Summer School 2022

55

55

Suspension of expiry in supplier recourse: new § 327u BGB

- Right of recourse expires within 6 months
- Claims to be made in the course of termination of the contract (lack of provision) or subsequent performance (provision of defective product)
- Limitation period runs from the date of
 - ✓ the termination of the contract by the consumer
 - ✓ the performed fulfillment of the claims for
 - ✓ supplementary performance



Herfurth & Partner - Alliuris Summer School 2022

56

56

Contractual deviation (B2B)

- §§ 445a, 445b BGB apply, same regulations as tangible goods: the supplier can exclude the recourse claims of its customer by means of a GTC clause or through an individual contractual agreement.



Herfurth & Partner - Alliuris Summer School 2022

57

57

Contractual deviation (B2C)

- If a consumer is at the end of the supply chain, the **new** § 327u IV BGB applies:
- It is **not possible** to conclude an agreement aimed at excluding the assertion of the rights specified in §§ 327u I to III BGB. These are **mandatory**. This prohibition shall also apply if the regulations are circumvented by other arrangements.
- The prohibition of waiver of §327u BGB is intended to protect the contracting party which is usually structurally inferior in the supply chain.



Herfurth & Partner - Alliuris Summer School 2022

58

58

alliuris

Thank you for listening to:

The new Sales Rules in Europe

Sara Nesler
Mag. Jur. (I), LL.M.

With the support of
Aline-K. Pehle

www.herfurth.de



Herfurth & Partner - Alliuris Summer School 2022

59

alliuris
INTERNATIONAL

Herfurth & Partner - Alliuris Summer School 2022

60

Materials | Compact

The new law on the sale of goods

Aline-Kristin Pehle, trainee lawyer, Hanover

January 2022

The European and German legislators are always keeping an eye on the further development of buyer and consumer protection. The legal requirements for retailers have recently become even more stringent as a result of the transposition of the new *EU directive on the sale of goods* into national German law. Dealers should react and adapt both their sales and operating modalities. The new regulations came into force on 01.01.2022 and have since been applicable to all contracts concluded from this cut-off date.

The new categories of goods

The general digitization of society is now also reflected in the new law on sales. From now on, the legislator will distinguish between *goods* in the *general* sense and *goods or products that are digital or contain digital elements*.

"Pure" *digital products* can be digital content or digital services.

Digital content is defined as data created and delivered in digital form.

Digital services, in turn, either enable the creation, processing, storage, or access to or of data in digital form, or they enable the sharing or interaction of the uploaded or created data.

Goods with digital elements are products that are linked to digital content or services in such a way that their provision is essential for the functional use of the products. This refers in particular to electronic goods.

It should be emphasized, however, that the regulations for the newly created category of digital goods initially apply only to contracts between entrepreneurs and consumers. For the sale of goods to entrepreneurs, only the general standards of sales law apply, regardless of whether the goods are analog or digital.

When is the purchased item free of defects?

The new provisions of the law on the sale of goods are accompanied by two new concepts of

material defects, one for goods in the general sense and another for digital goods. The two concepts of material defects have a similar structure and have made the requirements for freedom from material defects clearer. From now on, a (digital) good is basically only free of defects if it meets both subjective and objective quality requirements (and possibly also the necessary *assembly or integration requirements*). If the product to be sold deviates from the objective quality requirements, the deviation must be agreed on.

The general concept of material defect

The *subjective* conditions include the:

- *agreed* condition
- Suitability for *intended* use
- Handover with *agreed* accessories and assembly instructions

The *objective* conditions include the:

- Suitability for *ordinary* use
- usual and *expected* condition
- Conformity of the actual condition with the sample/specimen
- Delivery with *accessories* (incl. packaging, assembly or installation instructions, other expected instructions)

In addition, the requirement of *proper* assembly/assembly instructions must be fulfilled. This also applies to the common case that vicarious agents are commissioned and used for assembly.

The concept of material defects for digital goods

The *subjective* agreements include the:

- *agreed* condition
- Suitability for the *intended* use
- Provision as agreed in the contract
- Provision of *agreed* updates
-

The *objective* agreements include the:

- Suitability for *ordinary* use
- *usual* and *expected* condition
- Conformity of the condition with *test version* or *advance notice*
- Provision with *accessories* and instructions
- Provision of *updates* and information about them
- Provision of the *latest available* version
-

In addition, the requirement of *proper* integration/integration instructions must be met. This refers to the proper integration of a digital product into the consumer's digital environment. A digital environment includes both the hardware and the software or network connections.

Exhibition, used and B-goods

Particularly in the case of consumer transactions, it is no longer sufficient for quality reductions to be referred to in a general manner, e.g. by means of displays, in the product description or in the general terms and conditions. Instead, the individual consumer must be informed separately about the respective quality deviations and expressly agree to them when concluding the contract. Otherwise, the product is defective and the seller is liable accordingly according to the principles of liability for defects.

Obligations to act and provide information

With the special regulations on the provision of digital products and those with digital elements, the legislator aims to extend the life cycle of products in order to promote their sustainability as well as to strengthen security for users (keywords here are data protection and cybersecurity). Therefore, the focus is also on the obligation to update. Merchants must provide updates at regular intervals during the contractual provision period of the digital goods. Both the digital elements and the updates must actually be provided or made accessible. The consumer must also be informed in a timely manner of the upcoming changes and updates. If an entrepreneur fails to provide digital content or services, the consumer may be able to claim damages or even terminate the contract. Also, when failing to provide updates, the entrepreneur must be liable to the consumer for any resulting damages.

The legislator has not stipulated concrete provision periods for the digital elements and their updates; the duration of these periods depends on the concrete form of the contract, the usual period of use or advertising statements. If a permanent, i.e. unlimited, provision period is agreed, the seller's liability period is at least 2 years.

Digital goods in B2B business

Businesses that purchase digital goods from other companies (B2B) could also adopt individual statutory regulations for digital goods via individual agreements with their suppliers. The advantage of this would be better "fitting", especially of the new definition of material defects for digital goods. However, the adoption of individual regulations in the company's own purchasing terms and conditions should be carefully considered. Suppliers could refuse to give their consent in order to avoid an increased obligation to perform and liability that, from their perspective, is deliberately not intended by the legislator. The picture could be different, however, if the purchasing or supplied company has a strong market position and a correspondingly good negotiating position.

Further relief for consumers

Furthermore, entrepreneurs in B2C transactions must take into account additional facilitations

for the assertion of claims for subsequent performance and the withdrawal from the purchase contract for consumers and adapt their processes for subsequent performance management accordingly.

Setting a deadline and withdrawal

From now on, consumers no longer have to set an explicit deadline for rectification. It is sufficient if they notify the defect and, if necessary, make the goods available for rectification. It is important for the entrepreneur to document and keep track of how much time has passed since the defect was reported. Finally, if the entrepreneur allows a reasonable period of time for rectification to elapse, the consumer may withdraw from the contract. The specific duration of such a reasonable period depends on the type of product and the other circumstances of the individual case. There is no statutory provision in this regard.

Reversal of burden of proof

The fact that the reversal of the burden of proof - i.e. the presumption that the entrepreneur is responsible for a defect in the goods - is extended from a period of 6 months after handover of the purchased goods to a period of 12 months also works to the disadvantage of the seller. The entrepreneur must be able to specifically refute this legally presumed fault in order to avoid liability (which, however, often proves to be difficult).

Limitation

Changes have also been made to the provisions on the limitation periods for the consumer's rights in respect of defects; here, the expiry of these periods may be suspended:

In the case of analog or non-digital goods, the consumer always has at least 2 months to assert his rights in respect of defects. It only depends on whether the defect is still apparent within the (usually 2-year) limitation period. Even if the period has almost expired and is actually only less than 2 months, the expiration of the period is still delayed by 2 months. In the case of digital goods, the consumer always has at least 4 months to assert his defect rights as long as the defect still shows within the limitation period.

Normally, the limitation period begins to run from the handover of the purchased item. In the case of digital goods, however, the start of the period may be delayed. If permanent provision has been agreed, the start of the limitation period is only 12 months after the end of the provision period. And even in the case of updates, the period does not begin until 12 months after the end of the provision period.

Warranty

Entrepreneurs must also observe the new requirements for warranty declarations/agreements vis-à-vis or with consumers: The warranties must:

- point out the parallel existing legal warranty rights,
- be formulated in an easily understandable and transparent manner,
- designate the guarantor, the subject of the guarantee and the conditions for claiming (the how and whether),
- define the scope of the warranty (factual, spatial, temporal),
- be provided to the consumer on a durable medium (e.g. by e-mail or on paper).

Extensions in supplier recourse

If, in the end, the entrepreneur actually has to be liable for defects to his customer, he can, if necessary, turn to his supplier to indemnify himself. In the case of purchased goods, claims for recourse against the supplier are generally subject to a limitation period of 2 years from the date of handover of the goods by the supplier. However, this limitation period is suspended in favor of the entrepreneur. Thus, he can still assert his rights of recourse up to 2 months after he himself had to fulfill subsequent performance claims against a consumer. The expiry of the limitation period is thus "suspended".

Until now, this suspension of expiration was limited to a period of 5 years from the handover of the goods by the supplier to the entrepreneur. However, this time limit will no longer apply as of 01.01.2022. The consequence will be that the entrepreneur can still approach his supplier after more than 5 years. On the one hand, this will work in favor of the company performing the contract, but on the other hand, it will work to the disadvantage of the supplier.

Supplier recourse for digital goods

Even if the entrepreneur is liable to the consumer under a contractual relationship for digital goods, he may have recourse to his supplier.

Expenses that the entrepreneur must reimburse the consumer in the course of termination of the contract due to lack of provision or due to provision of defective products.

These recourse claims shall become time-barred within 6 months after the termination of the contract by the consumer or the performed fulfillment of the subsequent performance claims.

Recommendations for suppliers

Suppliers should always keep in mind the discontinuation of the limitation on the expiry of their customers' rights of recourse. If the end of the supply chain is not a consumer but an entrepreneur, they could include in their GTCs a retention of this time limit, which has so far been prescribed by law.

Recommendations for action for all companies

In order to comply with the stricter new regulations under sales law, companies should review and, if necessary, adapt their internal and external operating procedures; from purchasing and sales, to delivery and handover, to supplementary performance and claims against the supplier (keyword compliance).

If applicable, companies should:

- Update and adapt their General Terms and Conditions (GTC)
- Update and adapt their contracts with suppliers and manufacturers
- Adapt their model warranty agreements
- Update sales information, product descriptions and advertising claims
- Document the concrete handover/provision and assembly/integration
- Document the respective circumstances of the conclusion of contracts and their concrete design as well as the notification and rectification of defects,
- Identify the usual period of use and provision of (digital) goods and updates.

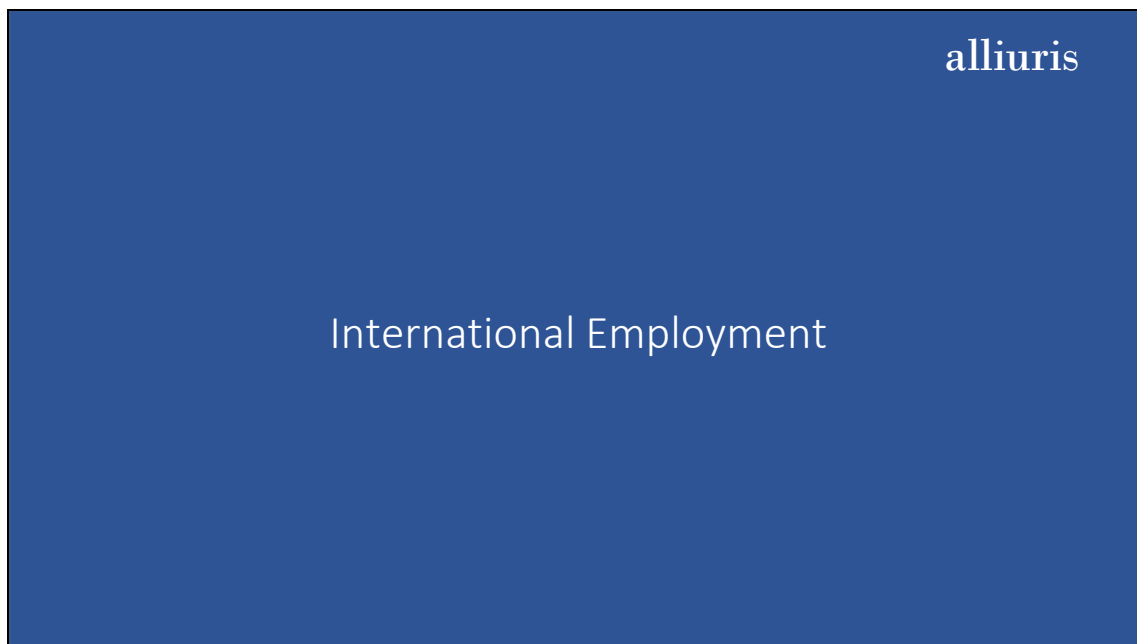
+ + +

Chapter Three

International Employment



1



2

Labour Law Principles

Mobile work

- ✓ Temporal/local relocation of work
 - Time and place of work can be freely chosen, digitalisation makes it possible to perform work around the clock and from anywhere in the world.
- ✓ Principles
 - contains clearly definable spatial and organisational points of reference
 - based on individual work situations with fixed and clearly identifiable employers, superiors and defined work tasks and conditions

Herfurth & Partner | Alliuris Summer School 2022

3

3

Principles of employment contract

- ✓ Start of the employment relationship
- ✓ Working time
- ✓ Remuneration, minimum wage
- ✓ Employer's duty to inform
- ✓ Contract language



Herfurth & Partner | Alliuris Summer School 2022

4

4

Tax Law

	Income from Germany	No income from Germany
Residence in Germany	Global income is subject to unlimited taxation in Germany	Foreign income is subject to unlimited tax liability in Germany
Residence abroad	Income from Germany is subject to limited taxation in Germany	Not taxable in Germany

Herfurth & Partner | Alliuris Summer School 2022

5

5

Social Security Law

Onboarding an employee from another EU member state

- ✓ To determine the applicable social security legislation within the EU, EEA and Switzerland, Regulation (EC) 883/2004 must be consulted:
- ✓ Social security contributions must always be paid in only one EU member state. In principle, social security law is based on the place of work.
- ✓ When employing workers from an EU country, domestic companies must ensure that they carry a so-called A1 certificate in addition to the European Health Insurance Card (EHIC).

Herfurth & Partner | Alliuris Summer School 2022

6

6

Social Security Law

Onboarding an employee from non-EU member state

- ✓ Territorial principle: Employees are subject to the social security law of the country in which they work.
- ✓ When there is no social security agreement between Germany and the two countries: problem of double insurance.
- ✓ On entry into Germany, (voluntary) health insurance is required
- ✓ With the start of employment, a change to German statutory health insurance is possible



Herfurth & Partner | Alliuris Summer School 2022

7

7

Social Security Law

Onboarding an employee from the USA

- ✓ The social security agreement between Germany and the USA applies only to pension insurance.
- ✓ Employees are still subject to the social security regulations of their home country if the following conditions are met:
 - Employee has not worked in Germany for longer than 60 months.
 - Employee is employed by a company to which he/she usually belongs in the home country.

Herfurth & Partner | Alliuris Summer School 2022

8

8

alliuris

Social insurances

Herfurth & Partner | Alliuris Summer School 20229

9

alliuris

Accident insurance



Social insurances

Herfurth & Partner | Alliuris Summer School 202210

10

alliuris

Accident insurance



Health insurance

Social insurances


Herfurth & Partner | Alliuris Summer School 2022

11

11

alliuris

Accident insurance



Health insurance

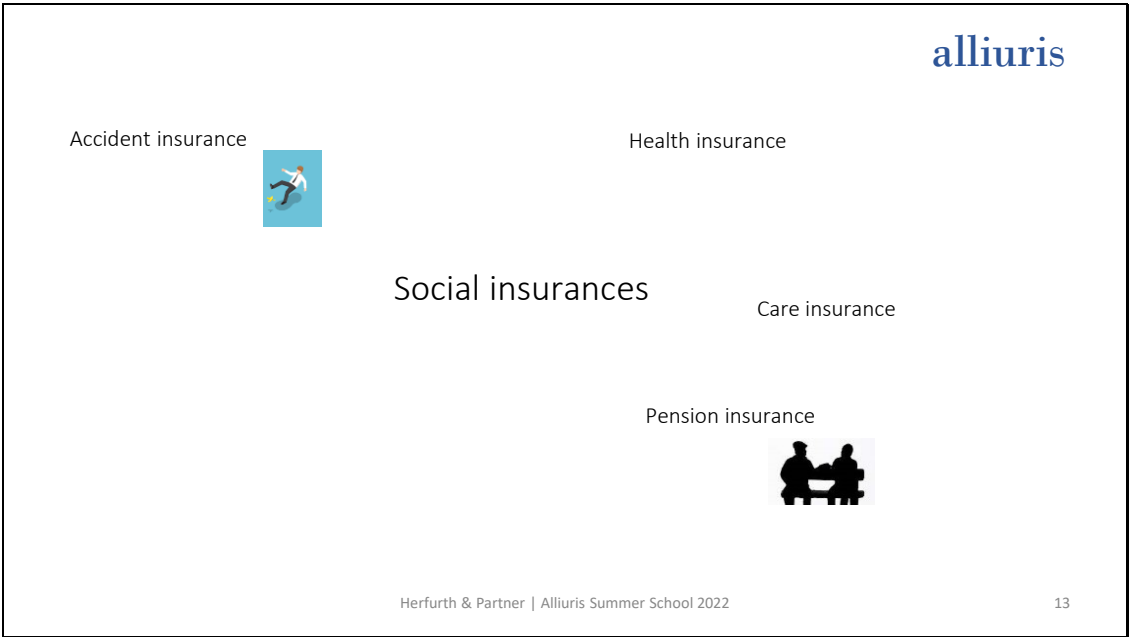
Care insurance

Social insurances

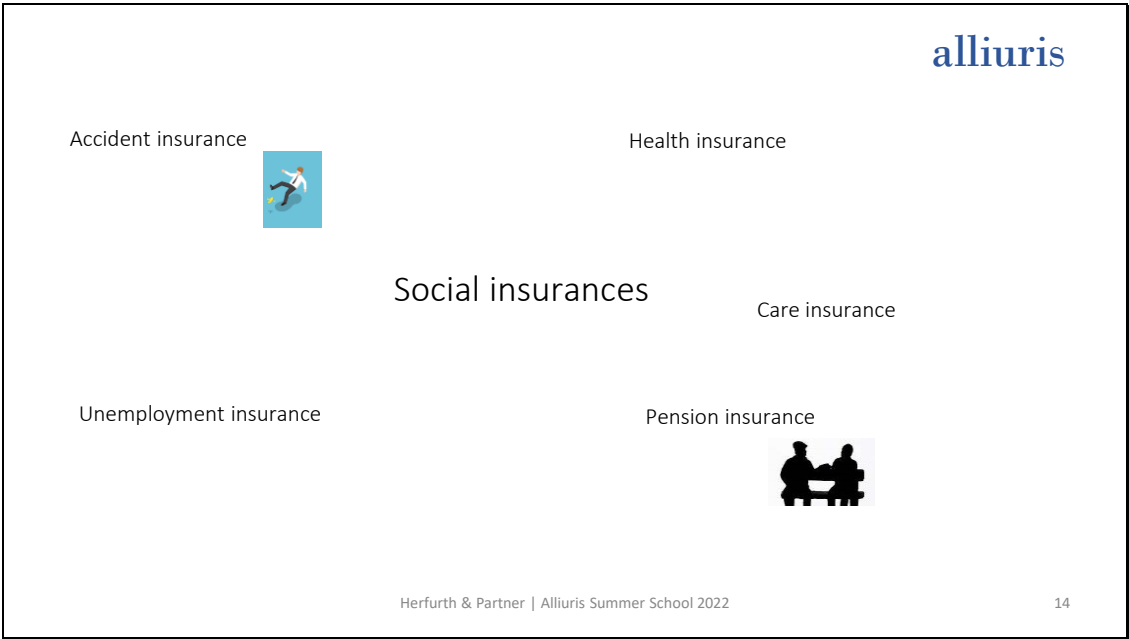
Herfurth & Partner | Alliuris Summer School 2022

12

12




13



14

alluris


Accident insurance



Health insurance

Care insurance

Pension insurance



Unemployment insurance

Social insurances

How does it work in your country?

Herfurth & Partner | Alluris Summer School 2022

15

15

alluris

INTERNATIONAL

16

Materials | Compact

Onboarding - bringing foreign employees on board

Stephanie Reese, attorney at law in Hanover

April 2022

The onboarding of foreign employees is becoming increasingly important against the background of the rising demand for skilled workers. New employees are hired and integrated into a company in a targeted manner. The goal of the onboarding process is to familiarise the new employee with the company and to integrate him or her quickly into the team and the corporate culture.

Good onboarding prevents new employees from quitting during the probationary period and instead creates an atmosphere in which new employees feel comfortable, which in turn leads to smoother work processes.

For onboarding to be successful, the process should be planned from start to finish and carried out accordingly.

In the following, the essential information on the preparation and process of onboarding in the case of an employee from a third country is presented.

Preparations

Already during the job interview, the company and the future foreign employee should discuss what both sides should bear in mind in the event of an agreement and what preparations need to be made in order to realise a smooth and speedy commencement of work.

Labour law basics

The parties to the employment contract must determine the beginning of the employment relationship and thus also the beginning of the social security obligation. At the same time, further regulations essential to the employment relationship, such as the working hours, must be agreed upon.

An employer has an increased duty of care when employing foreign workers. Thus, the company must inform the employee about the principles of German social security, among other things. The company must also cooperate in the approval procedure of the Federal Employment

Agency, which checks the foreign employee's employment in Germany before he/she starts work.

The employment contract should be drafted in German and at least in English in order to avoid any language-related ambiguities between the contracting parties as far as possible from the outset.

Visa and entry process

A foreign employee who plans to come to Germany to take up qualified employment must fulfil the following admission requirements:

- Concrete job offer in Germany has been received
- Foreign employee has at least A2 German language skills
- Foreign employee has recognised/comparable qualification and, if applicable, professional licence in the case of regulated professions
- Federal Employment Agency agrees to take up the qualified employment
- Subsistence of the foreign employee is secured

If these requirements are met, the next step is for the employee to make an appointment at the German embassy in his or her home country or in the country where he or she usually stays at the time in order to apply for a visa to enter Germany.

Upon entry into Germany, the foreign employee must provide proof of German health insurance.

After arriving in Germany, the permanent residence employee submits his or her application to the Aliens' Registration Office for a residence permit to take up qualified employment.

Family reunion

In order for the family of the employee who has come to Germany to join them, the following requirements must be met:

- Spouse (minimum age: 18 years) or parents have a valid residence title in Germany
- The family member joining them has at least A1 German language skills
- There must be sufficient living space available
- The livelihood is secured by the person already living in Germany

If the requirements are met, the next step is for the family member to make an appointment at the German embassy in the home country or country of habitual residence.

