

ALLIURIS ACADEMY | SUMMER SCHOOL 2020

DIGITAL BUSINESS & LAW

VIRTUAL, 20 - 24 JULY 2020

ORGANISED BY HERFURTH & PARTNER, HANOVER

Alliuris Summer School

20 – 24 July 2020

Corona Epidemic – Catalyst of Digitalization

Effects of Corona epidemic on contractual relations, dealing with law and work from home, global data protection and other legal issues related to digitalisation.

**ALLIURIS ACADEMY
SUMMER SCHOOL 2020**

Alliuris Academy Director:
Giuseppe Cattani, Avvocato, Milan

Legal Content Management & Moderator:
Antonia Herfurth, Rechtsanwältin, Hannover/Munich

Organisation & Conference Management:
Alisha Daley-Stehr, Hannover

Concept & Supervision:
Ulrich Herfurth, Rechtsanwalt, Hannover/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 Summer School 2020 took place from the 20th to 24th July. Due to the Covid-19 pandemic, unfortunately, there could not be a personal meeting, but instead of missing the conference, Alliuris had its first virtual Summer School. It was organised by Herfurth & Partner.

This new format of the Alliuris Academy was of great interest for the young lawyers, since there were 43 registrations from twelve countries all over the world – from China to Mexico.

Because of the current situation, this year's program was about "Corona Epidemic – Catalyst of Digitalization". The participants listened to presentations about the Corona epidemic as force majeure, work from home, business platforms, artificial intelligence and had an update on international data protection. The interesting and very up to date program was enriched by speakers from the UK, the Netherlands, India and Germany.

Although the participants enjoyed the Summer School, due to the virtual format there was no real social part of the conference this time. But hopefully we can catch up on it in a later stage in the future. Because Alliuris conferences are not only intended to be a source of know-how but also a platform for good personal cross border relations among the attendants – the strength of the Alliuris group.

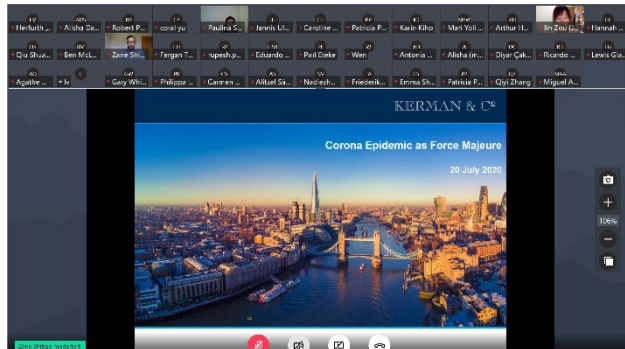
This report contains the subjects and materials that were contributed. We hope that this is another helpful stepstone for our young lawyers and helpful information for our member firms.

Hannover / Milan, July 2020

*Ulrich Herfurth
Chairman of the Board*

*Giuseppe Cattani
Academy Director*

Corona Epidemic as Force Majeure



Zane Shihab and Robert Paydon from Kerman & Co in London made the start of this year's Alliuris Academy with presentations about "Corona Epidemic as Force Majeure". While Zane's presentation dealt with "Commercial Contracts from a Sporting Perspective in relation to Force Majeure and Frustration", Robert guided the

young lawyers through "The English Court Process and how Disputes are resolved". Zane started by presenting the immense impact of Covid-19 on sporting and music events. He explained what is meant by force majeure and how to draft a force majeure clause without drafting mistakes which might exempt liability. Furthermore, the participants learned about the relation of force majeure clauses and the doctrine of frustration.

The second half of the speech was presented by Robert who introduced the young lawyers to the English litigation process. As there were participants attending from the Common law legal system as well as the Civil law legal system, he started by explaining the principles of Common law and the English legal (court) system. Afterwards, he deepened the explanation of the court proceedings and explained necessary steps, documents and the process of the proceedings.

Work from Home

Since work from home is a pervasive topic now – not only for lawyers advising their clients but also for everyone working from home –, the second day of the Alliuris Academy was all about remote work. It started with an open discussion guided by Alexander Steenaert from Marree en Dijkhoorn in Amersfoort. The young lawyers debated questions such as "Can an employer force an employee to work at home or, the other way around, to come to the office during the pandemic?", "What to do when an employee wants to come back to office even if he should stay at home due to extraordinary circumstances like Covid-19?"

Can the employer force him to stay at home?". The open discussion was followed by a presentation of Antonia Herfurth from Herfurth & Partner about home office agreements, their structure and rules. She explained important points to regulate in a home office agreement, important from the employer's as well as from the employee's point of view. Before the start of the Summer School, several questions were sent to the participants. In order to design the agreement, Antonia reviewed the participant's answers to the question "Which rules would you provide when drafting a "Work from Home"-agreement with employees?" and assembled them to an agreement. At the end of the day, the participants were provided with the jointly developed home office agreement.

Update on international Data Protection

Dr Manoj Kumar from Hammurabi & Solomon Partners in New Delhi updated the young lawyers on data protection in India in 2020. Within this frame, he talked about data protection, privacy and digitalization compliance for businesses. Dr Kumar has contrasted the Indian data protection regime with the EU data protection regime. For the lawyers, it was interesting to see where similarities lie and where differences lie. Dr Kumar's presentation was followed by a guest speech of Constantin Herfurth from Eversheds Sutherland in Munich.

Constantin gave a presentation on "International Data Transfers under the GDPR", so the participants had a complete picture of the actual data protection regime not only on an international level but also in the EU. Because of the current boost of videoconferences, the day ended with the question whether and, if yes, under which circumstances videoconferencing tools are compliant with data protection rules. Dr Kumar shared "The Indian Compliance Regime on the Data Processing Issues that confront Videoconference Service Providers" and Antonia gave a brief overview on videoconferencing providers which are considered as compliant with the GDPR.

Business Platforms

On the fourth day of the Academy, Ulrich Herfurth from Herfurth & Partner introduced the young participants to business platforms, their legal framework and problems. He covered the topics types of platforms, business and legal structures, liability, copyright, fake news and hate speech, competition law and ethics for platforms. Ulrich sensitised the young lawyers to the areas of law platforms reach into, depending on the type of platform and the actions of the users on the platform.

As the legal relationships of the parties connected to a platform, that is the platform itself, the shop and the consumer, are often not obvious, Ulrich illustrated how the parties are legally involved with each other. Furthermore, he explained how platforms are subject to data protection rules and taxation. Product and tax liability were topics touched as well as fake news and hate speech. In the latter case, Ulrich presented the German legal solution against it, the Network Enforcement Act. The speaker disclosed how networks and platforms develop a digital market power and how they have an impact on the market. The participants learned about a draft of an amendment to the German Law against Competition Restrictions which provides new criteria for dominant market power.

Artificial Intelligence

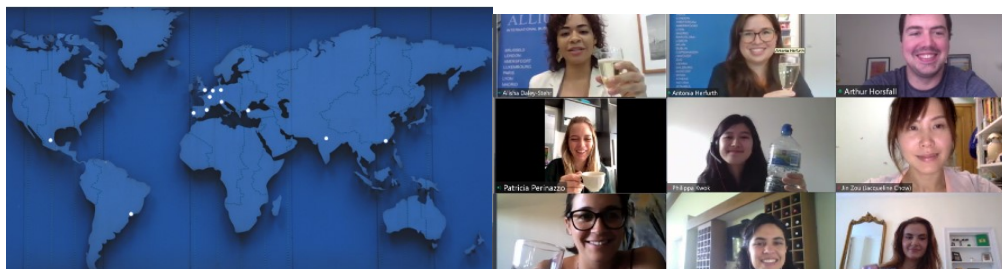


The week ended with the topic “Artificial Intelligence”. Ulrich Herfurth started his speech from the very beginning when defining “AI”, showing the background of AI and explaining the functioning of it. He continued by presenting which applications work with AI, on

how AI influences markets, the state and society. The second half of the presentation focused on AI in the legal framework: contracts, liability, data protection, intellectual property, management liability, competition law, regulatory, legal personality and ethics. Following on from the topic AI and ethics, the participants discussed openly about questions such as “Which ethic rules shall apply for the use of AI?” or “Who is liable for acts of AI?”. Inspired by the movie “Her”, the young lawyers debated whether it might be possible that an AI will be so humanised in the future that it is possible to get married to it or to appoint it as an heir.

Virtual Prosecco Date

The Summer School is not only about the professional exchange and getting to know young lawyers from other countries, but it is also, equally important, about the common social aspect. Usually the participants are making sightseeing trips together, enjoy local cuisine and learn more about the host country. Although a virtual conference does not provide such a common social experience, the participants did not want to miss it completely. Hence, they ended the Summer School together with a “Prosecco Date” on Friday afternoon.



Summer School Comments

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

"It's a pleasure and I'm very pleased to have the opportunity to participate in this great Alliuris Summer School. Time goes fast, today would be the last day for the event and we are going to learn and share some ideas about AI development issues and regulations and rules on AI as well with lawyers worldwide together. ... Looking forward to the last session about AI and toast for success of the first virtual Alliuris Summer School! Thank you very much!"

- Jacqueline Chow, Guangzhou -

"It has been a true pleasure to be part of this Summer School, hopefully we will be able to meet in person sometime in the future."

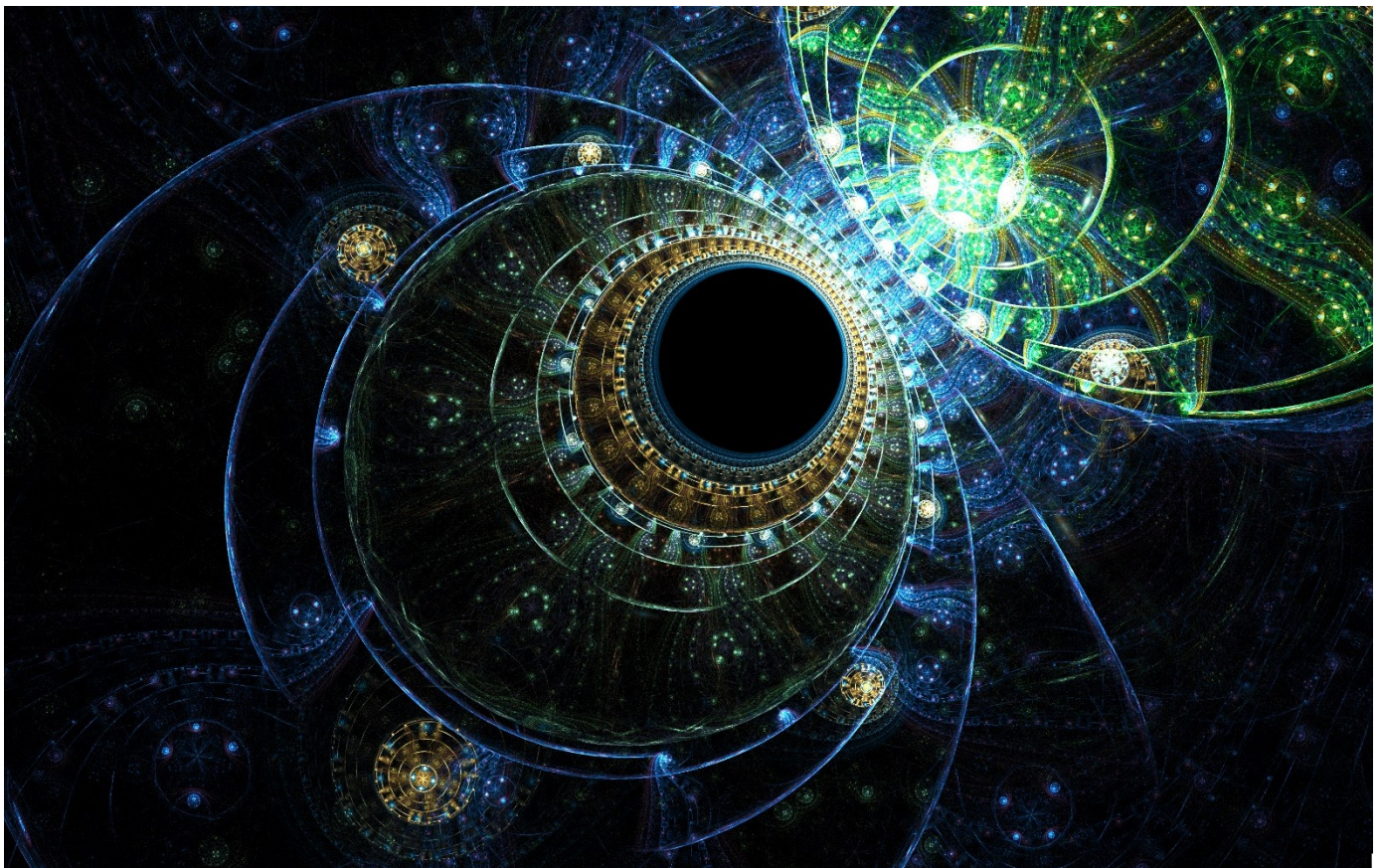
- Maria Inês Reis, Lisbon -

"I had the same feedback from Carmen Vidal, one of our young lawyers (who also attended the Madrid meeting). She is already a fan of Alliuris Summer School!"