Taxes

With regard to the foreign employee's income tax liability, the following principles apply, although in individual cases the respective double taxation agreement between Germany and the respective third country would always have to be examined:

- If the employee is resident in Germany and receives his/her income from Germany, all income is subject to unlimited tax liability in Germany.
- If the employee is resident in Germany and does not receive any income from Germany, the foreign income is subject to unlimited tax liability in Germany.
- If the employee is resident abroad and receives income from Germany, this income is subject to limited taxation in Germany.
- If the employee is resident abroad and does not receive any income from Germany, there is no tax liability in Germany.

Social security

In principle, the territorial principle applies in social security law. According to this, employees are subject to the social security law of the country in which they work. Anyone who works in Germany is subject to social insurance under the laws of that country.

Depending on the exact form of activity in the third country as the home country, there may also be a social insurance obligation in Germany. At this point, it is important to check in individual cases whether there is a social security agreement between Germany and the respective third country in order to avoid double insurance.

When entering Germany, the foreign employee must have (voluntary) health insurance. A change to statutory health insurance is then possible with the start of employment.

Data protection

Even before the employee starts work, the employer needs important information and documents from the employee, such as the residence and work permit and the personnel questionnaire. This already involves personal data processing, which must be legal under data protection law.

Companies must inform new employees about what they have to observe in terms of data protection law in their work. For example, employees must be obliged to observe confidentiality when handling personal data.

On the day the employee starts work, the company should ensure that authorisations for computer programmes and folders, among other things, are or will be set up at the workplace. If terminal equipment is made available, an inventory should be made before handing it out to the employee.

Accelerated procedure for skilled workers (Section 81 a AufenthG)

Since the entry into force of the Skilled Workers Immigration Act on 01 March 2020, companies and skilled workers from third countries have the possibility to shorten the entry procedure. The accelerated procedure for skilled workers is as follows:

Aliens Department

The foreign skilled worker authorises the employer to conduct an initial consultation with the immigration authority on behalf of the foreign skilled worker. The employer can then conclude an agreement with the foreigners authority on the implementation of the procedure and hands over all the necessary applications and documents for this purpose. In the next step, the foreigners authority checks the recognition of the foreign qualifications.

Federal Employment Agency

The Federal Employment Agency has to approve the deployment of the foreign skilled worker in Germany, so that it initiates the approval procedure after the foreigners authority has checked it.

If the Federal Employment Agency remains inactive for one week or does not notify otherwise, the consent is deemed to have been granted.

Foreigners' Registration Office

If the Federal Employment Agency has approved the assignment and all requirements have been met, the Foreigners' Registration Office then hands over the preliminary approval to the employer. The employer then forwards this to the foreign skilled worker in the third country.

German representation abroad

When booking an appointment for the issuance of a visa, the German skilled worker indicates that he or she has received prior approval. This makes it possible for the German diplomatic mission or consular post to make an appointment for issuing the visa within three weeks.

Registration office

After the skilled worker has entered Germany, he/she must register with the registration office of his/her place of residence within two weeks of moving in.

The registration is necessary, among other things, for applying for a residence permit at the Aliens' Registration Office, obtaining a tax ID or also for registering at school if the professional has school-age children.

Conclusion

However, successful onboarding is not yet complete once the preparations have been made and the employee has started work. Both the company and the employee should be aware that it is a process that also requires supportive measures beyond the start of work.

Supportive measures in this regard might include offering further training, conducting staff appraisals and promoting team building.

Furthermore, it is a good idea to provide the foreign employee with a mentor and to hold feedback discussions in which the company should also actively ask for further support.

+ + +

Chapter Four

The General Data Protection Regulation

THE GENERAL DATA PROTECTION REGULATION

Prof. Dr. Christiane Trüe LL.M.
City University of Applied Sciences,
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

- Regulation = directly applicable in the whole of the EU
- 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

- Territorial: EU – or EU-related
 - Processing in context with activities in EU
 - Processing regarding data subjects in EU
 - regardless of where processing takes place
- Substantive: all processes relating to personal data
 - Not: anonymous/non personal data, e.g. machine data
 - Ambit including individual piece of data up to commercial ,Big Data‘

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

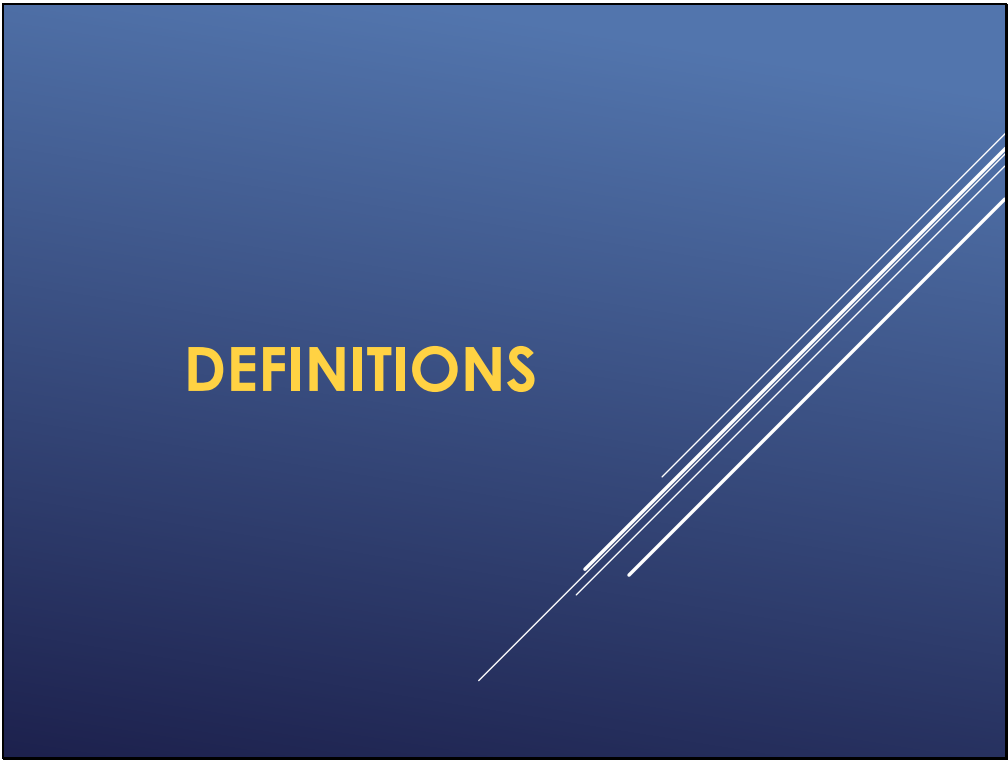
11

SCOPE OF APPLICATION OF GDPR

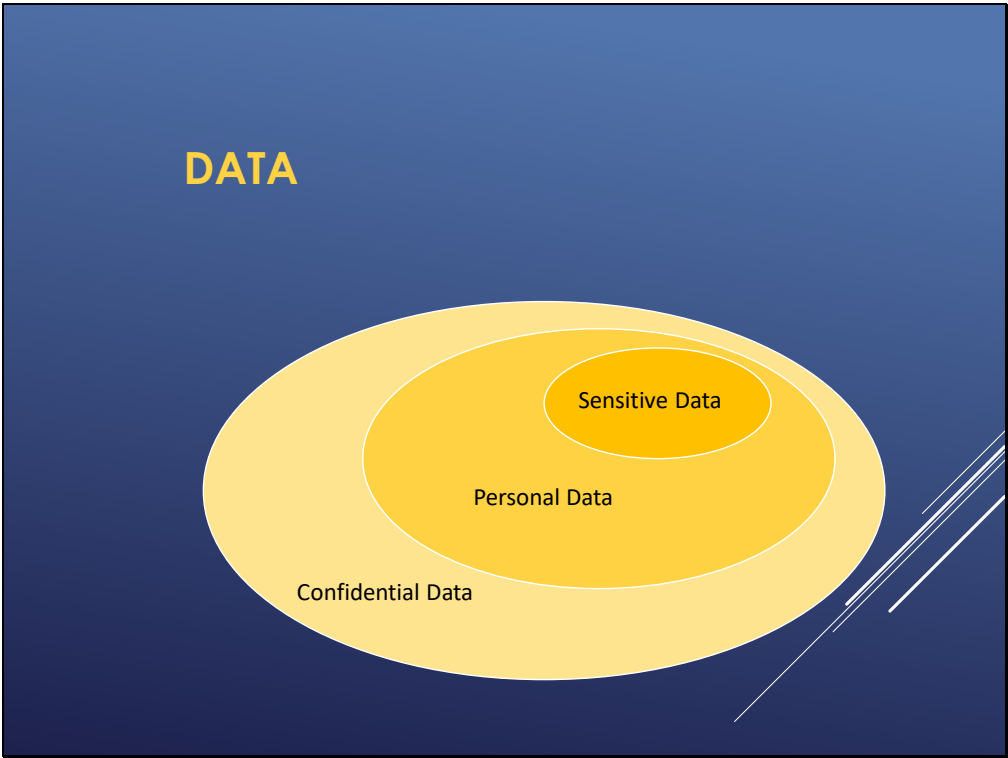
Article 3 Territorial scope

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

BIOMETRIC DATA

- facial recognition
- fingerprints
- voice recognition
- iris scanning
- palmprint verification
- retina recognition
- ear shape recognition

HEALTH DATA

- patient medical history
- data on disability
- illnesses,
- medical diagnosis,
- medical treatment,
- medical opinions
- fitness tracker data

GENETIC DATA

- 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

CONFLICTS OF RIGHTS & INTERESTS

23

CONFLICTING BASIC RIGHTS / HUMAN RIGHTS

Privacy/data protection
vs.
Information
Commercial Activity
Free Flow of data in the internal market
Academic Research

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 regarding more serious violations (listed)
- 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.
City University of Applied Sciences,
Bremen

Counsel to Herfurth & Partner
Hannover / Brussels

truee@herfurth.de



Chapter Five

Data Protection and international business:
Standard Contractual Clauses for trade with third countries



1



2

Agenda

- ✓ Introduction
 - Data protection in the EU
 - Third country transfer of personal data
- ✓ The new Standard Contractual Clauses
 - General information
 - Structure of new SCCs
 - Use of new SCCs
 - Newly introduced obligations
 - Implications for practice
- ✓ Summary
- ✓ Useful links

3

Introduction

4

Data protection in the EU

Herfurth & Partner | Alliuris Summer School 2022

5

5




Source: <https://gazeleconsulting.org/10-gdpr-memes-that-will-make-you-cry-with-laughter/>

Herfurth & Partner | Alliuris Summer School 2022

6

6




Data protection in the EU

Herfurth & Partner | Alliuris Summer School 2022

7

7



Data protection in the EU

- General Data Protection Regulation (GDPR), applicable as of May 25th, 2018

Herfurth & Partner | Alliuris Summer School 2022

8

8

alliuris

A regulation is a binding legislative act by the EU. It must be applied in its entirety by all Member States.

Data protection in the EU

- General Data Protection Regulation (GDPR), applicable as of May 25th, 2018

Herfurth & Partner | Alliuris Summer School 2022

9

9

alliuris

A regulation is a binding legislative act by the EU. It must be applied in its entirety by all Member States.


Data protection in the EU

- General Data Protection Regulation (GDPR), applicable as of May 25th, 2018
- GDPR lays down rules for the processing of personal data

Herfurth & Partner | Alliuris Summer School 2022

10

10



Data protection in the EU


- General Data Protection Regulation (GDPR), applicable as of May 25th, 2018
- GDPR lays down rules for the processing of personal data
- General rule: Processing only lawful, when explicitly allowed by legal basis (Art. 6 and 9 GDPR)

A regulation is a binding legislative act by the EU. It must be applied in its entirety by all Member States.

Herfurth & Partner | Alliuris Summer School 2022

11

11



Data protection in the EU

- General Data Protection Regulation (GDPR), applicable as of May 25th, 2018
- GDPR lays down rules for the processing of personal data
- General rule: Processing only lawful, when explicitly allowed by legal basis (Art. 6 and 9 GDPR)
- GDPR is effective in all EU Member States → processing and transfer of personal data within EU unproblematic

A regulation is a binding legislative act by the EU. It must be applied in its entirety by all Member States.

Herfurth & Partner | Alliuris Summer School 2022

12

12

alliuris

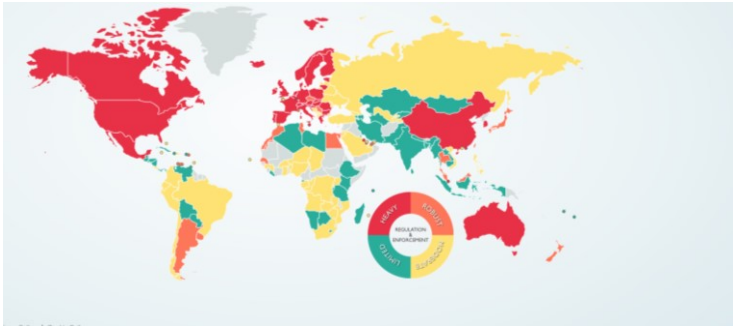
Third country transfer of personal data

Herfurth & Partner | Alliuris Summer School 202213

13

alliuris

Third country transfer of personal data



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

Herfurth & Partner | Alliuris Summer School 202214

14

Third country transfer means a transfer to countries outside the EU.

alliuris

Third country transfer of personal data

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

Herfurth & Partner | Alliuris Summer School 2022

15

15

alliuris

Third country transfer of personal data

Herfurth & Partner | Alliuris Summer School 2022

16

16

alliuris

Third country transfer of personal data

Legal basis for data processing

Lauwfulness of processing

processing of personal data as such lawful

legal basis Art. 6 and 9 GDPR

Herfurth & Partner | Alliuris Summer School 2022

17

17

alliuris

Third country transfer of personal data

Legal basis for data processing + Legal basis for third country transfer

Lauwfulness of processing

processing of personal data as such lawful

legal basis Art. 6 and 9 GDPR

and

Existence of an adequacy decision

third country ensures adequate level of data protection (Art. 45 GDPR) = safe third countries

transfer needs no further authorisation

currently 14 countries, e.g. Argentina, Japan, Republic of Korea, UK

or

Provision of appropriate safeguards

no adequacy decision = unsafe third countries

controller or processor provides appropriate safeguards (Art. 46 GDPR)

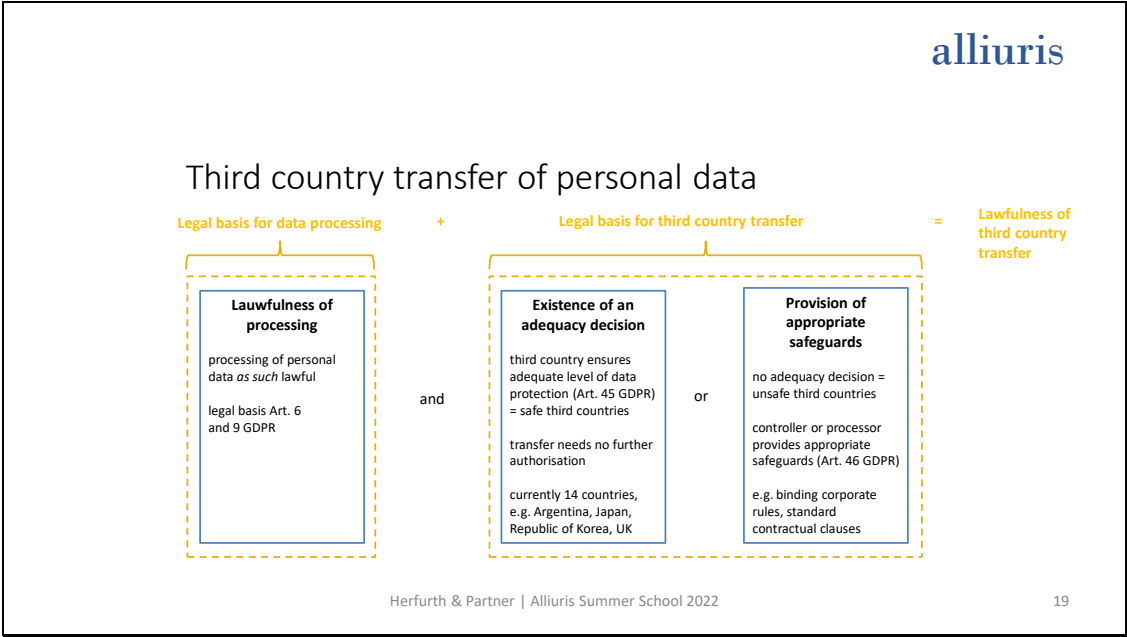
e.g. binding corporate rules, standard contractual clauses

Herfurth & Partner | Alliuris Summer School 2022

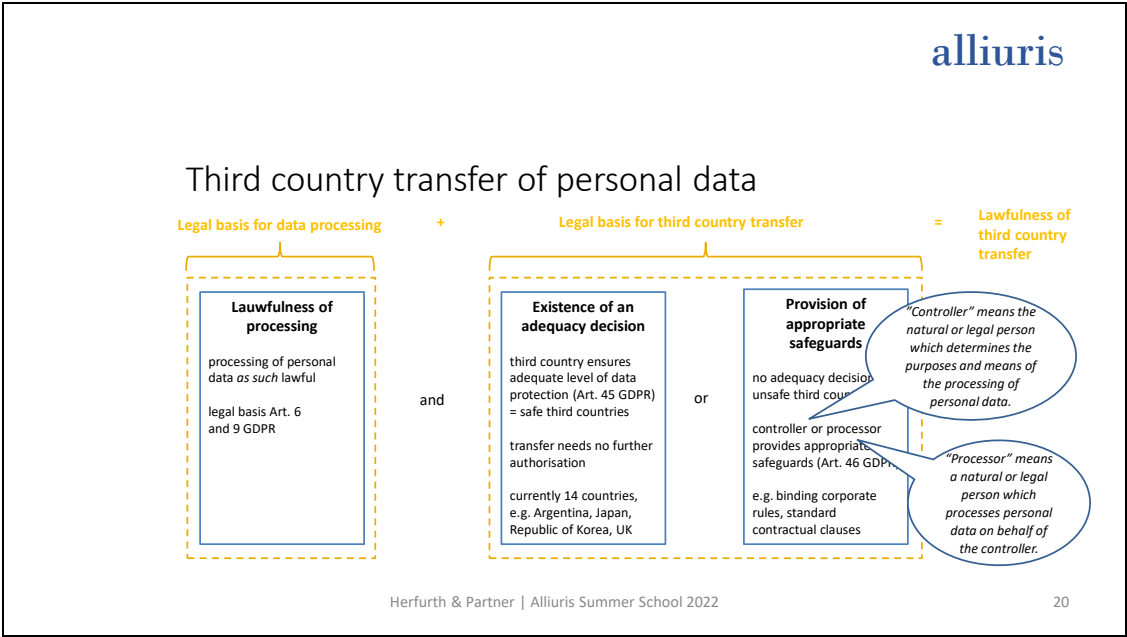
18

18

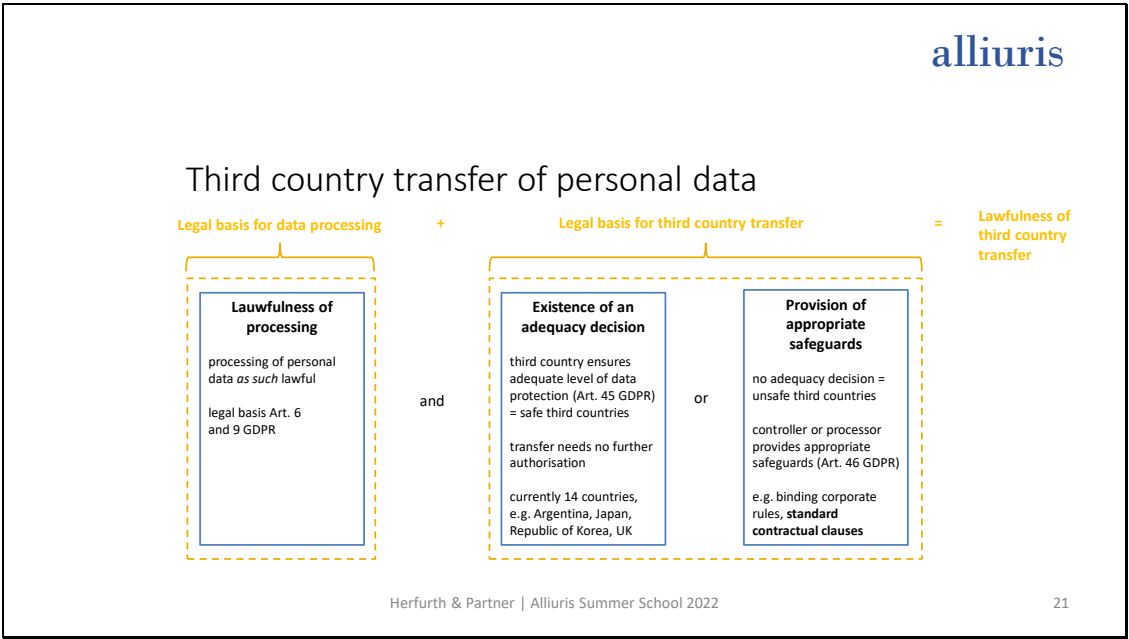
157



19



20




21

The new Standard Contractual Clauses

Herfurth & Partner | Alliuris Summer School 2022

22

22




General information

Herfurth & Partner | Alliuris Summer School 2022

23

23



General information

- SCCs are model contracts approved by the Commission
- applicable to third country transfer of personal data
- aim to provide contractual clauses which are fair and in accordance with applicable law
- new SCCs shall provide more legal certainty and flexibility for data transfers to third countries
- previous SCCs based on Data Protection Directive 95/46/EG from 1995
↔ new SCCs adaption to new GDPR from 2016
- new SCCs published on June 4th, 2021 by Commission