- Toni Fitó, Partner, Barcelona -

"We also had a couple of young lawyers participating the virtual Summer School and they enjoyed very much the format and the experience. No doubt, the social part and the possibility of meeting colleagues from other jurisdictions in person is a plus that cannot be easily replaced, but also this virtual edition of the Academy was definitively a success!"

- Giuseppe Cattani, Partner, Milan -



ALLIURIS ACADEMY

SUMMER SCHOOL
VIRTUAL, 20 - 24 JULY 2020

ORGANISED BY
HERFURTH & PARTNER, HANOVER

VIRTUAL

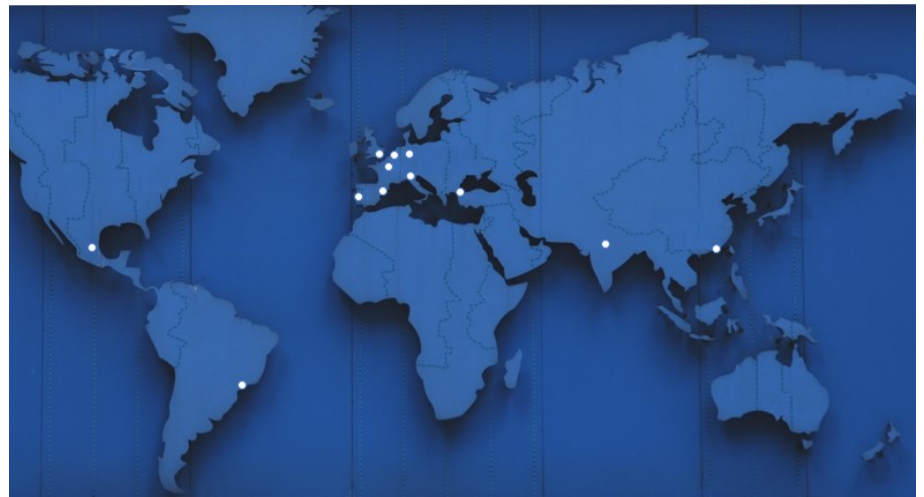




The Speakers and Organisers of the Alliuris Summer School 2020

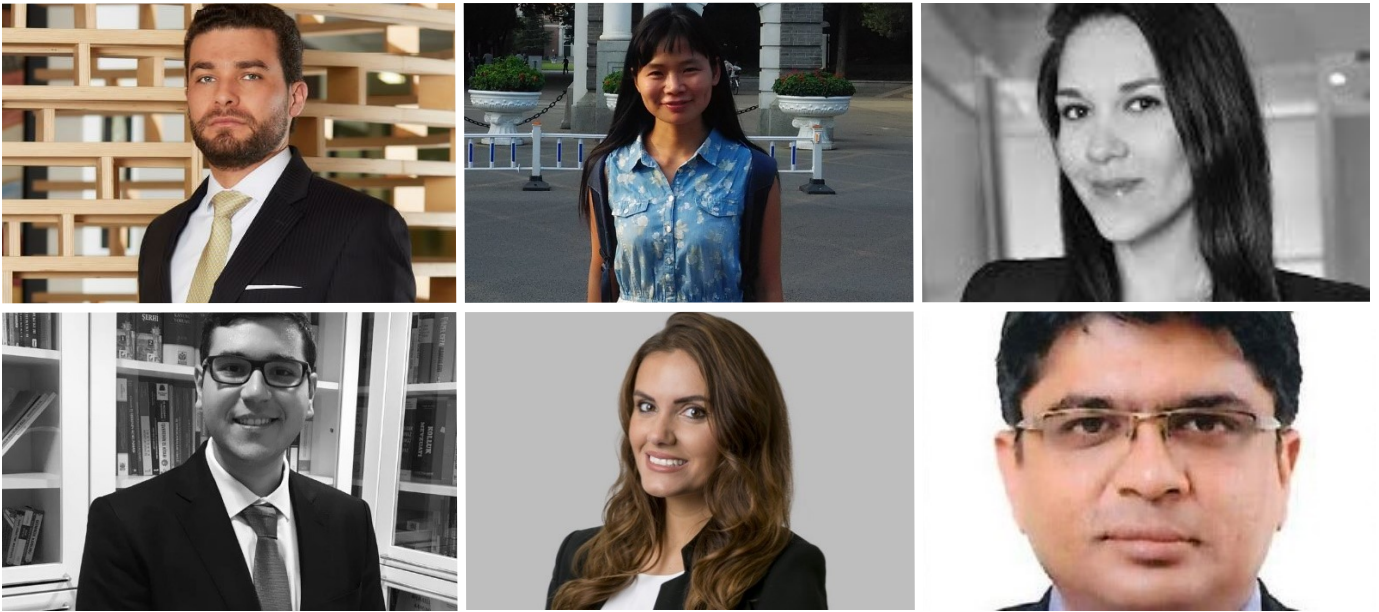
Herfurth & Partner in Hanover organised the conference





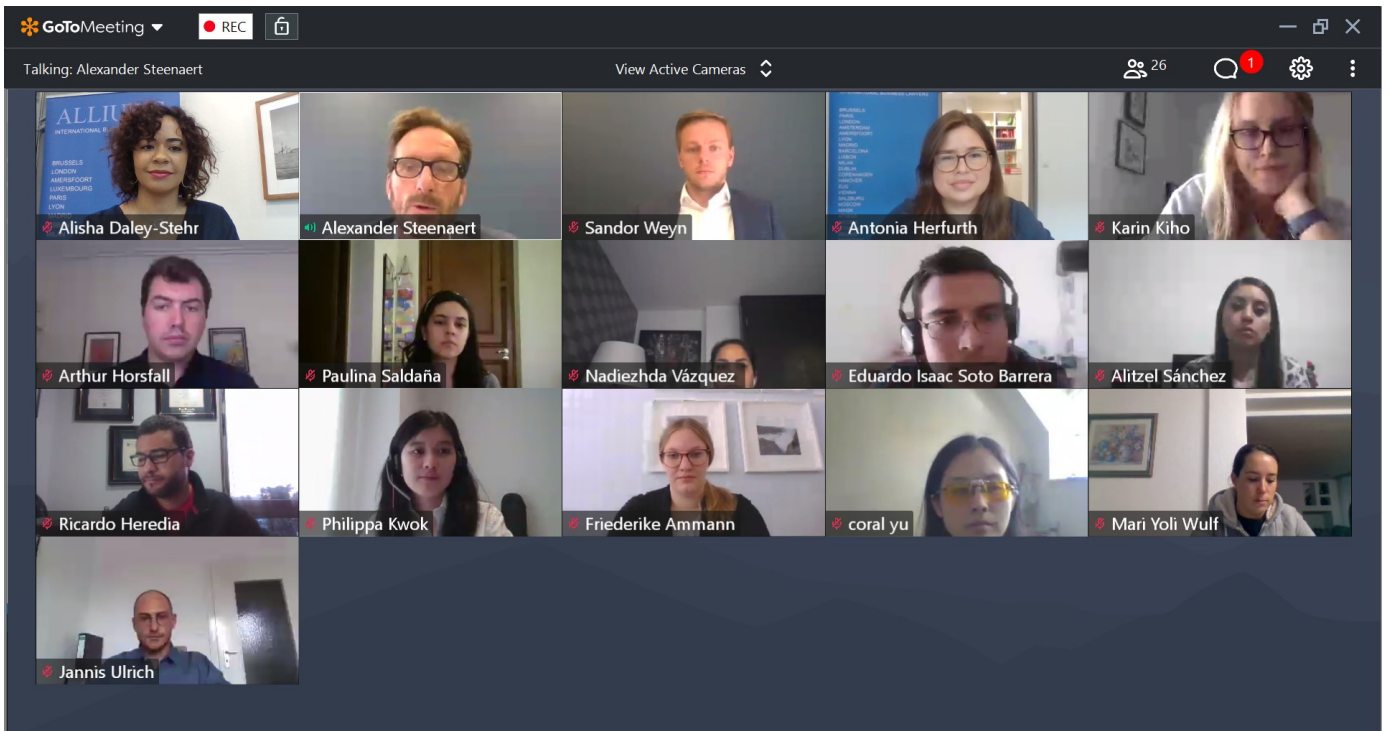
Young lawyers from China, India, Turkey, Germany, the Netherlands, France ,UK, Italy, Spain, Portugal, Brasil and Mexico attended the Summer School





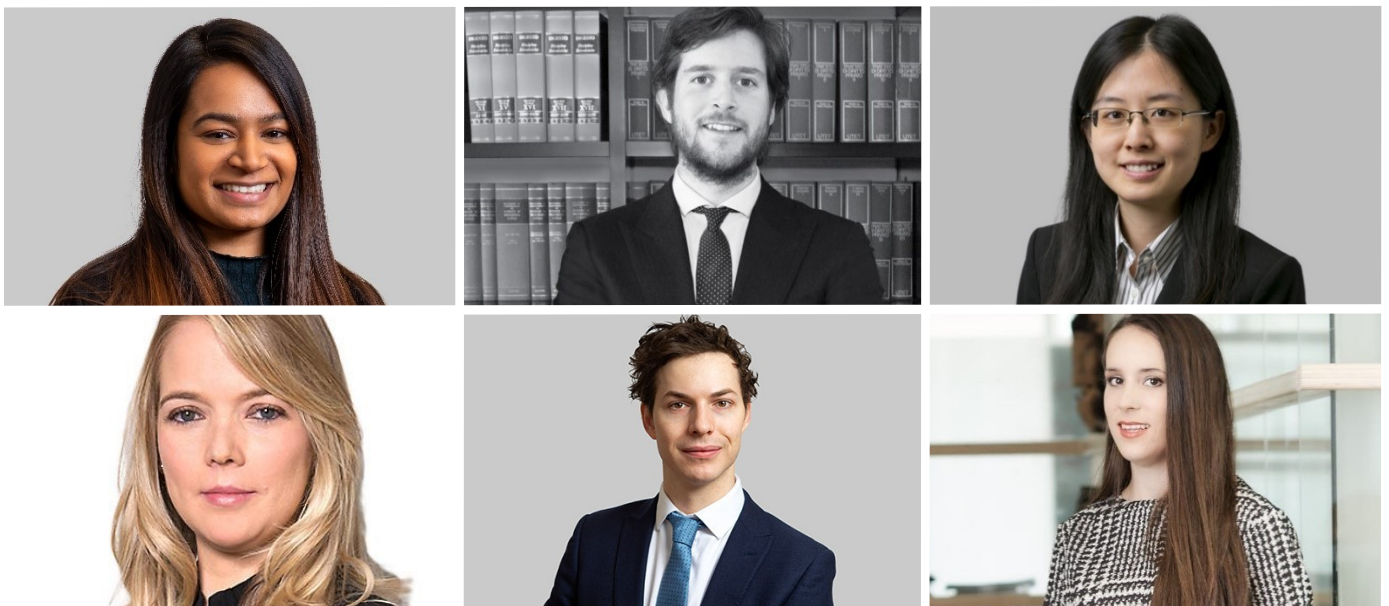
Day 1 of the Summer School: “Corona Epidemic as Force Majeure”





Day 2 “Work from Home”: Open discussion about question “How to apply data security and apply data protection mechanism in the case of work from home?”

A presentation slide with a blue background. At the top right, it says 'herfurth.partner'. The main title is 'Home Office Agreement'. Below the title, it reads 'Antonia Herfurth, Attorney at Law in Munich and Hanover, 21 July 2020'. The slide features a photograph of a modern building's glass and steel dome structure.





 **HAMMURABI & SOLOMON**
PARTNERS

INDIA 2020: DATA PROTECTION, PRIVACY & DIGITALIZATION COMPLIANCE FOR BUSINESSES

(An Outline on Data Protection Regime in India)