Herfurth & Partner | Alliuris Summer School 2022

24

24




Structure of new SCCs

Herfurth & Partner | Alliuris Summer School 2022

25

25



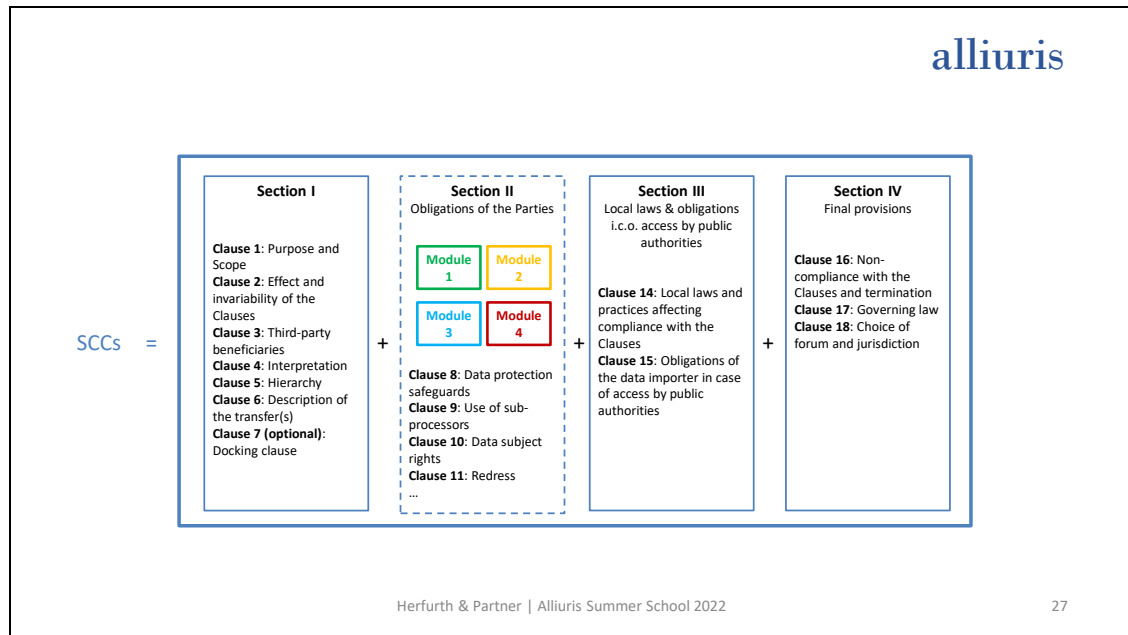
Structure of new SCCs

- one document that is modular in structure
- different modules cover different data transfer scenarios
- rules which apply to all scenarios and rules which apply to specific scenarios:
 - Section I** (i.a. "Purpose and Scope", "Effect and Invariability of the Clauses")
→ all scenarios
 - Section II** ("Obligations of the parties") → specific scenarios (modular)
 - Section III** ("Local laws and obligations in case of access by public authorities") → all scenarios
 - Section IV** ("Final provisions") → all scenarios

Herfurth & Partner | Alliuris Summer School 2022

26

26



27

alliuris

Scenarios under the new SCCs

- Module 1 – C2C: data transfer from EU controller to third country controller
- Module 2 – C2P: data transfer from EU controller to third country processor
- Module 3 – P2P: data transfer from EU processor to third country processor
- Module 4 – P2C: data transfer from EU processor to third country controller

Herfurth & Partner | Alliuris Summer School 2022 28

28

Module 1 – C2C

- data transfer from EU controller to third country controller
- was already covered by old SCCs

29

Module 2 – C2P

- data transfer from EU controller to third country processor
- was already covered by old SCCs
- however, under new SCCs, no additional data processing agreement necessary anymore (Art. 28 GDPR asks for such an agreement, Module 2 now covers this requirement)

30

Module 3 – P2P

- data transfer from EU processor to third country (sub-)processor
- introduced by new SCCs
- under old SCCs, if EU processor wanted to use third country (sub-)processor, the controller had to conclude data processing agreement with (sub-)processor
- under new SCCs, not necessary to conclude additional data processing agreement anymore as the requirement is fulfilled by new SCCs (similar to Module 2)
- leads to reduction of organisational workload for controller

Herfurth & Partner | Alliuris Summer School 2022

31

31


Module 4 – P2C

- data transfer from EU processor to third country controller, that is data retransfer
- introduced by new SCCs
- necessary to conclude additional data processing agreement (no fulfilment of requirement of Art. 28 GDPR by Module 4)
- discussed by practitioners, e.g. some argued that it feels “strange” that EU processor is subject to instructions of controller located in a third country where the GDPR does not apply

Herfurth & Partner | Alliuris Summer School 2022

32


32



Use of new SCCs

Herfurth & Partner | Alliuris Summer School 202233

33



Use of new SCCs

- can be concluded as individual contract or part of comprehensive contract
- must not be changed by the parties, otherwise legally void
- however, SCCs must be completed by the parties, e.g. in Clause 17 parties must choose the applicable law
- Clause 7 introduces an optional “docking clause” which allows third parties to join the contract anytime with consent of contracting parties
→ flexibility

Herfurth & Partner | Alliuris Summer School 202234

34

Use of new SCCs

L 199/56

EN

Official Journal of the European Union

7.6.2021

MODULE FOUR: Transfer processor to controller
These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of _____. (specify country).

Clause 18
Choice of forum and jurisdiction

MODULE ONE: Transfer controller to controller
MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
(b) The Parties agree that those shall be the courts of _____. (specify Member State).
(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
(d) The Parties agree to submit themselves to the jurisdiction of such courts.

MODULE FOUR: Transfer processor to controller
Any dispute arising from these Clauses shall be resolved by the courts of _____. (specify country).

35

Use of new SCCs

modules

L 199/56

EN

Official Journal of the European Union

7.6.2021

MODULE FOUR: Transfer processor to controller
These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of _____. (specify country).

Clause 18
Choice of forum and jurisdiction

MODULE ONE: Transfer controller to controller
MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
(b) The Parties agree that those shall be the courts of _____. (specify Member State).
(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
(d) The Parties agree to submit themselves to the jurisdiction of such courts.

MODULE FOUR: Transfer processor to controller
Any dispute arising from these Clauses shall be resolved by the courts of _____. (specify country).

36

alliuris

Use of new SCCs

modules

L 1199/56ENOfficial Journal of the European Union7.6.2021

MODULE FOUR: Transfer processor to controller

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of _____. (specify country).

Clause 18

Choice of forum and jurisdiction

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of _____. (specify Member State).

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

MODULE FOUR: Transfer processor to controller

Any dispute arising from these Clauses shall be resolved by the courts of _____. (specify country).

to be filled in by the contracting parties

Herfurth & Partner | Alliuris Summer School 202237

37

alliuris

Newly introduced obligations

Herfurth & Partner | Alliuris Summer School 202238

38

167

Newly introduced obligations

- Transfer Impact Assessment (TIA) (Clause 14 para. a-c)
 - data exporter and data importer have obligation to verify that third country has level of data protection equivalent to GDPR
 - likelihood of third country authority accessing personal data
- ensuring the level of data protection (Clause 14 para. f)
 - if data importer can no longer maintain level of data protection in third country, data exporter must take appropriate measures to restore it (so-called TOMs)

39

*"Data exporter"
means the entity
that transfers
personal data to
third country.*

Newly introduced obligations

*"Data importer"
means the entity in
third country
receiving personal
data.*

- Transfer Impact Assessment (TIA) (Clause 14 para. a-c)
 - data exporter and data importer have obligation to verify that third country has level of data protection equivalent to GDPR
 - likelihood of third country authority accessing personal data
- ensuring the level of data protection (Clause 14 para. f)
 - if data importer can no longer maintain level of data protection in third country, data exporter must take appropriate measures to restore it (so-called TOMs)

40

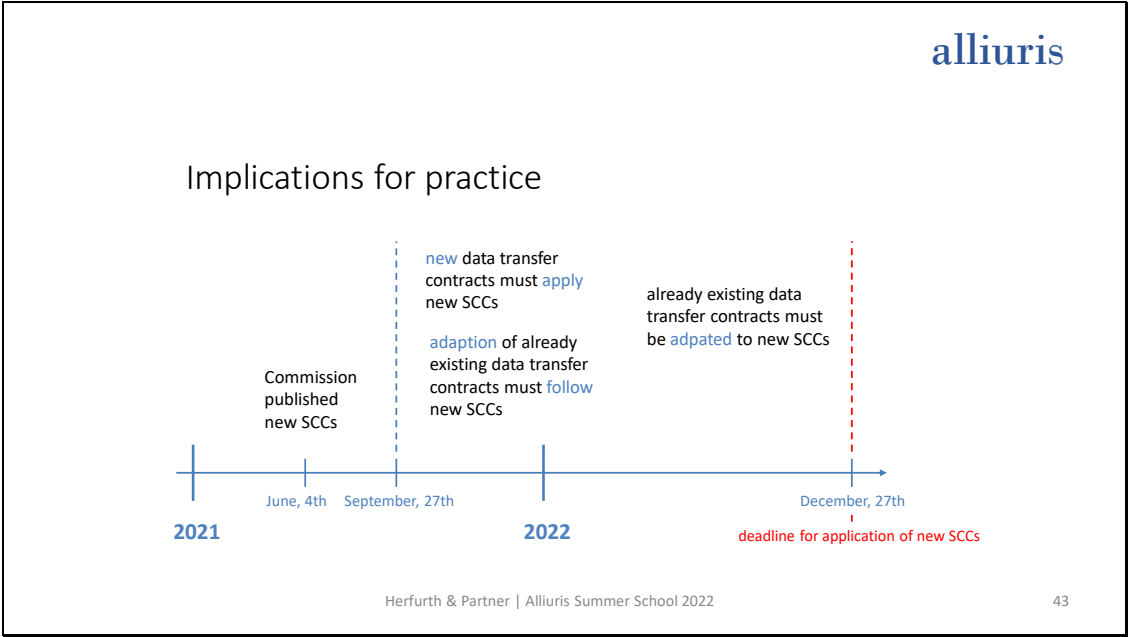
Newly introduced obligations

- extensive documentation requirements (Clause 14 para. d)
 - data exporter and data importer must comply with extensive documentation requirements, e.g. on TIA
 - on request of responsible data protection authority, documents must be made available to authority
- if level of data protection equivalent to GDPR does not exist or cannot be reached in third country, transfer is **not allowed**

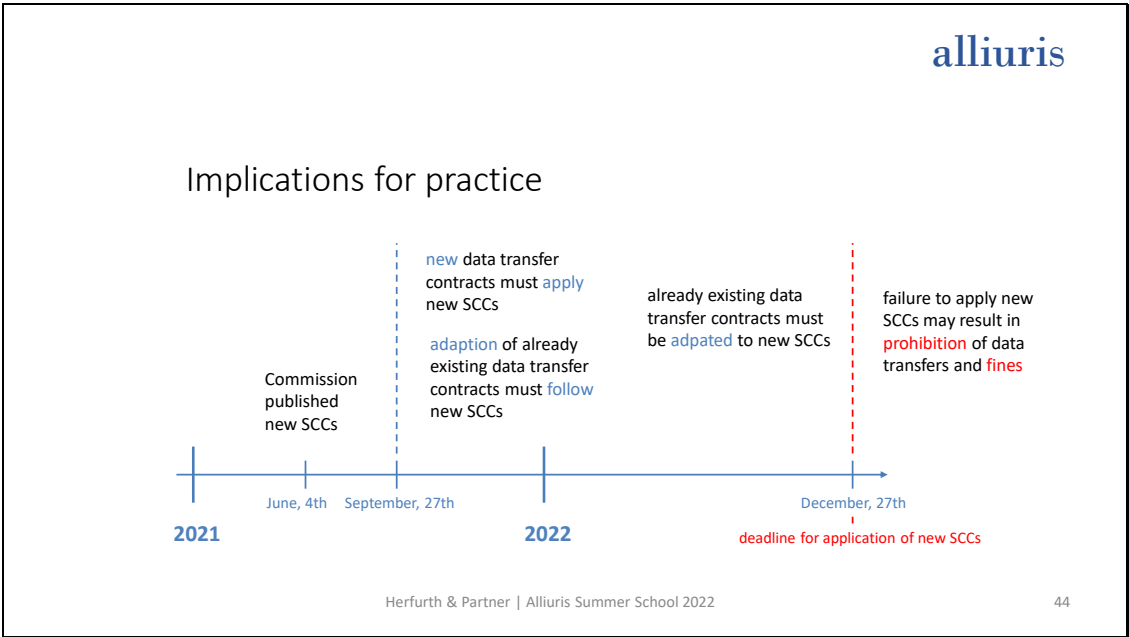
41

Implications for practice

42




43



44


alliuris

Implications for practice: Question 

Herfurth & Partner | Alliuris Summer School 202245

45

alliuris


Implications for practice: Question 

Do you think personal data can be transferred from the EU to the USA, China and Brazil?

Herfurth & Partner | Alliuris Summer School 202246

46

alliuris

Implications for practice: Question 


Do you think personal data can be transferred from the EU to the USA, China and Brazil?

If yes, what are the requirements?

Herfurth & Partner | Alliuris Summer School 2022 47

47

alliuris

Implications for practice: Question 

Do you think personal data can be transferred from the EU to the USA, China and Brazil?

If yes, what are the requirements?

Write in the chat!

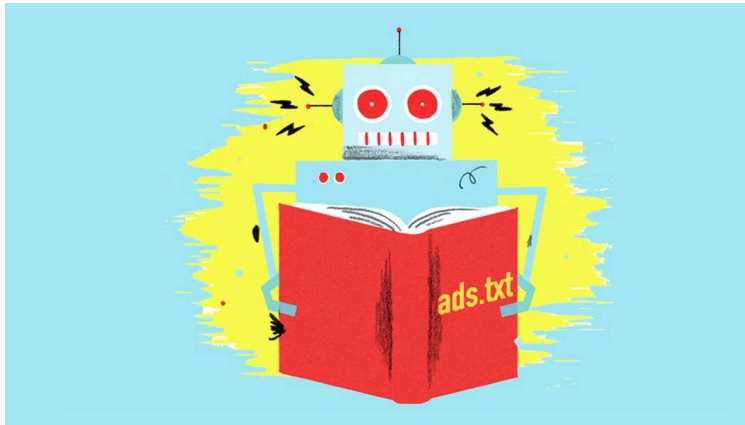
Herfurth & Partner | Alliuris Summer School 2022 48

48

Implications for practice: Answer

- Transfer of personal data to the USA, China and Brazil?
 - No adequacy decisions for the USA, China and Brazil
 - officially considered unsafe third countries by EU
 - transfer only based on SCCs
 - existing data protection laws considered within TIA
 - concerning USA, CJEU has declared Safe Harbor Principles and Privacy Shield null and void, but new data protection agreement is in progress

49



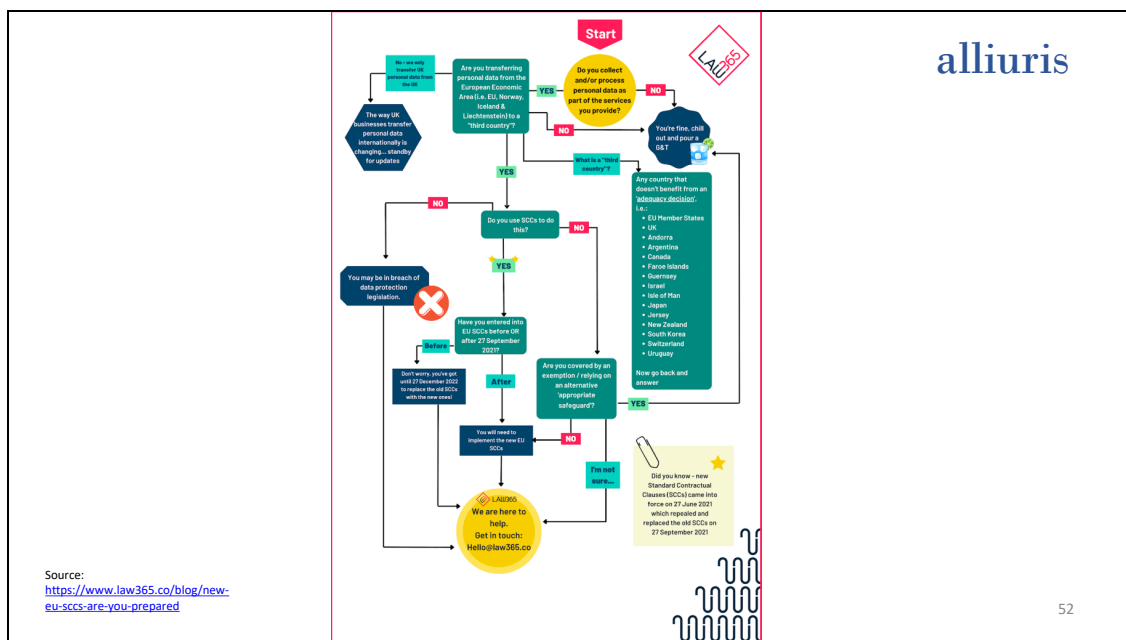
Source: <https://digiday.com/media/wtf-what-are-standard-contractual-clauses-gdpr/>

50


Summary


Herfurth & Partner | Alliuris Summer School 2022

51



52





Top 3 things to remember... 

Herfurth & Partner | Alliuris Summer School 2022

53

53



Top 3 things to remember... 

1. New SCCs have **modular structure** which covers C2C, C2P, P2P and P2C data transfers.

Herfurth & Partner | Alliuris Summer School 2022

54

54

Top 3 things to remember...



1. New SCCs have **modular structure** which covers C2C, C2P, P2P and P2C data transfers.
2. New SCCs introduce **new obligations** for controller and processor.

55

Top 3 things to remember...



1. New SCCs have **modular structure** which covers C2C, C2P, P2P and P2C data transfers.
2. New SCCs introduce **new obligations** for controller and processor.
3. All data transfer contracts must be compliant with new SCCs **by December, 27th, 2022.**

56

Useful links

Herfurth & Partner | Alliuris Summer School 2022

57

57

alliuris

- General information on data protection in the EU:
 - <https://gdpr.eu/>
 - https://ec.europa.eu/info/law/law-topic/data-protection_en
- General information by EU on SCCs:
 - https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en
- Text of the new SCCs (available in 24 official languages of EU):
 - https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en

Herfurth & Partner | Alliuris Summer School 2022

58

58

alluris

Antonia Herfurth

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

Mail herfurth_antonia@herfurth.de

Web www.herfurth.de



Herfurth & Partner | Alluris Summer School 2022

59

59

alluris

INTERNATIONAL

60

178

Materials | Compact

The new Standard Contractual Clauses of the EU

Antonia Herfurth, Attorney at law in Munich and Hanover

May 2022

On June 4, 2021, the European Commission issued new Standard Contractual Clauses (SCCs) for international data transfers.¹ The new SCCs are an adaptation to the General Data Protection Regulation, which came into force in 2018. Since September 27, 2021, new data transfer contracts and contract amendments may only be concluded using the new SCCs. By December 27, 2022, all old contracts must be adapted to the new SCCs. The old SCCs, which were still based on the Data Protection Directive 95/46/EC from 1995 and were up to 17 years old, have been replaced. If the old SCCs are continued to be used, the transfer of data can be prohibited and a fine can be imposed.

With the new SCCs, the Commission hopes for more legal certainty and flexibility in data transfers to third countries. For the parties, however, the data transfer will also become more complicated.

Overview

The processing of personal data must always be based on a legal basis, such as the consent of the data subject. If personal data are transferred to non-EU countries (third countries), this requires a further legal basis. If data crosses borders within the EU, the transfer is always permissible because the data protection level of the GDPR applies. Cross-border transfers to third countries where the GDPR does not apply, but on which the Commission has reached an adequacy decision, are also permissible. According to the Commission, they have an adequate level of data protection comparable to that of the GDPR and are considered “safe third countries” (e.g. Canada, Japan, UK). Third countries for which there is no adequacy decision are classified as “unsafe third countries”. The transfer of personal data is only permitted if the controller or processor has provided appropriate safeguards, these include SCCs. SCCs are model contracts approved by the Commission.

¹ The new SCCs are available under https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj.

Structure

The new SCCs for the transfer of personal data to third countries consist of one document with a modular structure. The four modules cover different transfer scenarios. Section I of the SCCs (e.g. “Purpose and Scope”, “Effect and Invariability of the Clauses”), Section III (“Local laws and practices affecting compliance with the Clauses”) and Section IV (“Final provisions”) are essentially applicable to all modules. The new SCCs include clauses on liability, applicable law and jurisdiction.

While the old SCCs only covered two scenarios, the new SCCs cover the following data transfer scenarios:

Module 1: C2C

Module 1 covers the transfer of data from a controller in the EU to a controller in a third country (*Controller to Controller*). The old SCCs already covered this situation.

Module 2: C2P

Module 2 covers the transfer of data from a controller in the EU to a processor in a third country (*Controller to Processor*). This situation was also covered by the old SCCs. However, the new SCCs have the advantage that controllers no longer have to conclude a separate processing agreement with processors in a third country. According to Article 28 of the GDPR, the processing of data by a processor may only take place on the basis of a (processing) agreement. Module 2 now covers this requirement.

Module 3: P2P

Module 3 covers the situation where a processor in the EU transfers data to a (sub-)processor in a third country (*Processor to Processor*). Processors in the EU can therefore use sub-processors outside the EU. This constellation was newly introduced. If a processor wanted to use a sub-processor under the old SCCs, it was necessary for the controller itself to conclude SCCs with the sub-processor. The processor could not independently use a sub-processor even though there was a processing agreement between the processor and the controller. This has now changed. Module 3 is similar to Module 2, with the consequence that parties no longer need to conclude a separate (sub-)processing agreement. This reduces the organisational burden on the controller.

Module 4: P2C

The scenario under Module 4 is also new and covers the (re-)transmission of data from a processor in the EU to a controller in a third country (*Processor to Controller*). Unlike Modules 2 and 3, Module 4 does not meet the requirements of Article 28 of the GDPR, i.e. separate data processing agreements must be concluded.

Individual questions regarding this module and its relevance for practice are discussed. For example, some data protection experts have commented that it feels “strange” that the processor is subject to the instructions of a controller located in a third country where the GDPR does not apply.

Use

The SCCs can be concluded as an individual contract or as part of a comprehensive contract. Like the old SCCs, they may not be changed. If the SCCs are changed, they are null and void. In particular, as part of a comprehensive contract, no further clauses may be included which contradict the SCCs or impair the fundamental rights or freedoms of the person concerned. If contractual or GTC clauses contradict the SCCs, the SCCs take precedence. However, the SCCs need to be supplemented in some parts. In Article 17, the parties must specify which Member State's law should apply to the SCCs, and in Module 3, the parties can choose between two options. In Article 18, the parties have to indicate which Member State's court should be competent. Furthermore, the Annex has to be filled in with information on the contracting parties, a description of the data transfer, etc.

Article 7 introduces an optional docking clause. According to this clause, an entity that is not a party to the SCCs may join them at any time with the consent of the contracting parties. The accession is done by filling in the Annex and signing Annex I.A. of the Implementing Decision (EU) 2021/914 which introduced the new SCCs. The docking clause allows for the accelerated accession of third parties, i.e. more flexibility.

Newly introduced obligations

As a result of the CJEU's Schrems II ruling in 2020, the SCCs introduce new obligations for data exporters and data importers. “Data exporter” means the person, authority, agency and other body in the EU that transfers personal data to a third country. “Data importer” means the entity in a third country that receives personal data.

Mandatory Transfer Impact Assessment

The new SCCs oblige data exporters and importers to verify whether the third country has a level of data protection that complies with the GDPR. In addition, the likelihood of third country au

authorities accessing the data can be taken into account. This so-called Transfer Impact Assessment (TIA) must be carried out for each individual data transfer. If the third country does not have an adequate level of data protection, the data exporter must attempt to achieve this level through additional technical security measures. Since both the assessment of third countries and the identification of appropriate additional measures are complex, the European Data Protection Committee (EDSA) adopted Recommendations on June 18, 2021, to assist both parties in six steps.² If local rules and practices mean that the SCCs cannot be definitively complied with, the data exporter may not transfer personal data to the third country. The SCCs do not bridge this gap.