Dr. Manoj Kumar
Founder & Managing Partner

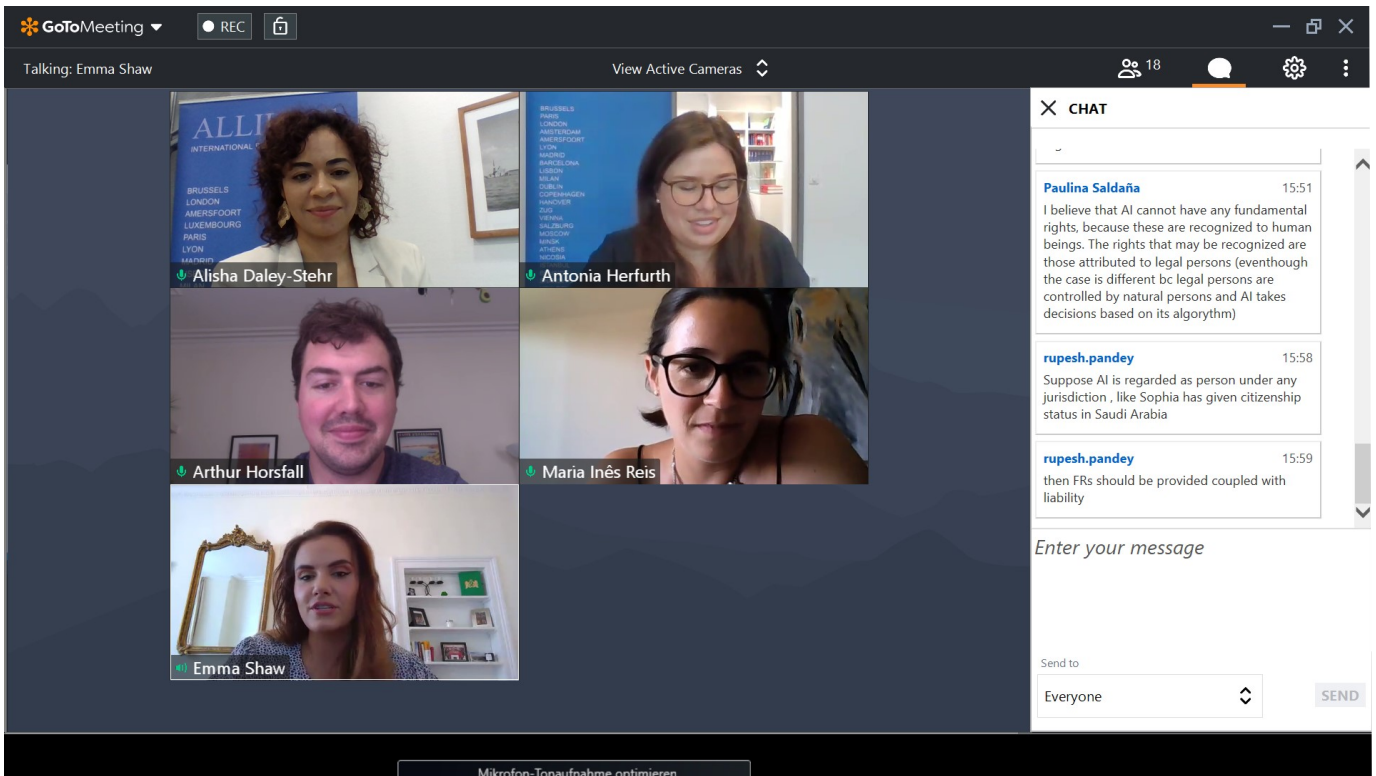
22/07/2020
©hammurabisolomonpartners

EVERSHEDS SUTHERLAND

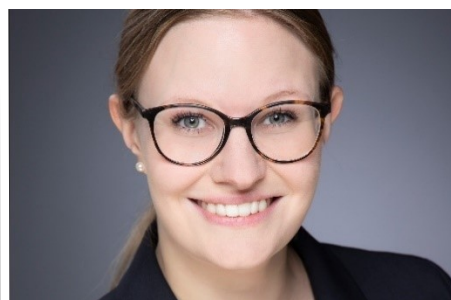
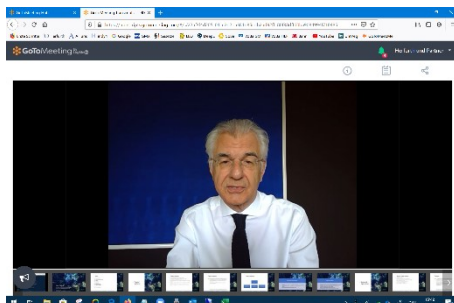
International Data Transfers under the GDPR

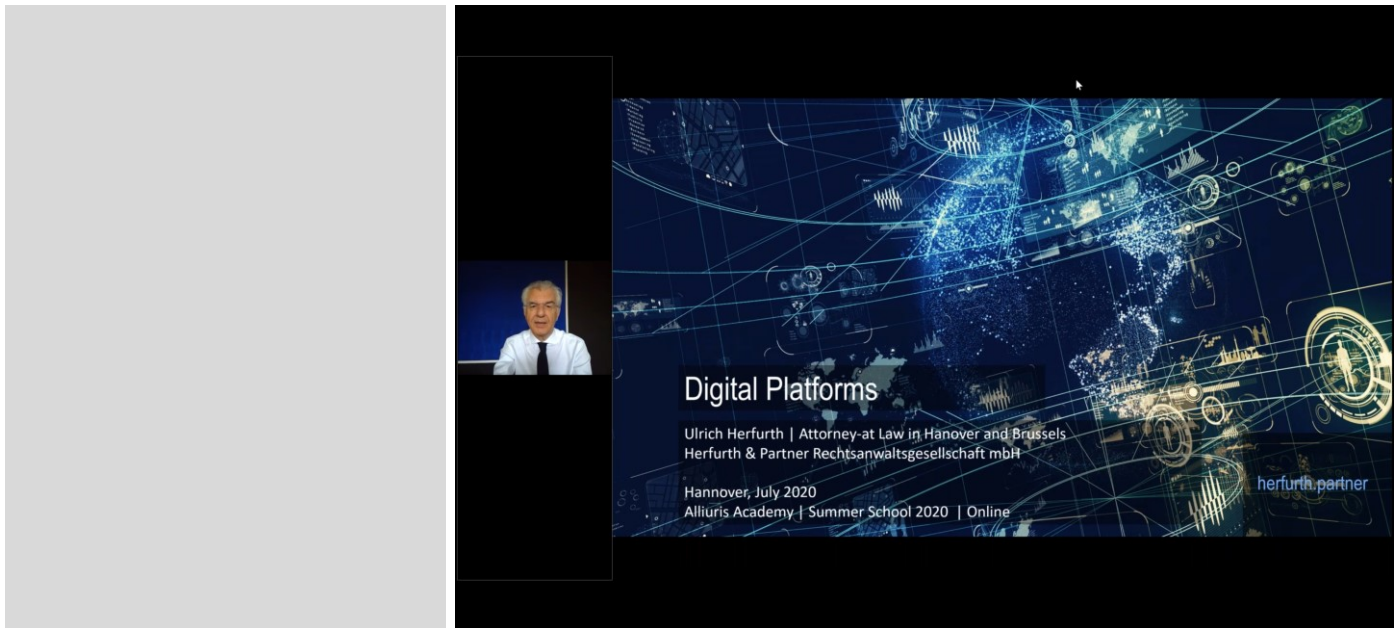
22. July 2020
Constantin Herfurth
Associate
Data Protection & Cybersecurity



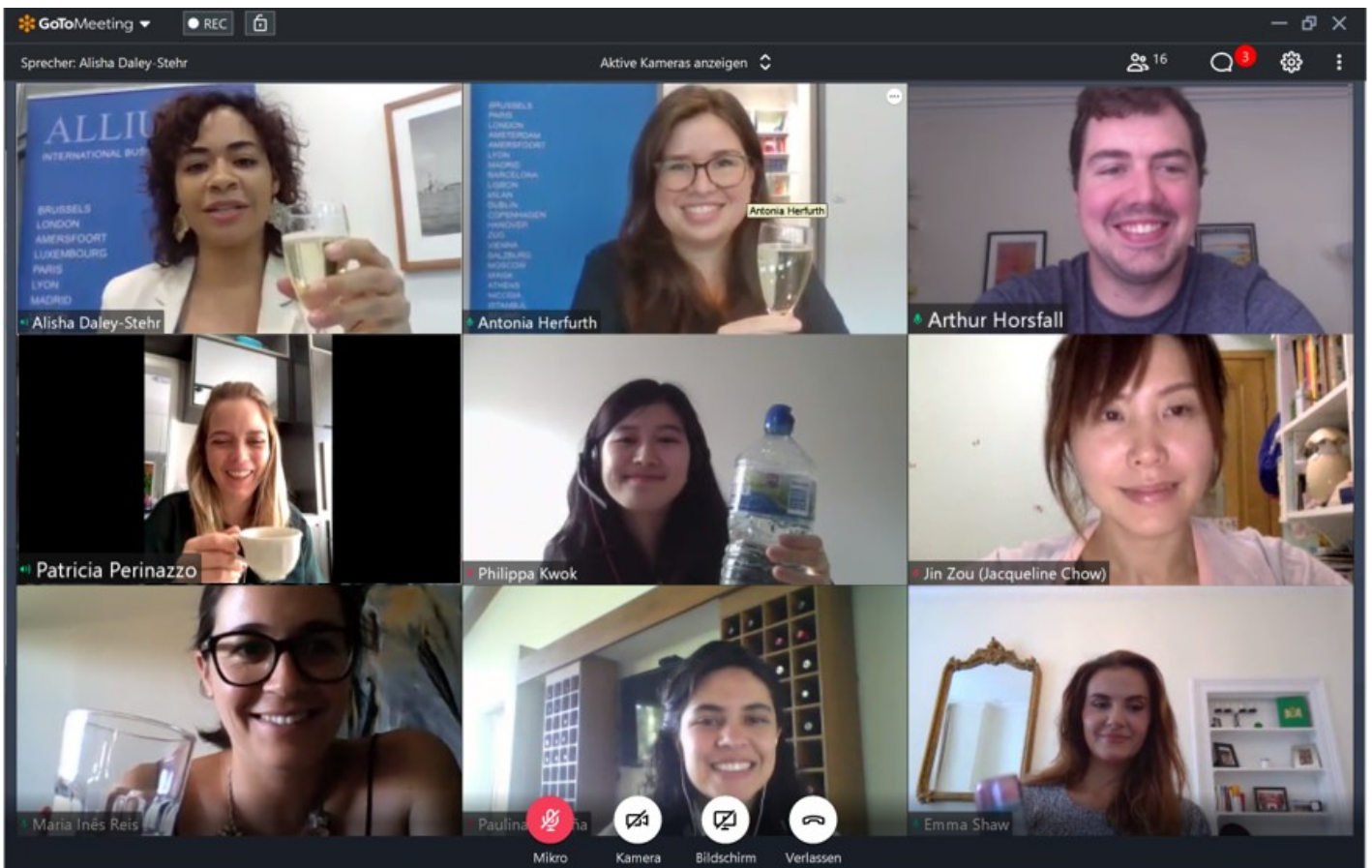


Day 5 "AI": Open discussion about AI and ethics.





Prosecco Date on Friday afternoon



Report

Contents

	<i>page</i>
I. Chapter One – Corona Epidemic as Force Majeure	5
1. Presentations	6
1.1. Commercial contracts from a sporting perspective in relation to force majeure and frustration (<i>Zane Shihab Kerman & Co</i>)	7
1.2. A guide to English court process and how disputes are resolved (<i>Robert Paydon Kerman & Co</i>)	12
2. Q&A	20
2.1. How is business and are supply chains affected by the epidemic?	21
2.2. Which type of force majeure could apply?	24
2.3. Which kind of national or international legal provisions for a post contractual adjustment of obligations exist in your country?	28
2.4. Which kind of rules has your country issued with respect to Corona and contractual obligations?	31
3. Materials	34
3.1. Corona and Force Majeure, Alliuris Compact, March 2020 (<i>Marc-André Delp Herfurth & Partner</i>)	35
II. Chapter Two – Work from Home	41
1. Presentations	42
1.1. Work from Home - Open Discussion (<i>Alexander Steenaert Marree en Dijkhoorn</i>)	42
1.2. Work from Home Agreements (<i>Antonia Herfurth Herfurth & Partner</i>)	45
2. Q&A	56
2.1. Which practical problems exist in the “work from home” mode?	56
2.2. Which laws exist in your country that affect work from home?	57
2.3. Which rules would you provide when drafting a “work from home” agreement with employees?	58

3.	Materials	59
3.1.	Draft of a Home Office Agreement compiled by the participants	59
3.1.	Work from Home, Alliuris Compact, April 2020 (<i>Antonia Herfurth Herfurth & Partner</i>)	63
III.	Chapter Three – Data Protection Update International	69
1.	Presentations	70
1.1.	India 2020: Data protection, privacy & digitalization compliance for businesses (<i>Dr Manoj Kumar Hammurabi & Solomon</i>)	70
1.2.	International data transfers under the GDPR (<i>Constantin Herfurth Eversheds Sutherland</i>)	88
1.3.	The Indian compliance regime on the data processing issues that confront videoconference service providers (<i>Dr Manoj Kumar Hammurabi & Solomon</i>)	97
	EU Standard Contractual Clauses, Controller to Controller (2001-497-EC)	98
	EU Standard Contractual Clauses, Controller to Controller (2004-915-EC)	100
	EU Standard Contractual Clauses, Controller to Processor (2010-87-EU)	109
	Privacy verdict by top court: Implications for business, October 2017 (<i>Dr Manoj Kumar & Pathik Arora Hammurabi & Solomon</i>)	112
	Boards must plan to meet EU data protection norms, January 2018 (<i>Dr Manoj Kumar & Shweta Bharti Hammurabi & Solomon</i>)	123
	India Japan's Digital Partnership, Legal Era, September 2019 (<i>Dr Manoj Kumar & Smriti Sharma Hammurabi & Solomon</i>)	128
	Privacy law and its commercial implications, December 2019 (<i>Dr Manoj Kumar Hammurabi & Solomon</i>)	132
1.4.	Videoconferences compliant with data protection (<i>Antonia Herfurth Herfurth & Partner</i>)	133
2.	Q&A	140
2.1.	Which kind of technical / practical problems about data protection exist in your country?	140
2.2.	Which modules shall be used for the establishment of a data protection management system?	143
2.3.	Which advice would you give to your client for cross border relations?	145