Data importers must provide the data exporter with relevant information for the assessment. If they have reason to believe that the level of protection is changing, they must notify the data exporters without delay.

Obligations to ensure the level of protection

If the data exporter has reason to believe that the data importer in the third country can no longer comply with the level of data protection, he must remedy the situation without delay. To this end, the data exporter must take appropriate measures, such as technical and organisational measures to ensure security and confidentiality, so-called TOMs. The EDSA has listed concrete examples of suitable TOMs in Annex 2 of its Recommendation. If the level of data protection cannot be maintained, the data exporter must suspend the data transfer. In this case, he is entitled to terminate the data transfer contract.

The data importer has a duty to notify if an authority requests him to disclose personal data. If the data importer is prohibited from notifying the data exporter and, if applicable, the data subject, due to the regulations of the third country, he must endeavour to have the prohibition on notification lifted. In addition, the data importer must check the legality of the official disclosure request and, if necessary, challenge it.

Extensive documentation obligations

Both the data exporter and the data importer are subject to extensive documentation obligations. For example, the TIA and all documents relating to official requests for the disclosure of personal data must be documented. The information must be made available to the competent data protection authority upon request.

² The Recommendations of the EDSA are available under: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en.

Data transfers to the USA, China and Brazil

Currently, data transfers to the USA, China and Brazil are only permitted on the basis of SCCs. However, after the CJEU annulled both the Safe Harbor Agreement and the Privacy Shield, the EU and the USA are seeking a new agreement for data transfers. Brazil and China have enacted new data protection laws that came into force in 2020 and 2021 respectively. Although both laws are intended to establish a strong level of data protection, the EU still considers both countries to be insecure third countries. However, the data protection laws can be taken into account in the TIA.

Recommendation for action

New contracts may only be concluded using the new SCCs, old contracts must be adapted by December 27, 2022. The following steps are recommended to ensure that data transfers to third countries continue to be GDPR compliant. The steps should be implemented as early as possible, as they can be extremely time-consuming:

1. Identification of existing contracts and adaptation to new SCCs.
2. Conclusion of new contracts only with the use of new SCCs.
3. Checking the legal situation and practice of the third country, i.e. carrying out a TIA. No data transfer to a third country without ensuring a level of data protection that complies with the GDPR.
4. Documentation of correspondence, measures, considerations, etc.

+ + +

Chapter Six

The new EU Regulation on competition restrictions in vertical markets (VBER)



1



2

Agenda

- Competition Law in the EU
- The new Vertical Block Exemption Regulation
- Main Changes
- Real case example
- Quiz

3

Competition Law in the EU

4

EU: exclusive competence in competition law

- The Lisbon Treaty of 2007 (in force since 2009) establishes the exclusive competence of the EU for competition rules within the internal market; Art. 3 of TFEU (**Treaty on the Functioning of the European Union**)
- This means that in these cases the EU, and not the member states, legislates on competition matters and concludes international trade agreements
- Member states are further competent for national competition



5

Main policy areas

- Cartels, control of collusion and other anti-competitive practices: art. 101 TFEU (**Treaty on the Functioning of the European Union**)
- Market dominance, prevention of abuse of firms' dominant market positions: art. 102 TFEU
- Control of proposed mergers, acquisitions and joint ventures: European Union merger law
- State aid, control of direct and indirect aid given by Member States of the European Union to companies: art. 107 TFEU



6

Main policy areas

- Cartels, control of collusion and other anti-competitive practices: art. 101 TFEU
- Market dominance, prevention of abuse of firms' dominant market positions: art. 102 TFEU
- Control of proposed mergers, acquisitions and joint ventures: European Union merger law
- State aid, control of direct and indirect aid given by Member States of the European Union to companies: art. 107 TFEU

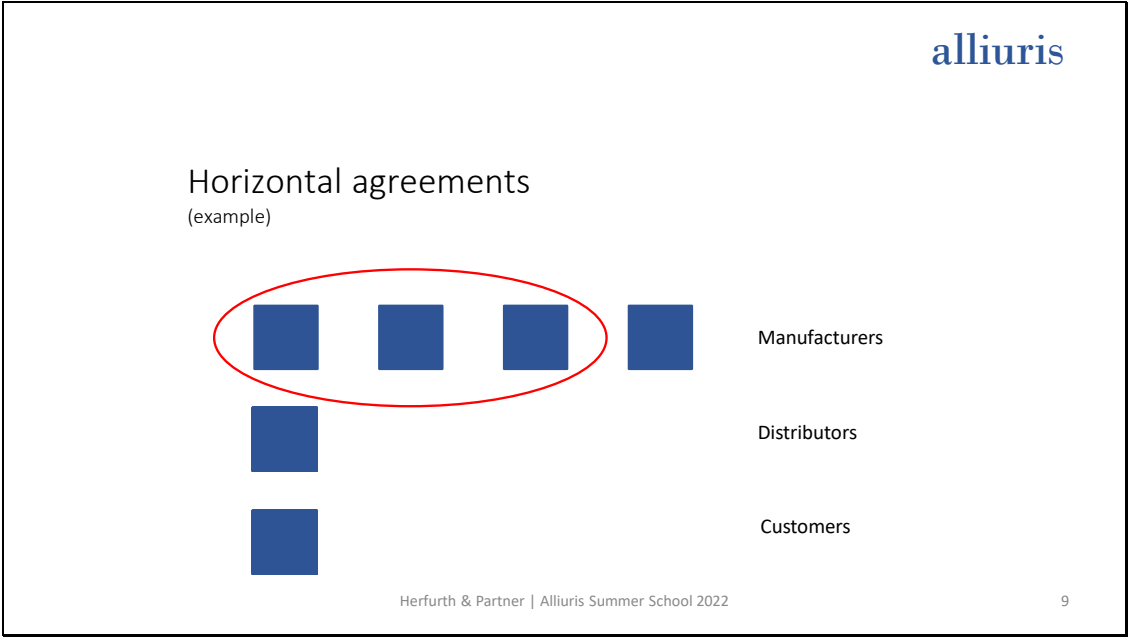


7

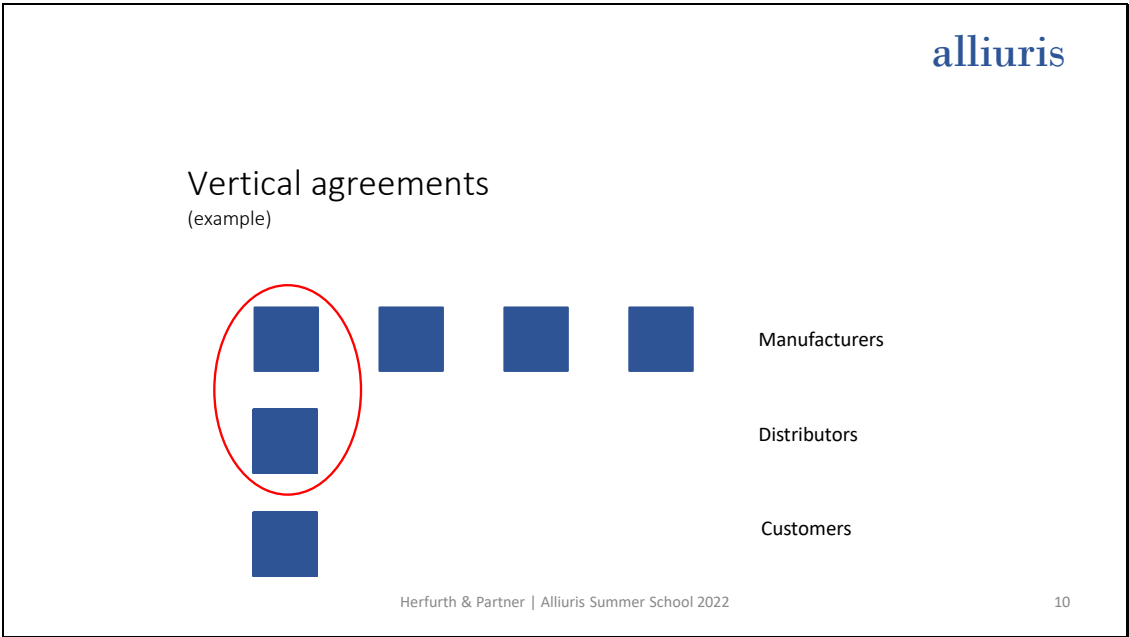
Cartel, collusion, anticompetitive practices: art 101 AEUV

1. The following shall be prohibited as incompatible with the internal market: all agreements between undertakings, decisions by associations of undertakings and concerted practices which may affect trade between Member States and which have as their object or effect the prevention, restriction or distortion of competition within the internal market, and in particular those which:
 - (a) directly or indirectly fix purchase or selling prices or any other trading conditions;
 - (b) limit or control production, markets, technical development, or investment;
 - (c) share markets or sources of supply;
 - (d) apply dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage;
 - (e) make the conclusion of contracts subject to acceptance by the other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of such contracts.
2. Any agreements or decisions prohibited pursuant to this Article shall be automatically void.

8



9



10

alliuris

Vertical agreements

An agent agreement is not a vertical agreement – the agent is in the sphere of the principal

Herfurth & Partner | Alliuris Summer School 2022

11

11

alliuris

Sometimes, agreements are beneficial:

- The EU competition law exempts certain types of agreements from the prohibition of art. 101 (1-2) where there are benefits for consumers

Herfurth & Partner | Alliuris Summer School 2022

12

12

Art. 101 (3) TFUE

3. The provisions of paragraph 1 may, however, be declared inapplicable in the case of:

- ✓ any agreement or category of agreements between undertakings,
- ✓ any decision or category of decisions by associations of undertakings,
- ✓ any concerted practice or category of concerted practices,

which contributes to improving the production or distribution of goods or to promoting technical or economic progress, while allowing consumers a fair share of the resulting benefit, and which does not:

- (a) impose on the undertakings concerned restrictions which are not indispensable to the attainment of these objectives;
- (b) afford such undertakings the possibility of eliminating competition in respect of a substantial part of the products in question.

13

Problem

- Individual assessment is needed
- Lack of legal certainty



14

Block exemption regulations

Pursuant to art 103 TFEU and with the purpose of increasing legal certainty, the European Commission issues block exemption regulations that specify the conditions under which **certain types of agreements** are exempted from the prohibition of restrictive agreements laid down in Article 101(1) TFEU



15

Art. 103 TFEU

1. The appropriate regulations or directives to give effect to the principles set out in Articles 101 and 102 shall be laid down by the Council, on a proposal from the Commission and after consulting the European Parliament.
2. The regulations or directives referred to in paragraph 1 shall be designed in particular:
 - (a) to ensure compliance with the prohibitions laid down in Article 101(1) and in Article 102 by making provision for fines and periodic penalty payments;
 - (b) to lay down detailed rules for the application of Article 101(3), taking into account the need to ensure effective supervision on the one hand, and to simplify administration to the greatest possible extent on the other;

....

16


The EU block exemption regulations

- Block Exemptions - **horizontal** agreements
- Block Exemptions - **vertical** agreements
- Licensing Agreements for the transfer of **technology**
- Legislation on competition in the **agricultural** and food sector
- Legislation on competition in the **insurance** sector
- Legislation on competition in the **postal** services sector
- Legislation on competition in **professional** services
- Legislation on competition in the **telecommunications** sector
- Legislation on competition in the **transport** sector



17

The EU block exemption regulations

- Block Exemptions - horizontal agreements
- **Block Exemptions - vertical agreements** 
- Licensing Agreements for the Transfer of Technology
- Legislation on competition in the agricultural and food sector
- Legislation on competition in the insurance sector
- Legislation on competition in the postal services sector
- Legislation on competition in professional services
- Legislation on competition in the telecommunications sector
- Legislation on competition in the transport sector

18

The New Vertical Block Exemption Regulation

Herfurth & Partner | Alliuris Summer School 2022

19

19

The new EU Regulations

- **New:** “Commission Regulation (EU) 2022/720 on the application of Article 101 (3) of TFEU (the Treaty on the Functioning of the European Union) to categories of vertical agreements and concerted practices”, and new “Guidelines on Vertical Restraints”, entered into force on 1 June 2022
- Short: Vertical Block Exemption Regulation (“**VBER**”) and “**Vertical Guidelines**”
- Substitute the old VBER, in force since 2010
- Several important changes for the treatment of distribution agreements under EU competition law



Herfurth & Partner | Alliuris Summer School 2022

20

20

Parallel: the new UK Regulations

- UK’s Vertical Agreements Block Exemption Order entered into force on 1 June 2022
- Interpretative Guidance (Vertical Agreements Guidelines) published on 12 July 2022
- The U.K. and the EU rules are very similar, but there are some crucial differences both in the letter and the interpretation of the legislation
- In cases where an agreement has an effect in both the U.K. and the EU, it is best to ensure compliance with the most stringent requirements in both pieces of legislation



21

Again:
What are vertical agreements?

Agreements between businesses operating at different level of the production, supply and distribution chain



22

Vertical block exemption

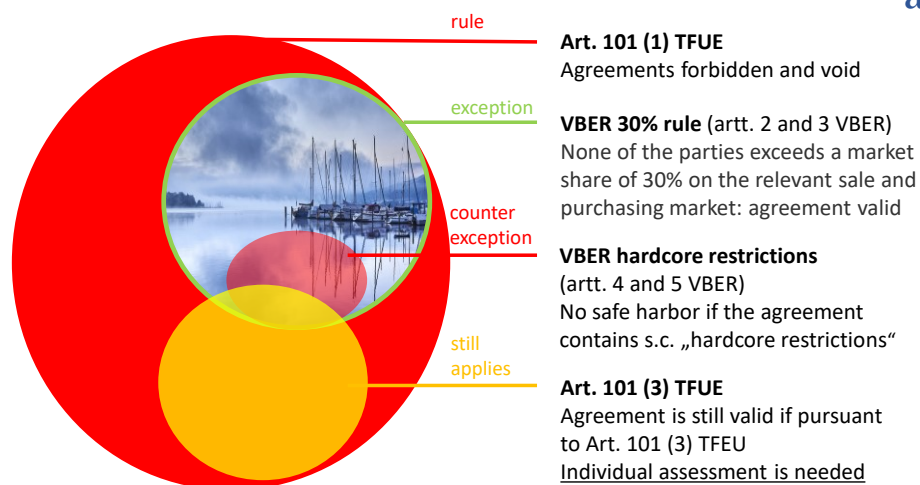
- The new VBER, like the old one, creates a safe harbor exemption from the principle of Article 101 (1) of the Treaty on the Functioning of the Union (TFUE), which forbids agreements, decisions, and concerted practices that are anti-competitive and distort the single market
- According to the VBER, Art. 101 (1) TFUE does not apply to vertical agreements if none of the parties exceeds a **market share of 30%** on the relevant sale and purchasing market, unless the agreement contains **hardcore restrictions**



Herfurth & Partner | Alliuris Summer School 2022

23


23



Herfurth & Partner | Alliuris Summer School 2022

24

24




Main Changes

Herfurth & Partner | Alliuris Summer School 2022

25

25



Note:

- ✓ The VBER has a very complex structure

exception → counter - exception → counter - counter - exception →

✓ *The purpose of this presentation is not to provide a complete picture of the situation, but only a simplified overview of the contents and main novelties of the new VBER*

Herfurth & Partner | Alliuris Summer School 2022

26

26

Note – color code

- ✓ The contents represented in the **left column** of the tables are covered by the vertical block exemption
- ✓ The contents of the **right column** are excluded. These kinds of agreements are not forbidden altogether, but an individual assessment under art. 101 (3) TFUE is needed
- ✓ The main novelties are written in **green** and in **red**

Included in the block exemption	Excluded from the block exemption
... new	... new

- ✓ Slides concerning the old VBER have a **grey background**

Herfurth & Partner | Alliuris Summer School 2022

27

27

Overview

- Dual distribution (Art. 2(4-6) VBER, Sec. 4.4.3 et seq. Vertical Guidelines)
- Parity obligations (Art. 5(d) VBER, Sec. 6.2.4 et seqq., Sec. 8.2.5 et seqq. Vertical Guidelines)
- Dual pricing (Sec. 6.1.2.1 (209) Vertical Guidelines)
- Online sales restrictions (Art. 4(e) VBER, Sec. 6.1.2 Vertical Guidelines)
- Exclusive distribution (Art. 4(b) VBER, Sec. 4.6.1 et seqq. Vertical Guidelines)
- Selective distribution (Art. 4(c) VBER, Sec. 4.6.2 et seqq. Vertical Guidelines)
- Resale prices (Art. 4(a) VBER, Sec. 6.1.1 Vertical Guidelines)
- Non compete clauses (Art 5 VBER, Sec. 6.2.1 et seqq. Vertical Guidelines)
- Online intermediation providers (Art. 2(6) VBER, Sec. 4.4.4 Vertical Guidelines)

Herfurth & Partner | Alliuris Summer School 2022

28


28

alluris


Dual distribution

(Art. 2 (4-6) VBER)


When a supplier is active both upstream and downstream, it may be in competition with his downstream costumer



supplier



own online store



independent retailers



Herfurth & Partner | Alluris Summer School 2022

29


29

alluris

Dual distribution: old



↓



Included in the block exemption	Excluded from the block exemption
	vertical agreements between competitors
dual distribution agreements	

Herfurth & Partner | Alluris Summer School 2022


30

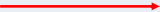
30

alliuris

Dual distribution: **new**

(Art. 2(4-6) VBER, Sec. 4.4.3 et seq. Vertical Guidelines)



Included in the block exemption	Excluded from the block exemption
	vertical agreements between competitors
dual distribution agreements, however: 	Dual distribution agreements relating to the provision of online intermediation services ("OIS") , where the OIS provider (e.g. e-commerce marketplace) also sells goods or services in competition with the companies to which it provides OIS
	Information exchange between the supplier and the buyer which is either: ✓ Not directly related to the implementation of the vertical agreement ✓ Not necessary to improve the production or distribution of the contract goods or services (See „black-white“ list in the Vertical Guidelines)

Herfurth & Partner | Alliuris Summer School 2022

31


31

alliuris

Parity obligations

(Art. 5(d) VBER, Sec. 6.2.4 et seq., and 8.2.5 et seq. Vertical Guidelines)

- Parity obligations (or Most Favoured Nation Clauses – MFNC) demand that a company offers its contracting party the same or better conditions as on other outlets (i.e. other platforms)




Herfurth & Partner | Alliuris Summer School 2022

32

32

Parity obligations: old



alliuris


Included in the block exemption	Excluded from the block exemption
All parity obligations	

Herfurth & Partner | Alliuris Summer School 2022

33

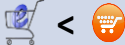



33

Parity obligations: new



alliuris

(Art. 5(d) VBER, Sec. 6.2.4 et seqq., and 8.2.5 et seqq. Vertical Guidelines)

Included in the block exemption	Excluded from the block exemption
	<div>„ Across-platform retail parity obligations“ – „wide parity clauses“, in which an online platforms prevents ist supplier from offering the same product on other retail platforms on better terms or a lower price</div> <div> < </div>
<div>All other parity clauses (i.e. relating to the own sale channel of the supplier).</div> <div> < </div> <div>-----></div>	<div>However, if narrow parity clauses are imposed by platforms covering a significant share of users without evidence of efficiency, the benefit may be withdrawn</div>

Herfurth & Partner | Alliuris Summer School 2022

34




34

alliuris

Dual pricing

(Sec. 6.1.2.1 (209) Vertical Guidelines)

Dual pricing occurs when the same distributor charges different prices for products intended to be sold online and products to be sold in brick-and-mortar stores






Herfurth & Partner | Alliuris Summer School 2022

35

35

alliuris

Dual pricing: old



Included in the block exemption	Excluded from the block exemption
	Dual pricing

Herfurth & Partner | Alliuris Summer School 2022


36


36

NS0

alliuris

Do you think it is fair?







Herfurth & Partner | Alliuris Summer School 2022

37

37

alliuris

Dual pricing: new  \neq 
(Sec. 6.1.2.1 (209) Vertical Guidelines)

Included in the block exemption	Excluded from the block exemption
Dual pricing	

Herfurth & Partner | Alliuris Summer School 2022

38

38

alliuris

Dual pricing: new

(Sec. 6.1.2.1 (209) Vertical Guidelines)

≠

Included in the block exemption	Excluded from the block exemption
Dual pricing	
To be noted:	
<ul style="list-style-type: none"> ✓ Price discrepancies must be reasonably related to the cost difference between online and offline channels 	<ul style="list-style-type: none"> ✓ The difference may not have the object of restricting sales to particular territories or customers, or of preventing the effective use of internet ✓ The supplier may not impose that the retail prices be lower or higher depending on the channel.