3.	Materials	149
3.1.	Data Protection in Foreign Business, Alliuris Compact, December 2018 <i>(Marc-André Delp Herfurth & Partner)</i>	149
IV.	Chapter Four – Business Platforms	155
1.	Presentations	156
1.1.	Digital Platforms <i>(Ulrich Herfurth Herfurth & Partner)</i>	156
2.	Q&A	185
2.1.	Which kind of online platforms do you know in your country?	185
2.2.	Which kind of regulation exists?	187
2.3.	What are the main legal problems with online platforms?	191
3.	Materials	195
3.1.	Providers, Platforms and Networks, Alliuris Compact, January 2016 <i>(Martin Heitmüller Herfurth & Partner)</i>	195
V.	Chapter Five – Artificial Intelligence	201
1.	Presentations	202
1.1.	Artificial Intelligence <i>(Ulrich Herfurth Herfurth & Partner)</i>	202
2.	Q&A	242
2.1.	Are there national rules about AI?	242
2.2.	Can AI conclude binding contracts?	245
2.3.	Who is liable for decisions and acts by AI?	248
2.4.	Are creations made by AI protectable by IP?	251
2.5.	Which kind of ethic rules should apply for the use of AI?	253
2.6.	How will AI influence expert work and legal work?	254
3.	Materials	260
3.1.	Artificial Intelligence and Law, HP Compact, January 2019 <i>(Ulrich Herfurth Herfurth & Partner)</i>	260

Chapter One

Corona Epidemic as Force Majeure

KERMAN & C^o


Corona Epidemic as Force Majeure

20 July 2020



1

Introduction



Zane Shihab | Partner and Head of Sport, IP & Media | +44 (0)20 7539 7312 | zane.shihab@kermanco.com

Zane provides practical commercial advice to global brands, international sporting bodies and events and high-profile individuals. He specialises in intellectual property and the drafting and negotiation of commercial contracts including sponsorship, joint venture, merchandising, broadcasting, new media, agency, distribution, franchise and image rights agreements, venue agreements, IP and software licenses. Zane is recognised by the Legal 500 2020 as a recommended sports lawyer.

Zane has negotiated numerous lucrative sponsorship and supplier agreements and other event related contracts on behalf of sporting events and governing bodies including the PGA European Tour, Ryder Cup, World Marathon Majors, London Marathon, RideLondon and the All England Lawn Tennis Club (Wimbledon). He is also an in-house Legal Counsel at Wimbledon advising all departments across the organisation (on a secondment basis). He has drafted and advised on the agreements connected to high profile Premier League football transfer and renegotiations, and has successfully represented well-known players in disciplinary proceedings brought by the Football Association of England.



2

Kerman & Co

- Independent mid-tier law firm in London (UK).
- Ranked by the Legal 500 UK as one of the leading law firms in the UK across a number of our specialist practice areas.
- Full service law firm: Corporate/M&A, Capital Markets, Commercial/IP, Litigation, Employment/Immigration and Real Estate.
- Some of our clients include:



KERMAN & CO

© 2020 Kerman & Co. All rights reserved.

3

COVID-19: Worldwide Impact on Events

- The Sport and Entertainment sectors hit hard as governments seek to curb COVID-19 outbreak.
- Number of Worldwide COVID cases has now surpassed 13.6 million.
- Sporting Events
 - 2020 Tokyo Olympics (postponed until 2021)
 - 2020 Wimbledon Championships (cancelled)
 - Formula 1 (behind closed doors)
 - Euro 2020 (postponed until 2021)
 - English Premier League (behind closed doors)
 - 6 Nations (final matches postponed)
 - The Open Championship (cancelled)
- Music Events (all cancelled)
 - Glastonbury
 - Coachella
 - Park Life Festival
 - Reading & Leeds
 - Isle of Wight
 - Download Festival
 - Creamfields



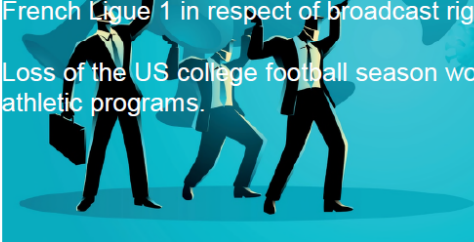
KERMAN & CO

© 2020 Kerman & Co. All rights reserved.

4

COVID-19: Impact on Events by numbers

- 500,000 were expected to attend 2020 Wimbledon Championships.
- Approximately 3,374,186 tickets to remaining Premier League games unused.
- An estimated £15bn lost in by sports clubs in sponsorship revenue globally.
- Approximately 700,000 attending Top 10 UK Music Festivals (all cancelled).
- TV money: BeIN Sports reported to have suspended payment of €42m to French Ligue 1 in respect of broadcast rights.
- Loss of the US college football season would result in \$4bn loss for college athletic programs.




KERMAN & C^o

© 2020 Kerman & Co. All rights reserved.

5

Stadium revenue

Leagues- Stadium and Arenas Revenues- US\$ million



League	Revenue (US\$ million)
MLB-US	2,256
NFL-US	1,400
NHL-US	1,089
NBA-US	1,011
Premier League-UK	718
La Liga-Spain	544
Bundesliga-Germany	504
MLS-US	296
Série A -Italy	217
Série A-Brazil	200
Ligue 1- France	182
Netherlands- 1st.Division	111
Turkey- 1st Division	88
Scotland- 1st Division	79
Portugal- 1st Division	51

KERMAN & C^o

© 2020 Kerman & Co. All rights reserved.

6

What is force majeure?

- "Superior force".
- Happening of events outside the control of the contractual parties (e.g. natural disasters, epidemics, outbreak of hostilities).
- No doctrine of force majeure in English law. Question of interpretation of contract.
- Force majeure clauses are contractual terms which anticipate and provide for the consequences for the parties of the arising of a supervening event.
- Example of clause:
 - Standard definition of what constitutes force majeure event.
 - Clause excuses one or both parties from performance of contract on occurrence of specified events.
 - Party exercising the force majeure clause will not be liable for its failure to perform contractual obligations.
 - Generally, a force majeure clause will require the defaulting party to use reasonable endeavours to prevent/ mitigate the effects of the force majeure.
 - Depending on the drafting, there may be a variety of consequences:
 - Not having to perform the contract in whole or part.
 - Excusing delay in performance.
 - Right of termination.