Herfurth & Partner | Alliuris Summer School 2022
39

39

alliuris

Online sales restrictions

(Art. 4(e) VBER, Sec. 6.1.2 Vertical Guidelines)

Included in the block exemption	Excluded from the block exemption
	The prevention of the effective use of the internet by buyers, or their costumers, to sell services or goods
<p>Other restrictions may fall within the block exemptions, i.e.:</p> <ul style="list-style-type: none"> ✓ Restrictions intended to ensure the quality of the buyers' online store ✓ Requirements that the buyer operates one or more brick-and-mortar stores and makes a minimum absolute volume of sales offline 	


Herfurth & Partner | Alliuris Summer School 2022
40

40

alliuris

Exclusive distribution

(Art. 4(b) VBER, Sec. 4.6.1 et seqq. Vertical Guidelines)



Included in the block exemption	Excluded from the block exemption
A supplier may appoint up to a maximum of five (previously only one) distributors in a particular territory or for a particular customer group	Restrictions of active or passive sales within the exclusive territory or customer group
Active sales restrictions: limit buyer's ability to actively approach customers	Some passive sales restrictions: concern made in response to unsolicited requests from individual
	New: operation of a website is in principle a form of passive selling. However,


Herfurth & Partner | Alliuris Summer School 2022
41

41

alliuris

Exclusive distribution

(Art. 4(b) VBER, Sec. 4.6.1 et seqq. Vertical Guidelines)



Included in the block exemption	Excluded from the block exemption
A supplier may appoint up to a maximum of five (previously only one) distributors in a particular territory or for a particular customer group	Restrictions of active or passive sales within the exclusive territory or customer group
Active sales restrictions: limit buyer's ability to actively approach customers	Some passive sales restrictions: concern made in response to unsolicited requests from individual
It is considered active if the website has a top-level domain corresponding to particular territories or it offers languages that are not commonly used in the territory where the distributor is established	New: operation of a website is in principle a form of passive selling. However,

42


alluris

Selective distribution

(Art. 4(c) VBER, Sec. 4.6.2 et seqq. Vertical Guidelines)

New: Codification of the Coty judgment and relaxation of the “equivalence principle” between offline and online sales from selective distribution systems

In Coty, the EU Courts stated that luxury goods suppliers may prohibit members of their selective distribution network from selling the contract goods through third-party platforms without infringing EU competition law



Herfurth & Partner | Alluris Summer School 2022


43

43

alluris

Selective distribution

(Art. 4(c) VBER, Sec. 4.6.2 et seqq. Vertical Guidelines)



Included in the block exemption	Excluded from the block exemption
Prohibiting sales through online marketplaces altogether, as a sales channel	Forbidding the use of entire advertising channels, such as search engines or price comparison websites is a hardcore restriction



Herfurth & Partner | Alluris Summer School 2022

44

44

alliuris

Exclusive + Selective distribution

Included in the block exemption	Excluded from the block exemption
<p>New: Combination of selective and exclusive distribution in different territories within the EU</p>	<p>Combination of exclusive and selective distribution system in the same territory</p>

Herfurth & Partner | Alliuris Summer School 2022


45

45

alliuris

Resale price maintenance

(Art. 4(a) VBER, Sec. 6.1.1 Vertical Guidelines)



Included in the block exemption	Excluded from the block exemption
	<p>Resale price maintenance ("RPM"), including fixing margins.</p> <p>The new Vertical Guidelines provide expanded guidance on RPM, including in relation to price monitoring and providing specific guidance on Minimum advertised prices ("MAPs") and fulfilment contracts.</p>

Herfurth & Partner | Alliuris Summer School 2022

46

46

alluris

Non compete obligations

(Art. 5 VBER, Sec. 6.2.1 et seqq. Vertical Guidelines)

Obligations preventing the buyer from manufacturing, purchasing or selling goods that are in competition with the contract goods, or clauses that force the buyer to purchase from the supplier more than 80% of the buyer's total purchases of the contract goods



Herfurth & Partner | Alluris Summer School 2022


47

47

alluris

Non compete obligations

(Art 5 VBER, Sec. 6.2.1 et seqq. Vertical Guidelines)




Included in the block exemption	Excluded from the block exemption
	Non compete obligation with duration > 5 years
Tacitly renewable obligations if, after 5 years, the buyer can effectively renegotiate or terminate the contract	

Herfurth & Partner | Alluris Summer School 2022

48


48



Online intermediation service providers

(Art. 2(6) VBER, Sec. 4.4.4 Vertical Guidelines)


- New: Providers of online intermediation services qualify as suppliers under the new VBER (Art. 1(1)(d) VBER)
- Restrictions related to price, territories and customers imposed by the online intermediation service provider on buyers of those services are hardcore restrictions



Herfurth & Partner | Alliuris Summer School 2022


49

49



Online intermediation service providers

(Art. 2(6) VBER, Sec. 4.4.4 Vertical Guidelines)



Included in the block exemption	Excluded from the block exemption
	Restrictions related to price, territories and customers imposed by the online intermediation service provider on buyers of those services

Note: the VBER does not apply to agreements relating to the provision of OIS where the provider of the online intermediation services is a **competing undertaking** on the relevant market for the sale of the intermediated goods or services (hybrid platforms). An individual assessment is needed. However,

- the new Vertical Guidelines state that, in absence of restrictions by object or **significant market power**, actions in respect of such agreements are **not likely to be prioritized** by the Commission

Herfurth & Partner | Alliuris Summer School 2022

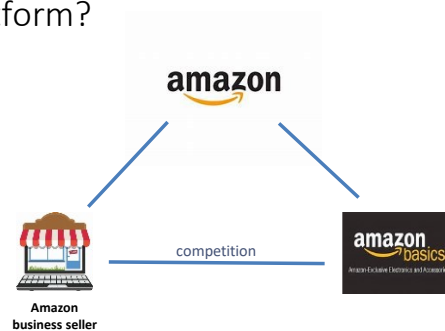
50

50

Can you think of an example of a hybrid platform?

51

Can you think of an example of a hybrid platform?



52

alluris

Real Case



Herfurth & Partner | Alluris Summer School 2022

53

53

alluris

Can Bree prevent
the buyer from:

Herfurth & Partner | Alluris Summer School 2022

54

54

alliuris

1) Selling the products online?


Can Bree prevent the buyer from:

BREE


↓

buyer

—



↓



Herfurth & Partner | Alliuris Summer School 2022

55

55

alliuris

1) Selling the products online?

2) Selling the products through online platforms?


Can Bree prevent the buyer from:

BREE


↓

buyer

—



↓




BREE


↓

buyer

—



↓



Herfurth & Partner | Alliuris Summer School 2022

56

56

alliuris

Q

Herfurth & Partner | Alliuris Summer School 2022

57

57

alliuris

Are the following constellations covered by the vertical block exemption?



All brands and cases given are examples only and do not represent the actual behavior of the respective companies

Herfurth & Partner | Alliuris Summer School 2022

58

58

Are the following constellations covered by the vertical block exemption?

Object of the question is the agreement represented with red arrows



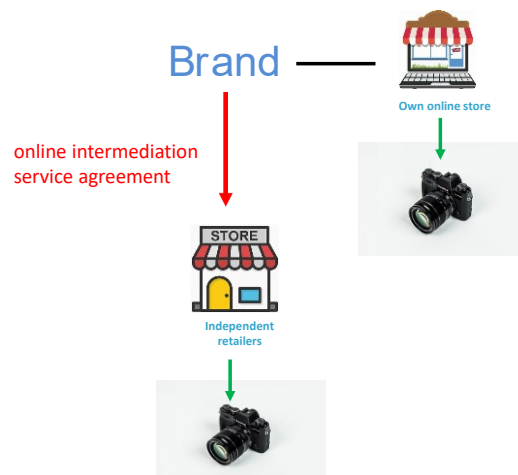
All brands and cases given are examples only and do not represent the actual behavior of the respective companies

Herfurth & Partner | Alliuris Summer School 2022

59

59

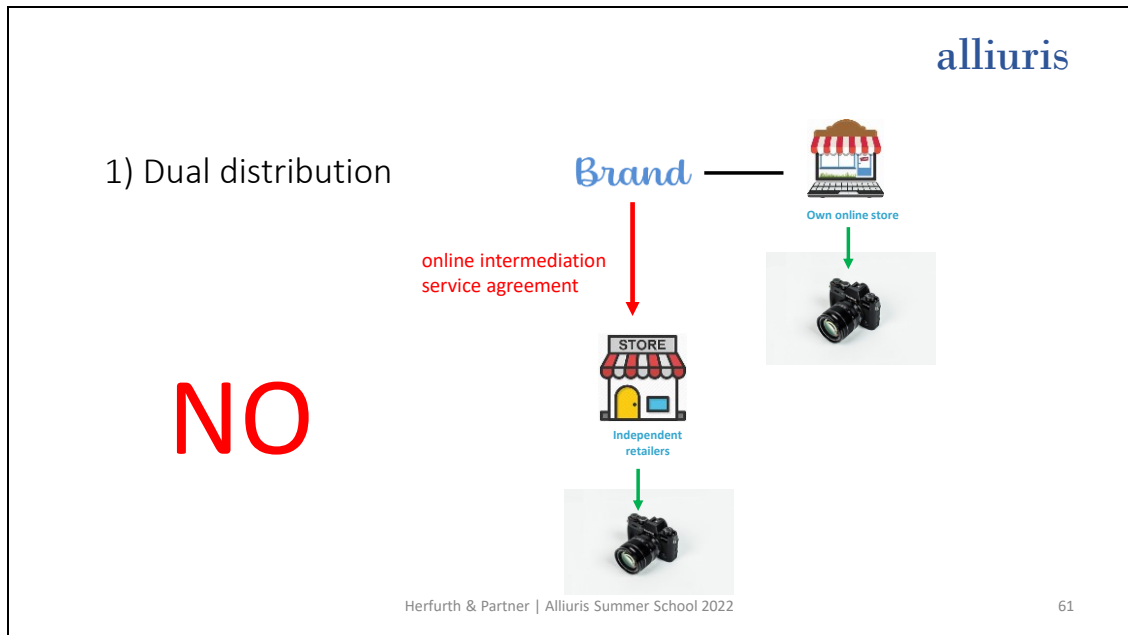
1) Dual distribution



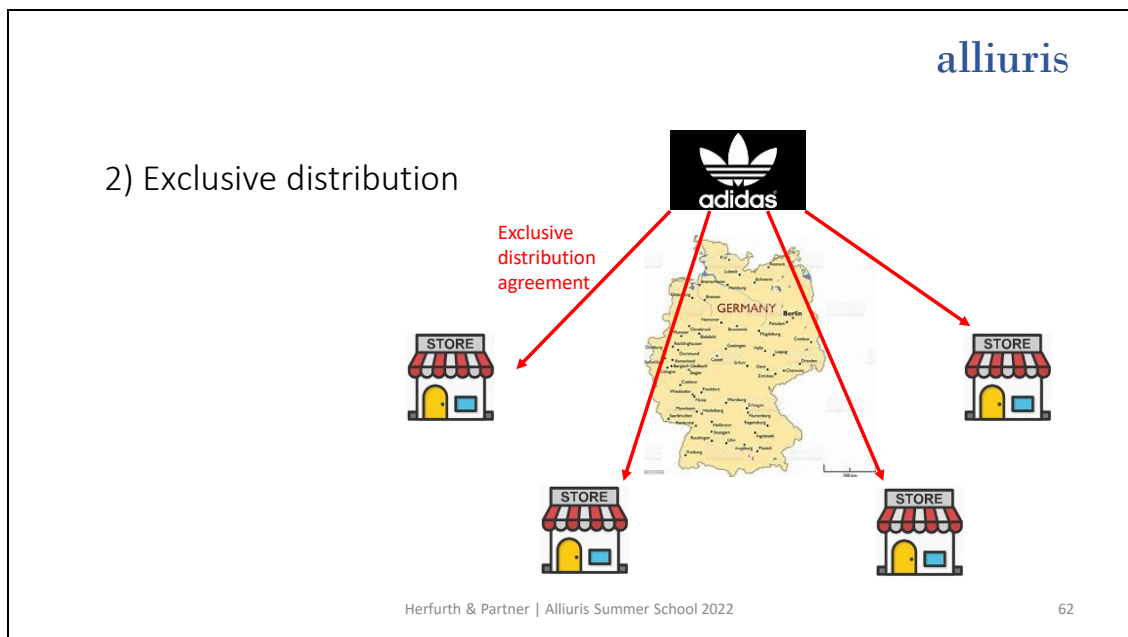
Herfurth & Partner | Alliuris Summer School 2022

60

60



61



62

alliuris

2) Exclusive distribution

YES

adidas

Exclusive distribution agreement

STORE

STORE

STORE

STORE

GERMANY

Herfurth & Partner | Alliuris Summer School 2022

63

63

alliuris

3) Dual pricing

50 €

60 €

STORE

?

?

?

?

?

?

Nike

?

?

Herfurth & Partner | Alliuris Summer School 2022

64

64

alliuris

3) Dual pricing

YES

Herfurth & Partner | Alliuris Summer School 2022

65

65

alliuris

4) Dual pricing + retail price

X € Y €

Herfurth & Partner | Alliuris Summer School 2022

66

66

alliuris

4) Dual pricing + retail price

50 €

60 €

X €

Y €

NO

Herfurth & Partner | Alliuris Summer School 2022

67

67

alliuris

5) Online sales restrictions

Buyer must operate one or more brick-and-mortar stores and makes at least 60% of the minimum absolute volume of sales offline

Manufacturer

✓

✗

Herfurth & Partner | Alliuris Summer School 2022

68

68

218

5) Online sales restrictions

Buyer must operate one or more brick-and-mortar stores and makes at least 60% of the minimum absolute volume of sales offline

YES

The diagram illustrates the requirement for a buyer to have brick-and-mortar stores. A 'Manufacturer' (represented by a gear icon) is shown at the top. A red arrow points from the manufacturer to the 'YES' scenario, and a black arrow points to the 'NO' scenario. The 'YES' scenario shows a laptop and a storefront labeled 'STORE' with a plus sign between them, a green checkmark below, and the word 'YES' in large green letters. The 'NO' scenario shows a laptop inside a red circle with a red 'X' below it.

Herfurth & Partner | Alliuris Summer School 2022

69

69

alliuris



Herfurth & Partner | Alliuris Summer School 2022

70

70

Useful links:

- ✓ General information on the VBER:
[2017 vber \(europa.eu\)](https://eur-lex.europa.eu/eli/reg/2017/107/oj)
- ✓ Text of the VBER:
[EUR-Lex - 32017R1070 - EN - EUR-Lex \(europa.eu\)](https://eur-lex.europa.eu/eli/reg/2017/107/oj)
- ✓ Text of the Vertical Guidelines:
[EUR-Lex - 52022XC0630\(01\) - EN - EUR-Lex \(europa.eu\)](https://eur-lex.europa.eu/eli/reg/2022/717/oj)

71

Thank you for listening to:

The new EU Regulation on Competition Restrictions in Vertical Markets

Ulrich Herfurth
Attorney at law, Hannover / Brussels

With the support of
Sara Nesler, LL.M.

www.hurfurth.de



72

Materials | Compact

Restrictions of competition in distribution

Ulrich Herfurth, attorney at law, Hanover/Brussels
Sara Nesler, Mag. jur. (Torino), LL.M. (Münster)

October 2022

Companies often have an interest in binding their distribution partners in certain ways in order to secure their position in the market. In doing so, they usually restrict competition. In contrast, the principle of free competition applies in the EU, and restrictive measures by companies are generally not permitted.

Therefore, the EU in principle prohibits all agreements, decisions and concerted practices that are anti-competitive and distort the internal market (Article 101(1) Treaty on the Functioning of the European Union / TFEU). However, an exception exists for certain types of agreements if they are beneficial to consumers. Nevertheless, it is problematic that each individual agreement and act must be assessed individually. This leads to a high degree of legal uncertainty, which is reflected in a high level of effort and risk for companies.

The block exemption regulations

In order to increase predictability and legal certainty, the European Commission adopts block exemption regulations (Art. 103 TFEU), thereby setting out the conditions under which certain types of agreements in certain market sectors are in principle deemed to comply with competition law. For such agreements, a BER creates a kind of "safe harbor". In total, there are currently six block exemption regulations, concerning: specialization agreements, research and development agreements, insurance sector, technology transfer agreements, motor vehicle spare parts and vertical agreements.

The new Vertical BER 2022

On June 1st, 2022, the EU has updated the Block Exemption Regulation on Vertical Agreements (Vertical Block Exemption Regulation) accompanied by the new Vertical Guidelines.

The new Verticals Block Exemption Regulation, like the previous one, creates an exception to the principle of prohibition of restrictions of competition for certain vertical agreements, i.e. between undertakings operating at different levels of the production, supply and distribution chain.

The updated version of the regulation includes several changes that may require or allow companies to adjust their distribution models.

Unlike other block exemption regulations, the Vertical Block Exemption Regulation applies irrespective of the sector. The prohibition of restrictions of competition in vertical agreements does not apply if none of the parties exceeds a market share of 30 % on the relevant sales and purchase market. However, this de minimis rule does not apply to the infringement of hardcore restrictions (Article 2 of the Verticals Block Exemption Regulation).

If the contract contains a hardcore restriction, the whole contract is excluded from the block exemption and individual assessment becomes necessary.

As a result, if a contract contains such an agreement, this may render the contract as a whole invalid. Companies should therefore review their existing contracts and adapt them if necessary; new contracts should be drafted in a legally compliant manner.

In addition, the Vertical Block Exemption Regulation contains a list of so-called "grey clauses" which must be examined in an individual assessment (Art. 5 Vertical Block Exemption Regulation). However, the exclusion from the block exemption does not extend to the entire contract, but only concerns the individual clause. Grey clauses should also be checked regularly and adjusted if necessary.

The most important innovations of the Vertical Block Exemption Regulation are presented below. This serves as an overview and does not replace individual advice.

Most important innovations: scope

Dual distribution

Where a supplier sells its goods both through independent distributors and directly, it may well be in competition with its distributor.

Under the old Verticals Block Exemption Regulation, vertical agreements between competitors were generally excluded from the block exemption and had to be assessed individually. Dual distribution, on the other hand, was permitted by the Vertical Block Exemption Regulation.

With the new regulation, dual distribution remains in principle exempt. However, particular caution applies to dual distribution in the context of the provision of online intermediary services (OIS), e.g. through hybrid platforms, and to the exchange of certain information between suppliers and buyers.

Main innovations on hardcore restrictions

OIS

Operators of *online intermediation services (OIS)* are considered suppliers under the new regulation. Price, territorial and customer restrictions imposed by a dual-distributing OIS provider on the customers of its services are now considered hardcore restrictions and are therefore prohibited.

Dual pricing

Under the old Vertical Block Exemption Regulation and its guidelines, so-called "dual pricing" was a core restriction. A supplier (e.g. wholesaler) was therefore not allowed to charge different prices to customers for online sales and for stationary sales.

From the perspective of the European legislator, the protection of online trade in this respect is no longer necessary and dual pricing is now permitted. A change of the own distribution structure is accordingly possible.

It should be noted, however, that price differences must be proportionate to the cost differences between online and offline channels. The aim of pricing policy must therefore not be to restrict sales to certain territories or customers or to virtually prevent the use of the Internet.

Furthermore, the supplier may not impose on its customers that its selling prices must be higher or lower depending on the distribution channel.

Restriction of online sales

Unlike the old Vertical Block Exemption Regulation, the new Vertical Block Exemption Regulation explicitly identifies the prevention of the effective use of the internet by buyers or their customers for the sale of services or goods as a hardcore restriction. Softer measures may be permissible, e.g. those aimed at ensuring the quality of the trader's online shop or requirements according to which the trader must operate one or more bricks-and-mortar shops or achieve a minimum volume of offline sales. This means for companies that such restrictive agreements must be reviewed in the sense of the clarifications of the new regulation and its guidelines in order to exclude the anti-competitive nature of such an agreement.

Exclusive and selective distribution systems

In the new Vertical Block Exemption Regulation, the rules on exclusive, selective and other distribution systems are structurally more differentiated. In principle, however, the rules remain similar. For instance, a restriction on the place of establishment of the buyer or a prohibition on sales to final consumers by a buyer at the wholesale level are still allowed.

As an innovation, the provider is now allowed to use up to five exclusive distributors in a certain area or for a certain customer group, previously it was only allowed to use one.

It is also of practical importance that the respective permissible restrictions on active or passive sales to protected customer groups or territories can now be extended to the second distribution level (previously only the first). Attention should be paid to the definitions of active and passive

sales in the new Vertical Block Exemption Regulation. Particular care should be taken when classifying the operation of websites.

Prohibition of sales via online marketplaces

Already in 2017, the ECJ had clarified that suppliers of luxury goods may prohibit their distributors in the selective distribution network from selling the contract goods via third-party platforms. This is not a prohibited restriction of competition.

The new Vertical Block Exemption Regulation now legally fixes this relaxation of the "equivalence principle" between offline and online sales. Accordingly, the supplier may generally prohibit its dealers from selling via online marketplaces as a sales channel, but not entire advertising channels such as search engines or price comparison websites. This remains an impermissible hard-core restriction.

Exclusive + selective distribution

The new rules continue to allow the combination of selective and exclusive distribution in different territories within the EU (e.g. selective in Spain and exclusive in France). Protection of the different forms of distribution from each other remains permissible, in particular, restrictions may now also be extended to the second level of distribution. The combination of an exclusive and a selective distribution system in the same territory is still not covered by the block exemption.

Resale price maintenance

Both direct and indirect price maintenance measures vis-à-vis authorized dealers ('second hand') remain prohibited.

If a supplier negotiates directly with the customer, e.g. a retail chain, he is allowed to involve a trader of his choice who delivers the goods to the customer at that particular price. The prerequisite is that the customer is bound to this trader and cannot choose any other trader.

The supplier is also permitted to set maximum selling prices and to make price recommendations.

Main innovations: grey clauses

Non-compete obligations

Non-compete obligations and clauses requiring the buyer to purchase more than 80 % of its total purchases of the contract goods from the supplier are still not exempted if the duration exceeds five years. However, tacitly renewable obligations are now exempted if the buyer can effectively renegotiate or terminate the contract after five years.

Most favoured nation clause

A most-favoured-nation (MFN) clause (or parity obligation) obliges a company to offer its counterparty the same or better conditions than on other sales markets. The old vertical BER provided for a full exemption for all parity obligations.

However, under the new Vertical Block Exemption Regulation, "wide parity clauses" are no longer covered by the block exemption. These are agreements whereby an online platform prevents its trader or supplier from offering the same product on other retail platforms on better terms or at a lower price.

All other parity clauses (relating to the provider's own distribution channel) remain exempt. However, if a platform dictates to its suppliers tight parity clauses covering a significant proportion of users without any evidence of efficiency, the exemption may be withdrawn.

Outlook

Companies, especially those with online sales, should legally review their existing and future distribution agreements.

In addition, despite the complexity of the subject matter, it is recommended to obtain a well-founded picture of the new BER - the changes and clarifications of the new vertical BER and the supplementary guidelines may well open up new possibilities for one's own distribution model.

+ + +

Chapter Seven

Quality and Security in the Supply Chain




1



2

alliuris

The Modular Contract System



3

alliuris

Framework Purchasing Agreement

Basics
Quantities, availability
Pricing
Order processing
Quality
Warranty, liability
Intellectual property
International
General provisions

Herfurth & Partner | Alliuris Summer School 2022

4

alliuris

Framework Purchasing Agreement

Basics
Quantities, availability
Pricing
Order processing
Quality
Warranty, liability
Intellectual property
International
General provisions

General conditions for purchasing

Provisions for the individual purchase contract

Order
Invoices
Payment
Retention of title
Warranty
Liability
Intellectual property

Herfurth & Partner | Alliuris Summer School 2022

5

alliuris

Framework Purchasing Agreement

Basics
Quantities, availability
Pricing
Order processing
Quality
Warranty, liability
Intellectual property
International
General provisions

General conditions for purchasing

Provisions for the individual purchase contract

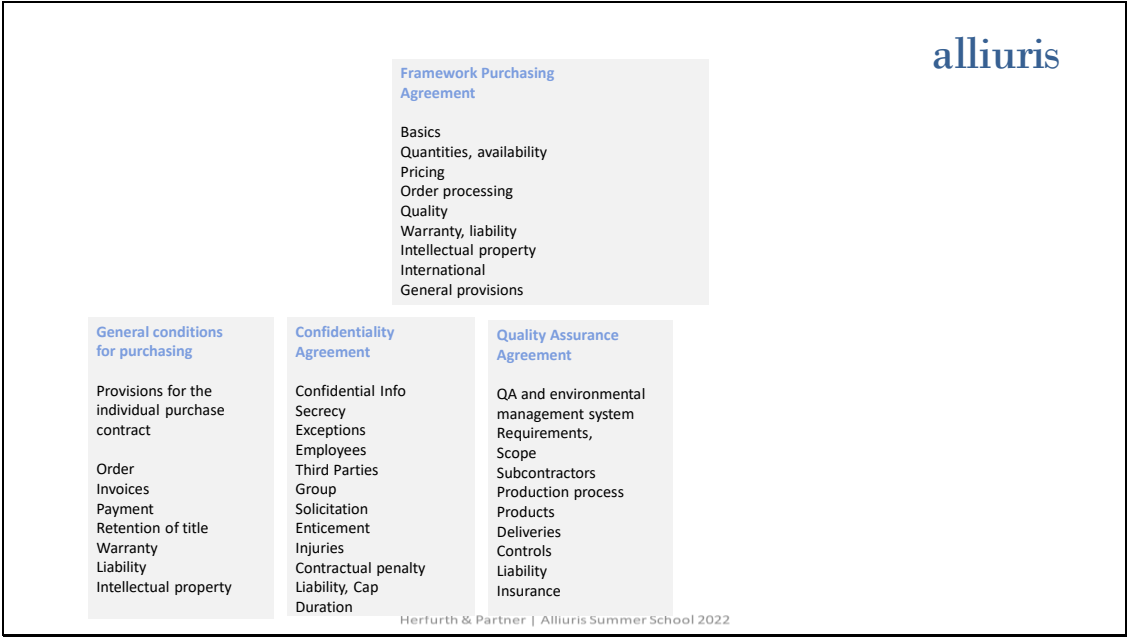
Order
Invoices
Payment
Retention of title
Warranty
Liability
Intellectual property

Confidentiality Agreement

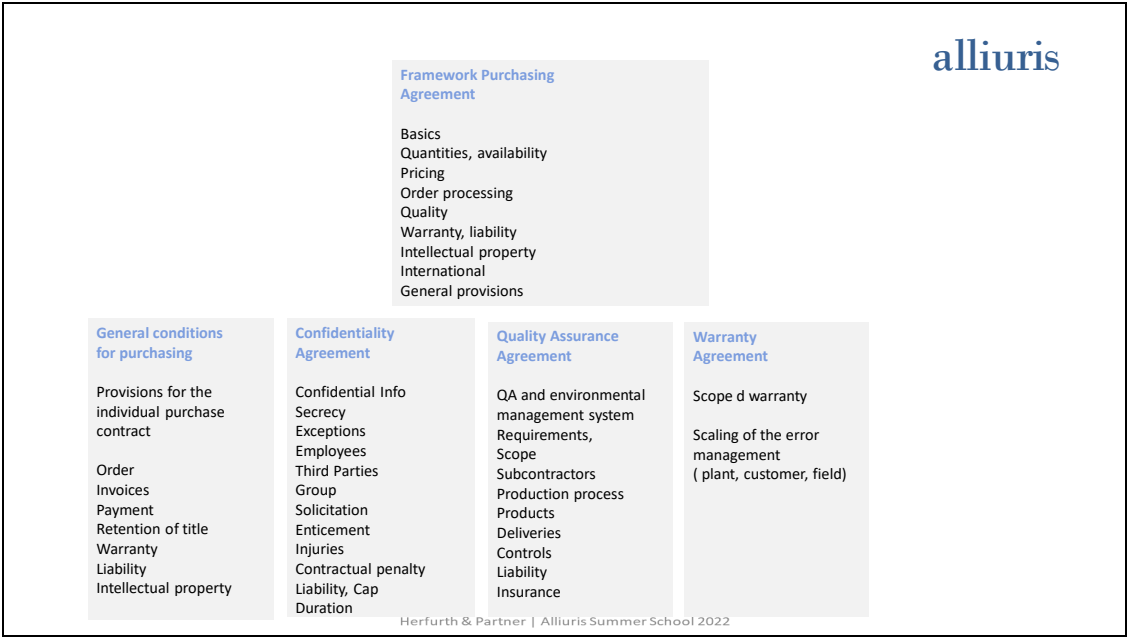
Confidential Info
Secrecy
Exceptions
Employees
Third Parties
Group
Solicitation
Enticement
Injuries
Contractual penalty
Liability, Cap
Duration

Herfurth & Partner | Alliuris Summer School 2022

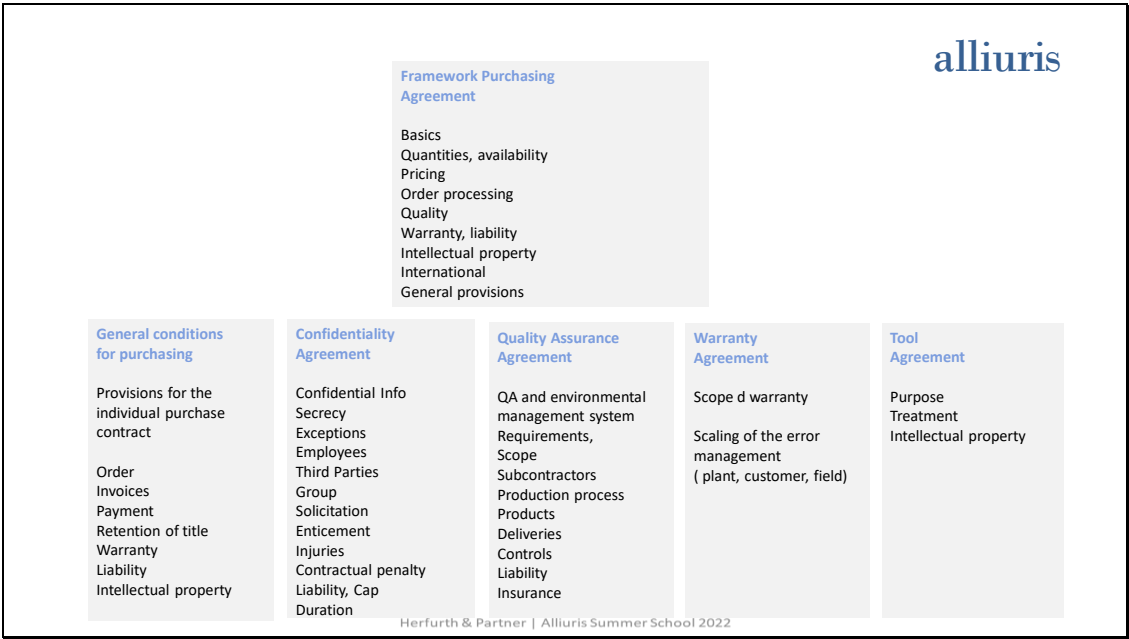
6



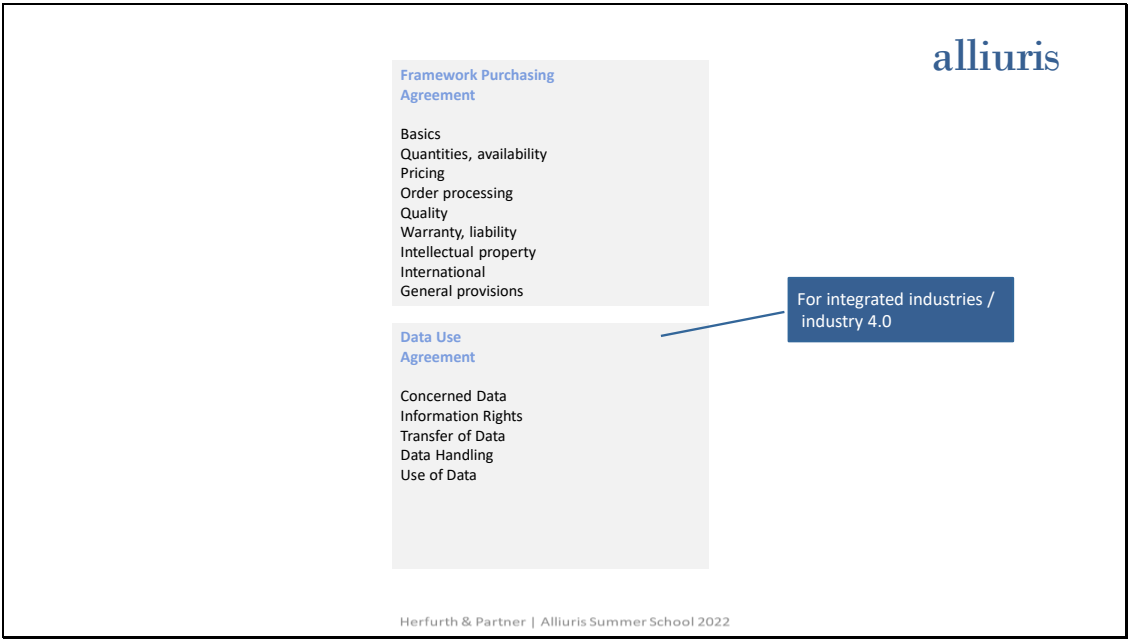
7



8



9



10

alliuris

Framework Agreements | Sale



11

alliuris

Framework supply agreements | Sale

- Subject of the contract, products
- Orders, acceptance
- Minimum volume
- Terms of delivery, transfer of risk, INCOTERMS
- Pricing
- Payment protection, retention of title
- Warranty, liability
- Product protection, design protection
- International contracts

Herfurth & Partner | Alliuris Summer School 2022

12

alluris

GTC Sale


- Order
- Prices
- Delivery and transfer of risk
- Invoicing, payment,
- Warranty, liability for defects
- Retention of title
- Liability
- Model protection
- Ancillary provisions
- Place of performance and jurisdiction
- International business

Herfurth & Partner | Alluris Summer School 2022

13

alluris

Framework Agreements | Purchase



14

Framework supply agreements | Purchasing

- Subject of the contract, products
- Series
- Orders, orders
- Readiness for delivery
- Terms of delivery, transfer of risk, INCOTERMS
- Pricing
- Quality assurance
- Warranty, liability
- Technology protection, design protection,
- Competition
- International business

Herfurth & Partner | Alliuris Summer School 2022

15

GTC Purchasing

- Orders/ Prices
- Delivery dates/ delivery and transfer of risk
- Orders/ acceptance
- Invoices/ payment
- Retention of title
- Warranty, liability for defects/liability
- Quality control / quality assurance / product modifications
- Industrial property rights of third parties/ trade and business secrets/ model protection
- Provisions on export control and foreign trade data
- Place of performance and jurisdiction
- International business

Herfurth & Partner | Alliuris Summer School 2022

16

alliuris

Additional contracts



17

alliuris

Additional contracts | Overview

- Quality Assurance Agreement
- Warranty agreement
- Tool Transfer Agreement
- Security Agreement
- Confidentiality Agreement / NDA

Herfurth & Partner | Alliuris Summer School 2022

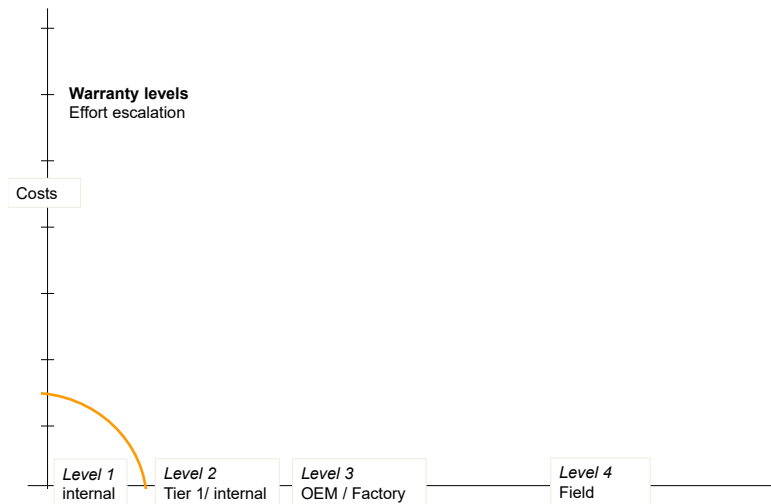
18

Quality Assurance Agreement

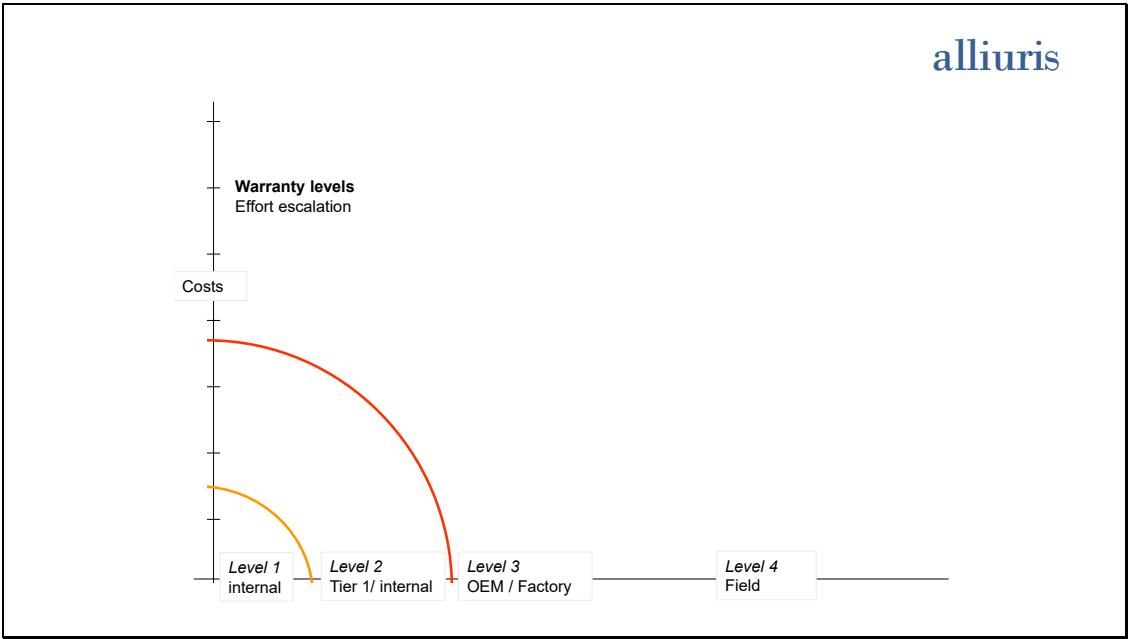
- Quality and environmental management system of the supplier
- Quality management system of subcontractors
- Audit
- Information and documentation
- Product life cycle agreements
 - Development, planning, release
 - Labeling of products, traceability
 - Delivery, incoming goods inspection, complaints and costs
 - Product liability/recalls
- Quality objectives
- General conditions of purchase
- Term of contract, termination
- Final provisions

Herfurth & Partner | Alliuris Summer School 2022

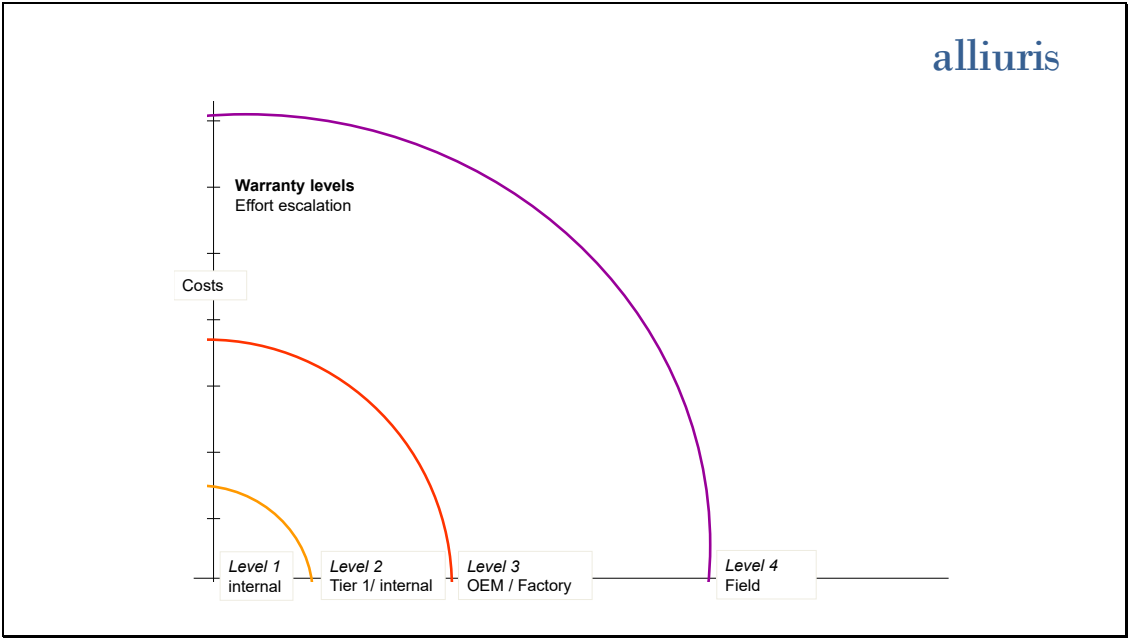
19



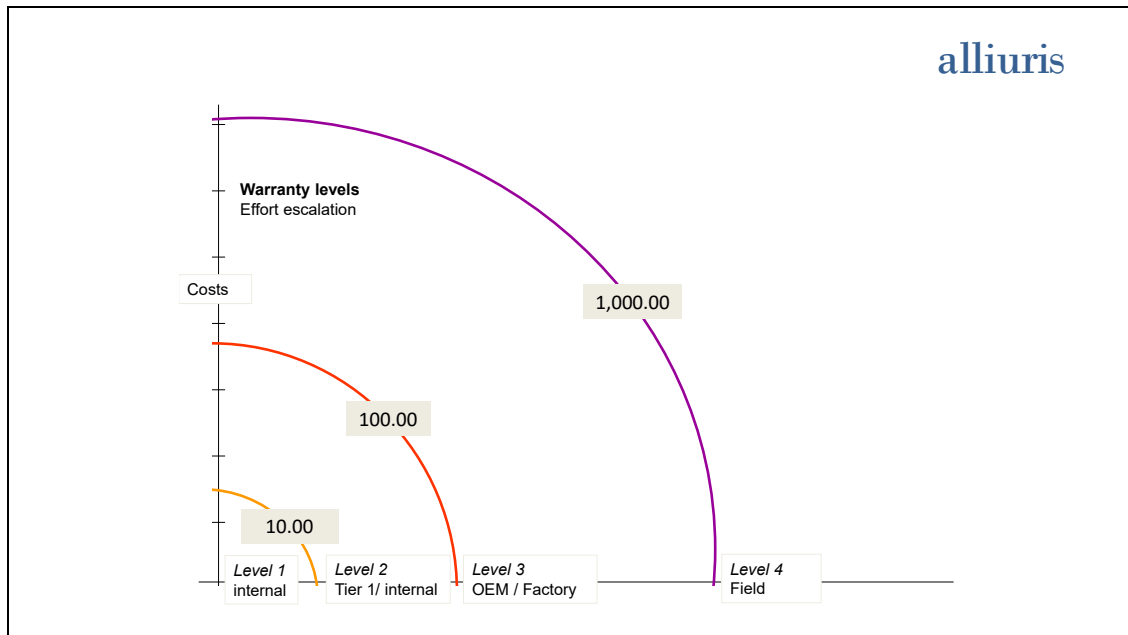
20



21



22



23

Warranty Agreement

- Subject of the contract
- Content and scope of liability for material defects
- Warranty period
- Time of error detection
- Error analysis / 8D-Report
- Warranty for "internal returns"
- Warranty for "factory returns"
- Warranty for field failures
- Minimum damage / damage lump sum
- Serial damage
- Damage after the expiry of the liability period (goodwill)
- Product liability
- General provisions

Herfurth & Partner | Alliuris Summer School 2022

The Alliuris logo is visible in the top right corner of the slide.

24

Tool Agreement

- Subject of the contract
- Handing over the tools / ordering of tools
- Minimum application rate
- Obligation of the supplier
- Transfer of the tools to third parties
- Handing over the tools to the customer
- Stocks

Herfurth & Partner | Alliuris Summer School 2022

25

Security Agreement

- Transfer by way of security
- Backup purpose
- Obligations of the collateral provider with respect to the collateral asset
- Statutory liens
- Guarantees of the guarantor
- Protection of the secured goods
- Recovery
- Retransfer and release of collateral
- Valuation of the collateral
- Final provisions

Herfurth & Partner | Alliuris Summer School 2022

26

alliuris

Data Use Agreement

- Concerned Data
- Information Rights
- Transfer of Data
- Data Handling
- Use of Data:
 - Process step
 - Aggregation ?
 - Analytics ?
 - Sale ?
 - Sale of Analytics ?
 - Etc
 -

Herfurth & Partner | Alliuris Summer School 2022

27

alliuris

Secrecy



28

Confidentiality Agreement / NDA

- Regulates certain rights and obligations when confidential information is provided (cooperation, before cooperation drawing, etc.)
- One-sided for one party, or ...
- two-sided, when both parties can be both a recipient

Herfurth & Partner | Alliuris Summer School 2022

29

Confidentiality Agreement / NDA


- Definition of confidential information / business secrets (?)
- Secrecy obligation
- Exceptions from secrecy
- Respondents
- Duration of confidentiality (the NDA is usually valid from the date of signing and applies to information provided since a certain date). The end of the information transfer (business relationship) is also regulated.
- Secrecy can be agreed for an unlimited period
- Injury consequences, penaltym, damagae compensation, cap
- Final clauses (severability clause, place of jurisdiction, etc.)

Herfurth & Partner | Alliuris Summer School 2022

30

alliuris

Warranty & Liability



31

alliuris

Problem Focus | Overview

- Warranty BGB / CISG
- Contractual penalty & liquidated damages
- Limitation of liability in general terms and conditions
- Product liability for suppliers

Herfurth & Partner | Alliuris Summer School 2022

32

Warranty BGB / CISG

- Withdrawal of the buyer
 - BGB: possible, if significant breach of duty
 - CISG: The aim is to maintain the contract, cancellation only in case of material breach of contract
- Quality free of defects
 - BGB: Deviation of actual condition from target condition
 - CISG: material breach of contract (e.g. deviation in quality and quantity)
- Supplementary performance in case of defect
 - BGB: customer can demand replacement of the defect good
 - CISG: only if lack of conformity is a fundamental breach of contract (otherwise price reduction)

Herfurth & Partner | Alliuris Summer School 2022

33

Contractual penalty, liquidated damages


- Liquidated Damages: some clauses prohibited pursuant to Section 309 No. 5 of the German Civil Code (BGB)
- Contractual penalty: amount of the contractual penalty, prohibited in some countries
- Comparison: liquidated damages and contractual penalty advantages/ disadvantages
- Recommendation

Herfurth & Partner | Alliuris Summer School 2022

34

alliuris

Product Liability



35

alliuris

Product liability for suppliers

- Under the ProdHaftG, product manufacturers are liable to injured persons even without fault
- Product is any movable thing, even if it forms a part of another movable thing or immovable thing (§ 2)
- A defect exists if a product does not provide the safety that can be expected under consideration of all circumstances (§ 3)
- A manufacturer is anyone who has manufactured the final product, a basic material or a partial product (§ 4) or who imports or transfers the product, e.g. for the purpose of sale, into the European Economic Area.

Herfurth & Partner | Alliuris Summer School 2022

36

Product liability for suppliers

- If the manufacturer cannot be determined, the supplier is deemed to be the manufacturer (exculpation possible)
- In the EU the importer is considered as the manufacturer
- In the EU a seller who labels the product can be considered as the manufacturer (*quasi-manufacturer*)
- If several manufacturers are liable to pay compensation for the same damage, they shall be jointly and severally liable (§ 5)

Herfurth & Partner | Alliuris Summer School 2022

37

Product liability for suppliers

- The obligation of the manufacturer of a partial product to pay compensation is excluded if the defect was caused by the design of the product into which the partial product was incorporated or by the instructions of the manufacturer of the product (§ 1 par. 3).
- Manufacturer of a partial product is thus liable to the injured party if the defect was in the partial product and not in a defective use of a partial product that is in itself free of defects
- Incorrect use in the final product is a design defect for which the manufacturer is responsible

Herfurth & Partner | Alliuris Summer School 2022

38

alliuris

Insurance



39

alliuris

Insurances

- Alignment of insurance conditions with product liability risks
- Product insurance policy must cover injuries of victims and cost of recall of the products
- Reconciliation of insurance conditions to contract terms with customers
- If contractual liability is greater than legal liability, loss of insurance coverage is threatened

Herfurth & Partner | Alliuris Summer School 2022

40

alluris

Thank you for listening to:

Quality and security
in the supply chain

Ulrich Herfurth
Attorney at law, Hannover / Brussels
www.herfurth.de



41

alluris
INTERNATIONAL

Herfurth & Partner - Alluris Summer School 2022

42

Chapter Eight

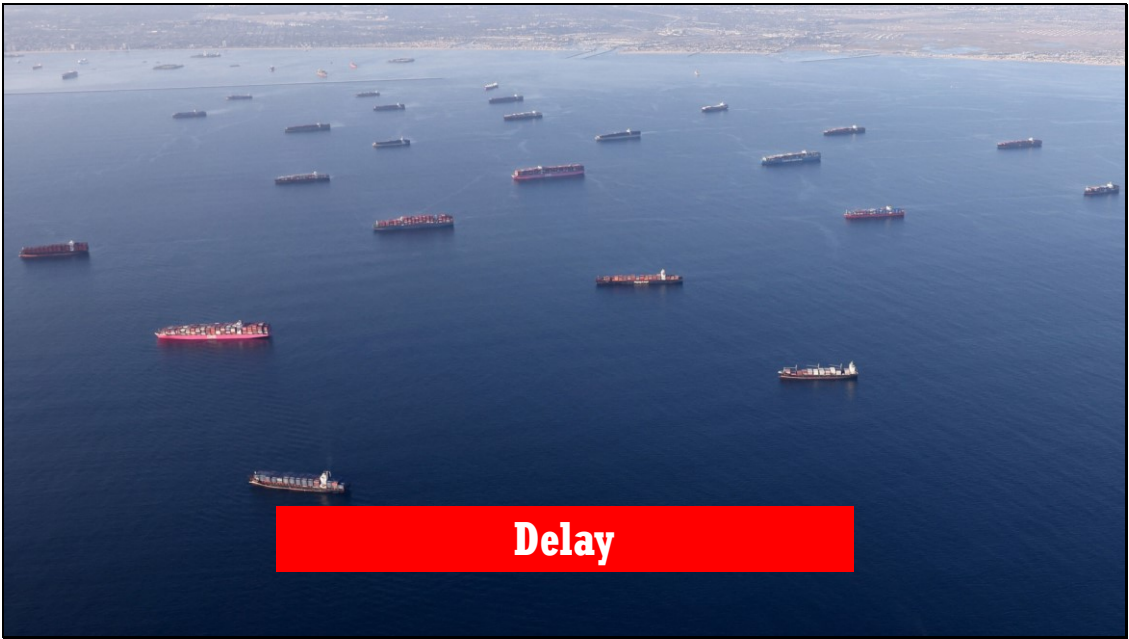
Supply Chain Problems



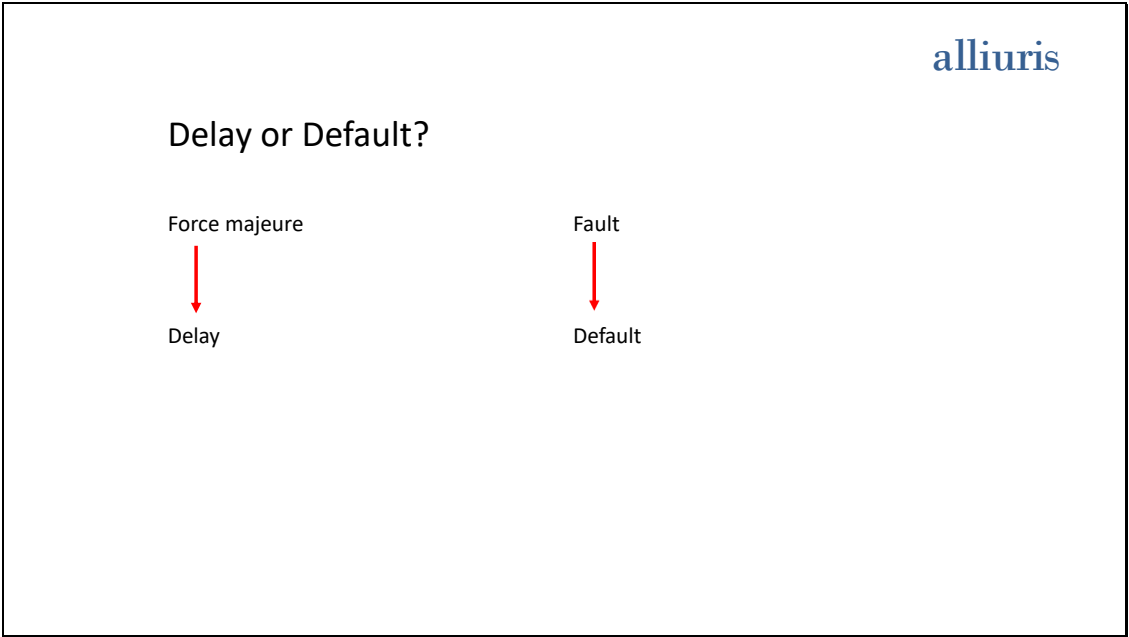
1




2



3




4




Delay or Default?

Force majeure



Delay


Fault



Default

Force majeure is a non-operational event caused externally by **elementary forces of nature or by the actions of third parties**, which is **unforeseeable** according to human insight and experience, **cannot be prevented** or rendered harmless by economically acceptable means **even by the utmost care** reasonably to be expected in the circumstances, and is also **not to be accepted** by the operating company because of its frequency

5



Events of force majeure

Events of force majeure shall include, e.g.:

- natural disasters, natural events, nuclear disasters, epidemics,
- war, civil unrest, acts of terrorism;
- general shortage of raw materials, consumables and supplies, where replacement is not possible at reasonable additional expense;
- failures due to machine damage, machine breakdowns and other operational disruptions
- ...

6

Consequences

Example of possible contractual clauses:

7

Consequences

Example of possible contractual clauses:

- Insofar as a Party cannot properly fulfil its contractual obligations by reason of force majeure, the other Party does not derive any rights to damage compensation there-from, irrespective of the legal grounds

8

Consequences

Example of possible contractual clauses:

- Insofar as a Party cannot properly fulfil its contractual obligations by reason of force majeure, the other Party does not derive any rights to damage compensation there-from, irrespective of the legal grounds
- In the event of impediments to performance due to force majeure, the delivery date shall be extended by the duration of the delay.

Provider
friendly

9

Consequences

Example of possible contractual clauses:

- Insofar as a Party cannot properly fulfil its contractual obligations by reason of force majeure, the other Party does not derive any rights to damage compensation there-from, irrespective of the legal grounds
- In the event of impediments to performance due to force majeure, the delivery date shall be extended by the duration of the delay.
 - ✓ Alternatively: In the event of impediments to performance due to force majeure, the delivery and payment date shall be extended by the duration of the delay, provided that the affected Party

Beneficiary
friendly

10

Consequences

Example of possible contractual clauses:

- Insofar as a Party cannot properly fulfil its contractual obligations by reason of force majeure, the other Party does not derive any rights to damage compensation there-from, irrespective of the legal grounds
- In the event of impediments to performance due to force majeure, the **delivery date** shall be extended by the duration of the delay.
 - ✓ Alternatively: In the event of impediments to performance due to force majeure, the **delivery and payment date** shall be extended by the duration of the delay, provided that the affected Party
- If the status of force majeure persists for a duration of more than (....) months, the Party not affected is entitled to terminate this Agreement without prior notice.

11


Survey

Answer **yes** or **no** and write the reason in the chat

12

alliuris

Is the Covid-19 Pandemic an event
of force majeure?

yes  no

Herfurth & Partner - Alliuris Summer School 2022

13

13

alliuris

Is the Ukraine war an event of
force majeure?

yes  no

Herfurth & Partner - Alliuris Summer School 2022

14

14

alliuris

Can force majeure result from a chain reaction?

```
graph LR; A[ ] --> B[ ]; B --> C[ ]; C --> D[ ]; D -. "force majeure?" .-> E[ ]
```

yes

no

Herfurth & Partner - Alliuris Summer School 2022

15

15

Shortage

16

256

Consequences

- ✓ Delay
- ✓ Objective impossibility of procurement
- ✓ Subjective impossibility of procurement

17



18

Dealing with price increases

- Force majeure? (-) “money has to be had”
- Is there a price escalation clause in the contract ?
- Disturbance of the basis of business: →
 - ✓ Contract adjustment
 - ✓ Resignation/termination
- MAC - material adverse change (M&A)
- Salvatory Clause

Circumstances, which have become the basis of the contract, have **changed seriously after** the conclusion of the contract and the **parties would not have concluded the contract** or would have concluded it with different content **if they had foreseen this change**

19

What market price fluctuation is still acceptable? And why?

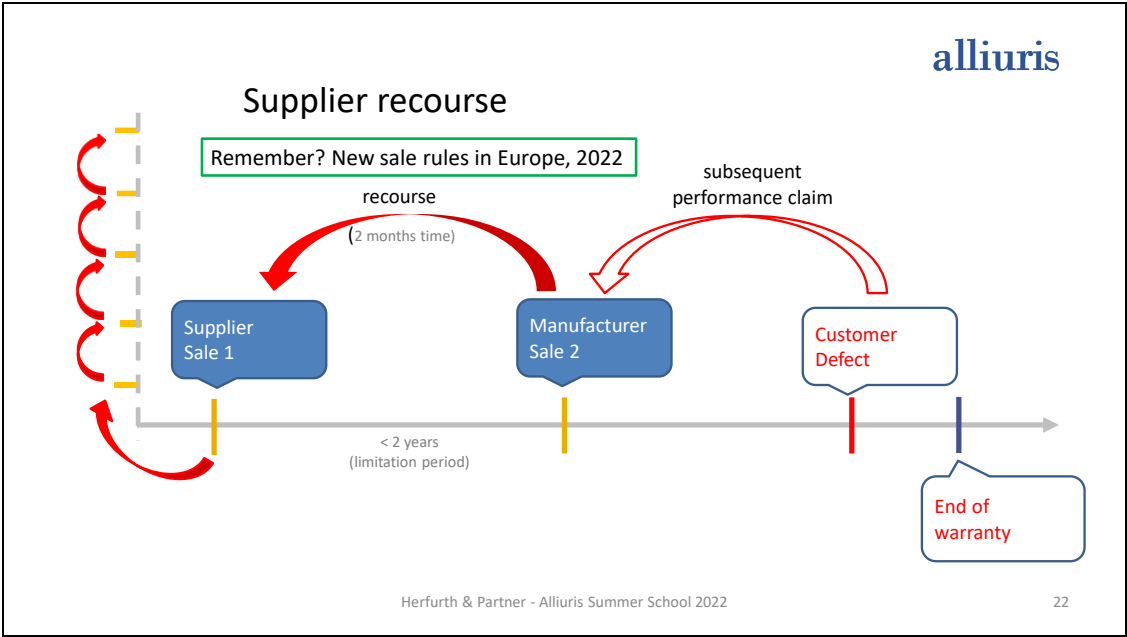


Please write in the chat

20



21



22

Contractual agreements

A supplier can generally exclude the recourse claims of its customer by means of a GTC clause or through an individual contractual agreement.

Pay attention:

- B2C (consumer at the end of the chain), specific requirements
- B2C and digital goods: It is **not possible** to conclude an agreement aimed at excluding supplier regress. The provisions are **mandatory**.



23



24

Current developments

- Germany:
Lieferkettensorgfaltspflichtengesetz (in force 01.01.2023)
- EU:
Supply Chain Act (draft directive)
Goal: ensure that companies respect human rights and comply with environmental standards within their global value chain. This includes, for example, the prevention of child and forced labor, the creation of safe and healthy working conditions, and fair wages.
- Trend:
Greater obligation for companies to identify, prevent, eliminate, or reduce the negative impact of their activities on human rights and the environment.

25

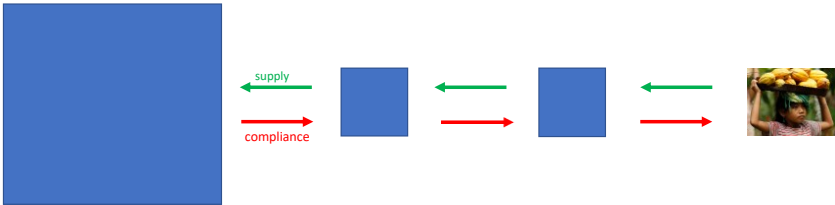
EU supply chain act

- Compliance obligations:
 - ✓ E.g. identify actual or potential negative impacts on human rights and environment
 - ✓ prevent or mitigate potential impacts
 - ✓ eliminate or minimize actual impacts
- Applies to:
 - ✓ Corporations with more than 500 employees and global net turnover > 150 million euros
 - ✓ Companies with more than 250 employees active in resource intensive industries
 - ✓ Compliance obligations are **likely to extend** further than just to the direct supplier, also to **SME** as part of the value chain.
- Sanctions:
 - ✓ Fines based on the company's turnover
 - ✓ Companies that have violated their due diligence obligations should, under certain circumstances, be liable under civil law for damage that has occurred along their value chain.

26

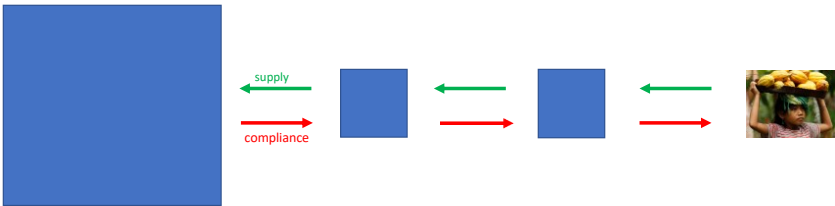
EU supply chain act: problem

Pushing duties through to medium-sized businesses / suppliers



27

Do you have an idea for a better system?



Please write in the chat

28

Certification

The trend toward certification is likely to increase. By obtaining certificates (EMAS, Green Button, SMETA, etc.), companies can more easily prove that they meet certain human rights or environmental standards. Certificates make the supply chain more transparent and increase the reputation and attractiveness of a company, especially in the face of increasing due diligence requirements.



29

alliuris

Thank you for listening to:

Supply Chain Problems

Ulrich Herfurth
Attorney at law, Hannover / Brussels

With the support of
Sara Nesler, LL.M.

www.herfurth.de



30



Materials | Compact

Contractual disruptions and Russia

Ulrich Herfurth, attorney at law, Hanover/Brussels
Aline-Kristin Pehle, trainee lawyer, Hanover

April 2022

The new EU sanctions against Russia pose challenges for companies with trade relations with Russian companies in many areas. Legal bans, rising prices and supply bottlenecks make the execution of contracts considerably more difficult, but do not per se release companies from their contractual obligations. The sanctions not only affect contracts with Russian trading partners but may also have an indirect impact on contracts with other trading partners, for example if Russian suppliers are involved.

This article provides information based on German law. The same general principles apply to other jurisdictions; however, appropriate legal advice remains indispensable.

Obligation to fulfill the contract?

If a contract regulates the delivery of goods or the provision of (financial) services that are directly or indirectly affected by the sanctions, contractual rights and obligations generally remain in place.

However, some sanctions regulations also provide for exceptions for certain purposes, pre-existing contract clauses for contracts concluded before February 26, 2022, and settlement periods. In this way, even though the service owed is actually affected by the sanctions regulations, the contractual partners do not encounter any difficulties in fulfilling the contract.

Framework supply agreements that already exist and still have a longer contractual term could also fall under the pre-existing contract clauses.

It should also be noted that the sanctions do not, so far, prohibit the transit of goods through Russia. An obligation to supply sanctioned goods to a creditor in another state is therefore still possible even if they must be sent through the Russian territory.

Exemption from the obligation?

Whether a contracting party has legal possibilities to exempt itself from individual obligations,

to adapt contracts or even to withdraw from them, depends on the individual case and is linked to narrow preconditions. In principle, inefficiency due to sharp price increases alone is not sufficient. Delivery failures must also be taken into account as part of the assumed procurement risk. If necessary, the contractual partner must change the supplier.

The possibility of release from a contractual obligation depends on whether (1) a provision for an exception from the contractual obligations has been agreed in the contract itself and (2) which choice of law has been made for the contract, i.e., whether German, foreign or UN sales law applies.

Contractual clauses

In commercial and supply contracts, there are mostly clauses called “force majeure” or “hardship clauses”.

Force majeure

“Force majeure” clauses regulate unforeseeable, unpreventable events that are beyond the control of the contracting parties. The clauses explicitly list the events that are to be recognized as force majeure at the factual level. These usually include natural disasters, terrorist attacks, labour disputes, pandemics, government seizures and expropriations - as well as embargoes and wars. However, the events mentioned are not usually listed exhaustively. In individual cases, therefore, it must be examined whether an event not listed is comparable in its scope and consequences to the other events. The contractual partner must also be able to demonstrate that this event is unforeseeable and uncontrollable and that it is the actual cause of the impairment of the contractual performance.

As a legal consequence, the contractual partner is released from the obligation to perform as long as the said event continues and he cannot legally or actually fulfil his contractual obligation precisely because of this event. Neither a fault nor a delay in performance can be attributed to him – thus, he is not obliged to pay damages.

Problems can arise if Russian contract law is to be applied and embargoes or sanctions are not listed in the force majeure clause, as Russian courts often do not classify sanctions as force majeure.

Hardship

The hardship clauses become relevant when, in case of force majeure, it is still legally and factually possible for the contractual partner to fulfil the obligation to perform but only with considerable practical and financial expenditure which makes the fulfilment unreasonably difficult

over a longer period of time. Hardship clauses grant the contracting parties the right to adjust the contract (in terms of time or price) or even to terminate it. However, hardship clauses are less common than force majeure clauses.

Legal provisions

Statutory provisions can also be relevant for a release from the contractual obligations or from the contract itself. First, it must be considered which legal system is applicable. If two German companies are the contracting parties, German law is usually applicable. However, if one of the contracting parties is not domiciled in Germany, the parties often make their own choice of law. In the absence of such a choice, according to the Rome I Regulation of the EU, the national law applies to sales contracts in which the contracting party owing the performance typical for the contract has its registered office.

German law

Under German law, there are several provisions that may allow for a release from the obligation to perform, for an adjustment of the contract or for a release from the contract.

Impossibility of performance

If, for example, sanctions explicitly and strictly prohibit the export of certain goods from Germany to Russia, a German debtor's performance is legally impossible. A violation of the EU sanctions is punishable under § 18 of the Foreign Trade and Payments Act if it is committed intentionally, and under § 19 of the Foreign Trade and Payments Act it is an administrative offense if it is committed negligently. German law provides for subjective and objective impossibility. This is a case of so-called subjective impossibility (§ 275 (1) BGB). Subjective impossibility occurs when the performance is impossible for one particular debtor. As a result, if the debtor notifies his contractual partner (= creditor) of this impossibility, he is released from the obligation to perform. The creditor may in turn withdraw from the contract.

Another case of subjective impossibility occurs when the debtor is hindered to perform by practical and for him personally insurmountable obstacles. For example, the debtor could invoke it if it is not possible for him to move goods from one place to another due to blockades of transport routes caused by war, or if goods have been confiscated. Here, too, the debtor is not responsible for the impediment to performance and not liable for damages.

In addition to subjective impossibility, § 275 (1) BGB also includes objective impossibility. This occurs if the promised performance is impossible for everyone. A conceivable case of application could be the owed delivery of custom-made products or the provision of services to a Russian company, which no one else can produce or perform in the owed manner because, for example, the supplier's individual know-how is required. If this good or service may no longer be exported

to Russia, the debtor can invoke the objective impossibility of the performance to be released from the obligation.

Interference with the basis of the contract

When the contract is concluded, the performances owed to each other are typically in a relationship of equivalence. An interference with the basis of the contract occurs when this equivalence relationship is massively shifted, so that the exchanged services no longer have a value in relation to each other and an extreme loss-making transaction is threatening.

In Germany, the interference with the basis of the contract is regulated by § 313 BGB. The provision requires that (1) essential circumstances on which the contract was based have changed seriously and (2) the parties would not have concluded the contract or would not have concluded it in the same way if they had known about these new circumstances and that (3) the party burdened by this can no longer be expected to adhere to the contract after weighing the interests of both parties. As a legal consequence, the affected contracting party can demand an adjustment of the contract or withdraw from it, whereby the adjustment has priority as a milder means.

In practical terms, sanctions can induce an extreme rise in the costs for production and procurement of goods or services. As a result, these can be far higher than the agreed price or remuneration.

A massive shift in the equivalence ratio can also occur if payment obligations are to be made in another currency and the exchange rates of one's own currency and the foreign currency unexpectedly and unforeseeably differ greatly. Currently, this danger exists in particular if payments are to be made in Russian roubles instead of EUR or USD. According to German law, an interference with the basis of the contract should then be assumed. In this case, the payment creditor would also have a right to adjust or withdraw from the contract.

Russian law also recognizes the right to adjust the contract due to an interference with the basis of the contract, but changes in exchange rates/foreign exchange rates are usually not recognized as such.

UN Sales Convention

The UN Convention on Contracts for the International Sale of Goods also recognizes the exemption from the obligation to perform due to force majeure. Art. 79 CISG regulates the conditions for a release from the obligation to perform, based on a "cause of impediment beyond the control of the debtor" which could not be expected at the time of the conclusion of the contract.

Cancellation of the contract

If both parties agree that it is no longer reasonable and feasible for them to maintain the contractual relationship in the future without major problems, they can also jointly decide to terminate the contract; the basic principle of private autonomy applies.

Future contracts

When concluding future contracts, care must be taken that the promised performance does not fall within the catalogue of sanctions. Otherwise, the contracts may be invalid or void due to the violation of a statutory prohibition (§ 134 BGB).

It should also be noted that the debtor of a performance may be liable for damages to his contractual partner if he knew or should have known of an impediment to performance due to the sanctions already at the time of conclusion of the contract (§ 311a BGB).

If delivery difficulties are foreseeable or could increase due to the sanctions, new contracts should include clauses that grant a right to adjustment (e.g., price increase or refusal of performance) or a right of withdrawal or termination. In the case of foreseeable payment uncertainty, the parties could also agree on a retention of title until the price has been paid.

Investment protection and payment guarantees

Entrepreneurs should also note that Russia is taking or has taken countermeasures against the western sanctions that endanger foreign investors in Russia.

For example, companies from countries that have imposed sanctions against Russia with more than 100 employees and a balance sheet total of at least 1 billion roubles may in future be placed under the supervision of the Russian state. Further measures by the Russian government are not ruled out.

In addition, Russian companies are economically unstable. Payment defaults are to be feared. So far, it has been possible to make use of export credit guarantees as well as investment guarantees. These can no longer be relied on. The guarantees of the Federal Republic of Germany for export business to Russia, for example, have now been stopped until further notice. The consequences will also affect small and medium-sized enterprises to a considerable extent.

+ + +

The EU's Sanctions against Russia

Steffen Töhte, lawyer in Hanover

March 2022

Russia's war of aggression against Ukraine, which has been going on for more than a month now, is a major concern for European politics, especially from an economic point of view. The European Union has reacted with a whole package of economic sanctions against Russia. The measures, some of which are very far-reaching and drastic, represent a novelty in European foreign policy in their scope but also in their intensity, their reach should not be underestimated. The English trade press even speaks of a "financial warfare" with regard to the sanction measures. However, the consequences of these economic sanctions also directly affect companies that maintain trade relations with Russia. The aim of this article is to provide an overview of the most important sanction measures in force and then to show how companies can react to the difficult situation.

Finances

The SWIFT exclusion of certain Russian banks and their subsidiaries has received a lot of media attention. SWIFT (=Society for Worldwide Interbank Financial Telecommunication) is a Belgium-based organization that provides an infrastructure for financial transactions by banks. A total of about 11,000 banks worldwide are connected to the network and about five trillion dollars are transferred via SWIFT every day. This makes it the world's largest and most important network for international payments. By excluding Russian banks from SWIFT, transactions to or from Russia are virtually impossible. In the past, SWIFT exclusion has already been applied to Iran and Venezuela, with sometimes serious economic consequences for the countries concerned. The exclusion affects seven selected Russian banks, with the main exceptions being banks that are important for payment transactions in the energy sector.

The granting of new loans or credits to certain legal entities that have been included in the corresponding sanctions list is also prohibited. The only exceptions are loans and credits that are specifically and demonstrably intended to finance non-prohibited imports or exports of goods and non-financial services.

However, the economically most powerful instrument on the escalation scale so far is probably the blockade of the Russian central bank's transactions abroad. All assets of the central bank abroad have been frozen. Russia thus largely loses access to its foreign reserves which were built up through commodity trading. Without access to these foreign currencies, the rouble will be further destabilised, and devalued.

Trade in goods

Although the European Union's sanctions do not lead to a total embargo, severe restrictions apply to trade in goods with Russia. In particular, export restrictions have been further tightened with respect to certain dual-use goods by significantly expanding the list of goods through the European Union Regulation 2022/328. Dual-use goods are those with a dual purpose, meaning they can be used for civilian or military purposes. Until now, an export license had to be applied for goods included in the list of the European Union's Dual-Use Regulation. The new sanctions regulation now places a general ban on the export of such goods to Russia. The provision of technical assistance, brokering services or financial assistance are now also covered by this ban.

The newly adopted European Union Regulation 2022/328 also bans the export of goods in the aviation, electronics, IT, telecommunications, sensor technology and shipping sectors. The regulation contains lists of goods in the annexes. Among other things, this is intended to make it more difficult for Russia to modernize oil refineries and other key industries in the Russian economy.

The ban on the export of luxury goods to Russia is also new, cf. Regulation 2022/428. Several goods are affected including wines, watches, works of art or musical instruments, with separate value limits applying in each case. For most listed luxury goods, however, a value limit of €300 per piece applies. "Piece" means the good in its respective form for use/consumption (e.g. a bottle of wine).

Significant are also the additional measures undertaken by single European states. The German government, for example, has decided to suspend export guarantees (so-called Hermes cover) and investment guarantees by the German government for Russia and Belarus until further notice. Meanwhile, there is even an EU-wide ban on export credit and investment guarantees for Russia.

However, the comprehensive changes in exports do not apply to transit trade. This refers to deliveries of goods through Russia to another country.

The customs procedure is also affected by the changes. According to the German Chamber of Industry and Commerce (DIHK), ATA Carnets will no longer be issued for Russia or Belarus. A simplified customs procedure is therefore no longer possible.

In addition, an amendment to Regulation 2014/833 leads to a comprehensive import ban on iron and steel products. This applies both to goods originating from Russia and to goods from third countries exported from Russia.

Transport sector

The EU airspace will be closed to all aircraft that are either Russian-owned, Russian-registered or Russian-controlled. This has implications for European manufacturers in this sector. They are prohibited from exporting, selling, supplying or otherwise transferring aircraft and equipment to Russian airlines. This also includes all related repair, maintenance and financial services.

Further measures

The sanctions adopted are directed not only against the Russian Federation itself, but additionally against currently 893 individuals and 65 entities in Russia and abroad that support the war of aggression against Ukraine (as of March 31, 2022). The assets of the sanctioned individuals and entities have been frozen and they may also not be provided with financial resources. Individuals are also banned from entering the country. The names of the individuals and entities concerned can be found in the Official Journal of the European Union.

Large parts of the sanctions have also been extended to Belarus.

With regard to the Donetsk and Luhansk regions, there is a comprehensive trade embargo, Regulation 2022/263. Goods from these regions may no longer be imported into the European Union in principle.

Violation of the sanctions

Violation of EU sanctions constitute criminal or administrative offenses. The legal basis are Sections 18 and 19 of the Foreign Trade and Payments Act and Section 82 of the Foreign Trade and Payments Ordinance. In addition, companies face heavy fines. Above all, however, they run the risk of being included in one of the sanctions lists in the event of serious violations.

Effects on business practice

The highly dynamic events surrounding the sanctions already imposed against Russia are complex and confusing. However, this in no way exempts affected companies from adapting to the new legal situation and taking the necessary actions to this end. All sanction regulations of the European Union take immediate effect from the time they come into force, without the need for an act of transposition into national law.

First of all, all processes in the company should be checked for possible references to Russia or

Belarus. The initial focus must be on possible business contacts with sanctioned persons or entities. This applies to both existing business contacts and new business. To this end, it is advisable to conduct in-depth research in the case of suspicious business contacts.

With regard to the European sanctions list, it is advisable to use a website where the various legal acts containing sanctions lists can be searched, for example (in German): <https://www.finanz-sanktionsliste.de/fisalis>. If there are also business contacts with US companies, the “SDN List” and the “Entity List” of the BIS should also be checked. If a business contact appears on one of the sanctions lists, the trade relationship must be terminated. Basically any business contact with sanctioned persons is prohibited. At a minimum, a detailed case-by-case review is required to determine whether certain legal transactions are feasible.

For the export of goods to Russia or Belarus, the tightening of export restrictions must be observed. However, some sanctions regulations contain so-called old contract clauses. This means that contracts already concluded can still be fulfilled in individual cases despite the existing export ban. As a rule, however, the prerequisite for this is that the contract was concluded before February 26, 2022, that it involves non-military end users and that the transaction is carried out for non-military purposes. Furthermore, a special authorization must be applied for from the competent authority (i.e., the BAFA in Germany) in due time.

Existing Hermes cover continues to protect exporters against non-payment from Russia. If deliveries to Russia are still outstanding, the coverholder Euler Hermes should be contacted. In the case of collective cover (whole turnover policies), cover is no longer available for new shipments to Russia.

If business relationships exist with Russian banks that are affected by the SWIFT exclusion, payment transactions should be stopped. If possible, money shall be transferred from a sanctioned bank's account to non-sanctioned banks. In this case, it is essential to notify the change of account details to all relevant contractual partners.

Regarding Donetsk and Luhansk regions, all transactions should be stopped.

The company's IT infrastructure must also be examined for risks. Particularly Russian software (e.g., “Kaspersky”) should be viewed critically against the backdrop of cyberattacks. The German BSI (Federal Office for Security and Information Technology) also reports a significant increase in hacker attacks during the Ukraine conflict. Medium-sized companies are also affected.

In addition to the sanctions-related effects on business practice, the actual consequences of the war must also be taken into account. Airspace closures, interrupted rail links - especially to China - a lack of fuel and a shortage of logistics personnel are leading to severe disruptions in supply chains. Delays are to be expected here, with no end to the supply bottlenecks in sight.

If legal or factual circumstances cause problems in the fulfilment of contractual obligations to

Russian companies, it must be examined in each individual case to what extent legal claims for fulfilment, adjustment of the contract or termination of the business relationship can be considered. This depends to a large extent on the specific contractual agreements between the parties. It should be noted, however, that some of the sanctions regulations themselves contain provisions in this regard.

+ + +

Business related sanctions in Russia

Thomas Brand, attorney at law, Brand & Partner, Moscow

April 2022

Sanctions between the EU and Russia are also hurting uninvolved entrepreneurs. While the sanctions imposed by the EU (exclusion of several Russian banks from the SWIFT system, embargoes on certain groups of goods and the sanctioning of certain individuals) are well known, there is often no precise knowledge about the restrictions imposed by the Russian side, which also and especially affect Western entrepreneurs with activities in Russia.

The Russian president has already signed several counter-sanctions decrees that, among other things, "establish a special procedure for doing business with foreigners associated with states that commit unfriendly acts against the Russian Federation and its citizens."

Here you will find the most important information and updates, with a focus on the areas of business and law.

Transactions with real estate and securities in Russia require approval

On March 6, the Russian government issued new rules for transactions with companies from "unfriendly countries." Russian companies must submit transactions with companies and individuals from "unfriendly countries" to a specially established governmental commission on foreign investment for approval. The new regulations cover the granting of loans (in rubles and foreign currency) and the purchase and sale of securities and real estate, as well as other transactions. The governmental commission may approve the proposed transaction with or without reservations or reject it. Real estate transactions between foreigners and Russian citizens are considered approved.

Russian companies are obliged to exchange foreign currency into rubles (Presidential Decrees No. 79, No. 126, Instructions of the Central Bank)

Russian companies (and thus also subsidiaries of Western companies) have been required to exchange 80% of foreign currency received from foreign companies under foreign trade contracts into rubles since February 28, 2022. This requirement applies to foreign exchange received in Russian accounts on or after January 1, 2022. The mandatory exchange must be made within three working days from the date of receipt of the foreign currency, or now for the first time for all amounts received since January 1, 2022. In addition, as of March 1, foreign exchange transactions related to the provision of foreign currency by residents for the benefit of non-residents under credit agreements are prohibited.

Since March 25, the Central Bank has introduced a procedure providing for exemptions from general rules for the sale of foreign exchange proceeds and payment of shares, capital contributions for non-residents.

The decision establishes the procedure by which the Central Bank grants permission:

- Sale of currency proceeds later than 3 days;
- Reduction of foreign currency sales by the amount of foreign currency liabilities to Russian banks;
- Payment of interest, contributions or shares in the capital/assets of a non-resident;
- Transfer of foreign currency to a non-resident under a corporate contract.

The decision also provides for the list of documents required to obtain a permit. The Central Bank shall issue a permit or a refusal within 10 working days of receipt of all required documents.

Foreign exchange restrictions for private individuals

Private individuals have been allowed to export a maximum of USD 10,000 since March 2 (calculated according to the current central bank exchange rate). Foreign currency transfers made by foreigners who do not work in Russia and come from unfriendly countries are fully restricted for 6 months.

In addition, a ban on export of foreign currency in cash equivalent to more than 10 thousand US dollars from Russia was introduced from 2 March 2022.

The Central Bank ordered that citizens can withdraw only 10 thousand US dollars in cash from foreign currency accounts until September 9, regardless of the currency. Payments above this amount will be made in rubles. VAT will no longer be charged on the sale of gold bars and coins. On March 25, the Central Bank of Russia published a decision on further restrictions on payments abroad. Within the framework of its powers under the Presidential Decree of March 18, the Central Bank has set a ceiling on the payment of advances by residents to foreign legal entities and individuals.

The ceiling is 30% of the amount of obligations under each contract and applies to:

- Service contracts and work execution contracts by non-residents;
- Contracts providing for transfer of information and results of intellectual property/activity.

The Central Bank's Decision of 25.03.2022 provides for certain exceptions, e.g. for resident credit organizations as well as for financial services contracts.

Under the decision, non-residents - legal entities from "unfriendly" states - cannot buy currency in Russia.

Capital Controls

On March 18, 2022, the Russian President signed a decree on further temporary measures in the area of foreign exchange regulation to ensure financial stability. The decree enacts a new procedure for meeting obligations to certain foreign creditors. Under this decree, certain transactions require the approval of the Russian Central Bank. Normal commercial transactions are generally not affected. The granting of loans to subsidiaries and the distribution of dividends from Russian limited liability companies to their foreign shareholders are not affected by the decree.

In addition, the Central Bank is authorized to restrict the scope for remittances to foreign companies and individuals. The Central Bank may grant a resident person conducting foreign trade transactions permission to meet the requirements for compulsory exchange of foreign currency under Decree No. 79 of February 28, 2022, within a period other than that provided for, or to exempt such person from compulsory exchange altogether. The document regulates, for example, advance payments by residents in favor of non-resident legal entities and individuals under contracts, transfers of funds from accounts opened with Russian credit institutions, and purchase of foreign currency on the Russian foreign exchange market.

External administration for companies with foreign participation planned

The Russian government plans to introduce a draft law "On External Administration for the Administration of Organizations" to the Russian Parliament in the near future, which, among other things, will regulate the procedure for appointing external administration for Russian companies with foreign shareholders from so-called "unfriendly states".

The draft law has already been approved by the "Governmental Commission for Legislative Activities". On March 16, the Tax Service and the Central Bank expressed their comments. Whether and when the draft law will be introduced into the parliament, the Duma, has not yet been determined.

The aim of the law is to prevent subsidiaries of foreign companies from ceasing their activities in Russia for no reason or for political motives, thus endangering jobs and the Russian economy as a whole. The draft law stipulates that the foreign management function is to be transferred to the state-owned company "VEB.RF" (State Investment Company for the Promotion of Russian Development Projects), which, among other things, carries out the fiduciary management of state assets. In the case of financial organizations, i.e. banks in particular, these functions are to be performed by the "Agency for Deposit Insurance", which acts as insolvency administrator for insolvent banks.

However, third-party administration is envisaged only in the case of larger companies that meet the following criteria:

- the foreign participation from an "unfriendly state" is above 25%;
- the book value of the company's assets according to the latest financial statements exceeds RUB 1 billion (approx. EUR 8.2 million) and/or the average number of employees in the month preceding the application for the appointment of third-party administration exceeds 100 people;
- the company's activities have ceased in violation of the law.

Please note that it is not yet clear whether this bill will be approved, and if so, in what version. Currently, the Draft is being actively discussed among business community.

Export ban and legalization of parallel imports

The government has drawn up a list of goods and equipment previously imported into Russia from abroad that are temporarily banned from export from Russia.

Presidential Decree No. 100 of March 9, 2022:

prohibition and restrictions on import and export of certain goods and raw materials until December 31, 2022.

Government Decree No. 311, dated March 9, 2022:

Prohibition on the export of over 200 types of goods, esp:

- household appliances;
- medical devices;
- technical products;
- agricultural products;
- electrical equipment.

Government Decree No. 313 of March 9, 2022:

Ban on export of the following goods to "unfriendly countries" (esp. EU):

- wood;
- raw wood materials;
- wood coating materials;
- other untreated wood materials.

Government Decree No. 506 dated 29.03.2022

The Russian government has decided to allow the import of original goods of foreign origin without the consent of the rights holders (parallel import). The liability for parallel import is abolished.

Previously, this was officially permitted only with the consent of the rights holder. The Ministry of Industry and Trade is currently drawing up a list of goods that can be imported without the consent of the right holder. This is intended to make it possible to circumvent foreign sanctions for the benefit of Russian consumers, especially in the luxury goods segment.

The basis for this permissibility of parallel import is an amendment to the law of 08.03.2022 (Federal Law No. 46-FZ).

However, the goods imported to Russia will continue to be subject to all necessary customs and control procedures.

+ + +

The EU Approach to Supply Chains

Steffen Töhte, lawyer in Hanover

February 2022

After the German legislature passed the "Law on Corporate Due Diligence in Supply Chains" (LkSG) in June 2021, the EU Commission is now also presenting a draft directive on corporate due diligence. In the future, companies will be obliged at the EU level to identify, prevent, eliminate, or reduce the negative impact of their activities on human rights and the environment. The draft directive goes beyond the German Supply Chain Act in terms of both scope and content of the due diligence requirements and places greater obligations on companies.

Scope

According to the draft directive, the new due diligence obligations apply to all corporations based in the EU with more than 500 employees and a global net turnover of more than 150 million euros (Group 1). Companies that do not meet both thresholds will still be required to comply if they are primarily active in certain resource-intensive industries and have more than 250 employees and global net sales of more than EUR 40 million (Group 2). According to the final catalog, resource-intensive industries comprehend the textile industry, agriculture and forestry (including fisheries, food production, wholesale trade in agricultural raw materials, live animals, timber, foodstuffs and beverages), and the extraction of and trade in mineral resources and raw materials. However, the regulations will not apply to Group 2 companies until two years later. Regardless of the number of employees, companies from third countries will also be addressed if they generate sales of either EUR 150 million in any industry or EUR 40 million in one of the resource-intensive industries within the EU.

According to estimates by the EU Commission, the directive would affect around 13,000 European companies and 4,000 companies from third countries operating in the EU. This means that 99 percent of the European economy, in particular small and medium-sized enterprises (SMEs), would not fall within the direct scope of the new due diligence requirements. Indirectly, however, they may be affected, for example as suppliers to large companies, if these in turn are obliged to provide a proper supply chain.

From a factual point of view, the due diligence obligations basically cover the entire value chain. The business activities of the companies concerned, and their subsidiaries are covered. The supply chains must be monitored in both directions for possible violations of the provisions of the directive: this applies to suppliers and customers. According to the wording of the draft directive, however, the obligation to monitor within the supply chain is limited to those companies with which there is an established business relationship. The draft directive defines such an es

established business relationship as a direct or indirect business relationship which, due to its intensity or duration, is or is expected to be permanent and does not merely represent an insignificant or incidental part of the value chain. What exactly is meant by this remains unclear and is likely to be a point of discussion in the further legislative process.

Extension of due diligence obligations

The legislative goal of the EU Commission is to ensure that companies respect human rights and comply with environmental standards within their global value chain. This includes, for example, the prevention of child and forced labor, the creation of safe and healthy working conditions, and fair wages. A practical example of a violation of environmental standards is the sometimes excessive water pollution caused by mining for the extraction of raw materials.

To achieve this goal, companies must make due diligence an integral part of their corporate policy, identify actual or potential negative impacts on human rights and the environment, prevent or mitigate potential impacts, eliminate or minimize actual impacts, establish a grievance mechanism, monitor the effectiveness of due diligence policies and measures, and communicate publicly about their due diligence performance.

If companies have identified violations of human rights or environmental standards in their value chain, they must take appropriate measures depending on the severity of the violation in each individual case. In the case of minor violations or suspected violations, it may be sufficient to enter into contractual agreements within the supply chain, whereby the draft directive explicitly requires that contractual agreements must always be accompanied by appropriate measures for verification and compliance. In the event of serious violations, a company may also be obliged to terminate the business relationship completely. This could present companies with the difficult practical task of finding new suitable suppliers, as supply chains worldwide are already under strain.

Direct due diligence obligations with regard to negative consequences for the climate have not yet been stipulated in the draft directive. However, companies in Group 1 must have a plan to ensure that their business strategy sufficiently takes into account the goals of the Paris Climate Agreement (limiting global warming to 1.5° C).

The draft directive also does not contain any provisions on the import of products manufactured using forced labor. However, the EU Commission is already working on a separate legal instrument. This should prevent such products from entering the European market in the future.

Sanctions

The draft directive contains various sanction mechanisms for breaches of the due diligence. On

the one hand, it obliges the member states to create suitable and appropriate sanctions when transposing the directive into national law. In particular, fines are to be imposed on the companies concerned. The amount of the fine is to be based on the company's turnover. Companies that are required to draw up a climate plan (especially Group 1) are also to make the payment of bonuses to management dependent on compliance with the climate plan.

According to the draft directive, companies that have violated their due diligence obligations should, under certain circumstances, be liable under civil law for damage that has occurred along their value chain. Those affected by human rights violations or environmental damage could thus claim compensation from companies in the EU. However, the draft directive does not provide for any easing of the burden of proof in favor of the affected parties. Potential plaintiffs would still have to present and prove all the requirements for a claim for damages. On the other hand, a genuine exclusion of liability for companies is only envisaged in cases where the obligated company has already obtained contractual assurances along the supply chain, additional protective measures were not initiated and the damage that occurred was caused by an (indirect) supplier.

Comparison with German supply chain law

The structure of the draft directive is based on the German Supply Chain Act, but its content goes beyond it in many respects. First, the scope of the directive is broader. For example, from 2023 the German regulations will only apply to companies with more than 3,000 employees, with the limit being lowered to 1,000 employees from 2024. Nevertheless, this is still twice as many employees as in the draft directive. According to the will of the EU Commission, significantly more companies would therefore be directly affected by the due diligence obligations. Also, the control obligations for companies under the German Supply Chain Act generally only apply to the direct supplier, while the draft directive establishes control obligations for the entire value chain.

It is also striking that the German Supply Chain Act does not contain any provisions relating to climate protection, bonus payments or liability. In particular, the issue of civil liability for damage along the value chain, which has been intensively debated in this country, is likely to become an issue again in the wake of the EU directive.

Next steps

The draft directive will now be submitted to the European Parliament and the Council. There, the draft will be discussed and voted on, and if necessary, amendments will be proposed. Once the final version of the directive has been adopted, the member states will have two years to transpose it into national law. In this case, for example, the German Supply Chain Act would

have to be adapted to the then applicable European requirements. Only then will the directive take legal effect for German companies in the form of the German implementation.

Practical implications

The EU Directive is expected - irrespective of its final version - to stipulate higher due diligence requirements for the companies addressed. On the one hand, more companies than before could be obliged to monitor their supply chain. Secondly, the control obligations are then likely to extend further than just to the direct supplier. Above all, contractual agreements to fulfill due diligence obligations will probably increase. This will not only affect companies within the scope of the directive, but also SMEs as part of the value chain. To this end, the draft directive explicitly urges member states to support SMEs in fulfilling their due diligence obligations. The member states are to set up and operate appropriate websites, platforms, and portals for this purpose.

The trend toward certification is also likely to increase. By obtaining certificates (EMAS, Green Button, SMETA, etc.), companies can more easily prove that they meet certain human rights or environmental standards. Certificates make the supply chain more transparent and increase the reputation and attractiveness of a company, especially in the face of increasing due diligence requirements. It is also possible that the EU directive will lead to a concentration of suppliers. From a market economy perspective, the directive is intended to ensure a fairer playing field. Companies should not enjoy any advantage by violating human rights or environmental due diligence obligations. The extension of the scope of application to companies from third countries is also intended to contribute to this.

However, one thing can already be said with certainty: For companies, especially in the so-called high-risk industries, the monitoring and control of their own value chain will become increasingly important in legal terms. Because of the threat of sanctions and the potential risk of civil liability, companies should be required to examine their business relationships and supply chains for any violations and remedy them as soon as possible.

Regardless of the fate of the draft directive, the German Supply Chain Act will already come into force in large part on January 1, 2023.

+ + +