FORCE MAJEURE
In a contract, force majeure shall be defined as an event beyond the control of the parties which shall be automatically extended for a period of time.

KERMAN & CO

© 2020 Kerman & Co. All rights reserved.

7

Force majeure drafting

- Acts, events or circumstances beyond the reasonable control of the party concerned.
- Usually lists the 'events' which will be included as force majeure.
- Be careful to include all eventualities – 'expressio unius est exclusion alterius'.
- Commercial decision which 'events' to include – industrial action, supplier default.
- Can include 'sweep-up' language if list of 'events' not exhaustive.
- Tandin Aviation Holdings Ltd and Aero Toy Store LLC [2010]:
 - Case concerned the purchase of aircraft and whether the economic crash triggered the force majeure clause.
 - Held by Court that the sweep-up' phrase "any other cause beyond Seller's reasonable control" had to be read in context of entire clause (i.e: the specific examples listed) which made no remote reference to economic downturn.

KERMAN & CO

© 2020 Kerman & Co. All rights reserved.

8

Is the COVID-19 pandemic a Force Majeure event?

- It depends on the drafting.
- No reported case law in England & Wales on the operation of Force Majeure clauses in the context of a global pandemic.
- The burden of proof is on the party seeking to rely on the force majeure clause to prove that the event had triggered the clause (*Channel Island Ferries* [1988] 1 Lloyd's Rep 323).
- This is a high threshold – considerably higher than 'more difficult'.
- Government restrictions may have made it impossible to perform contract, but evidence would be required to show this.
- It has been held that a force majeure event must be the only effective cause of default by a party under contract – it must be solely due to the event that you cannot perform your obligations.

KERMAN & C^o

© 2020 Kerman & Co. All rights reserved.

9

Doctrine of Frustration

- Where parties have agreed force majeure clause, generally be no room separately to invoke the doctrine of frustration. The parties have already anticipated and provided for contractual consequences of the supervening event in the contract. But what if your contract does not contain a Force Majeure clause?
- General Rule: if performance of a contract becomes more difficult or even impossible, the party who fails to perform is liable in damages
- The common law Doctrine of Frustration is the exception to this general rule. It allows the contract to be discharged automatically when the 'frustrating event' occurs so the parties no longer bound to perform their obligations.
- Frustration will only apply in certain restricted circumstances where performance of the contract has become impossible, illegal or radically different on account of something arising after the formation of the contract.
- Frustration is a relatively narrow doctrine: the Courts are wary to allow parties to use it to "escape a bad bargain" (*Edwinton Commercial Corp v Tsavliris Russ (Worldwide Salvage & Towage) Ltd (The Sea Angel)* [2007] EWCA Civ 547 at [111]).
- As frustration "kills the contract" automatically and forthwith, it is not to be lightly invoked and is confined to "very narrow limits" (*Bingham LJ in The Super Servant Two* [1990] 1 Lloyd's Rep 1).

KERMAN & C^o

© 2020 Kerman & Co. All rights reserved.

10

Doctrine of Frustration

Test for Frustration

- The 'frustrating event' occurs after the contract has been formed;
- It is so fundamental that it is considered to be 'striking at the root' of the contract and is entirely beyond contemplation of the parties at the time of entering the contract;
- It is not due to the fault of either party; and
- The 'frustrating event' has rendered performance of the contract impossible, illegal or fundamentally different from what was envisaged at the time of contract.

KERMAN & C^o

© 2020 Kerman & Co. All rights reserved.

11

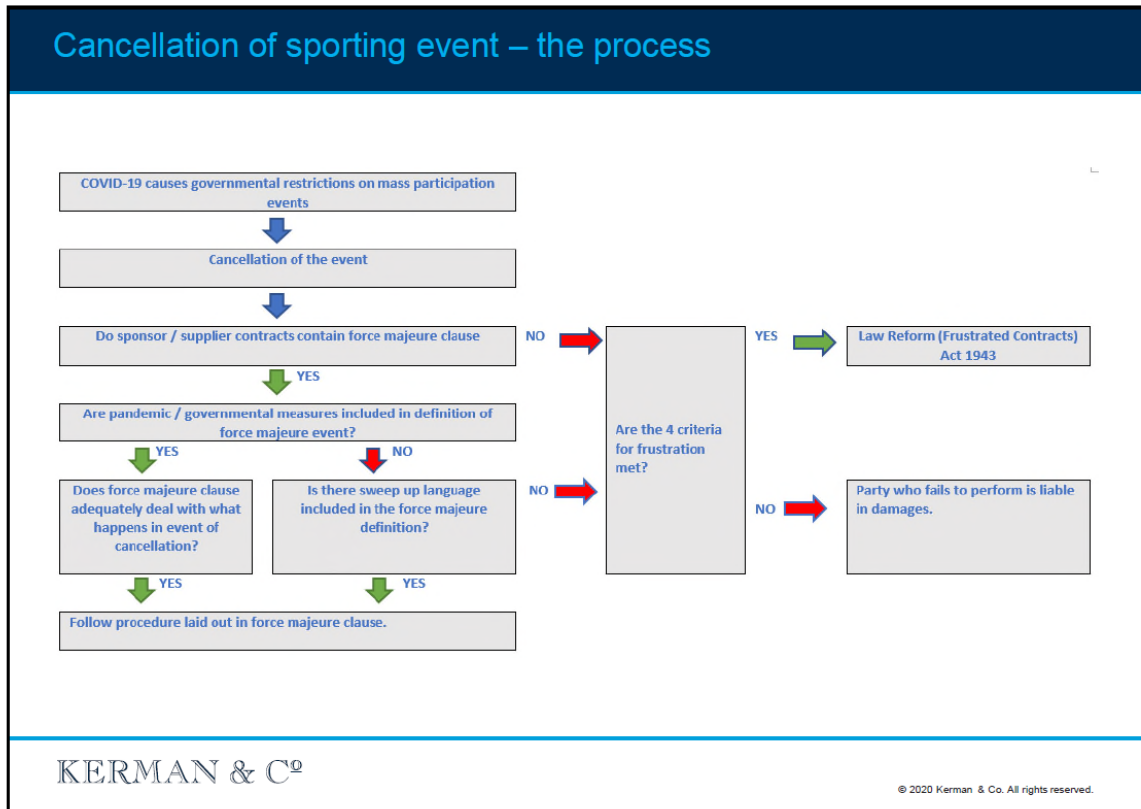
Doctrine of Frustration

- If you do manage to prove Frustration, the Law Reform (Frustrated Contracts) Act 1943 ("**LRA**") will determine the ability of a party to recover money paid under contract before the occurrence of the frustrating event.
- This statute applies to most commercial contracts governed by English law.
- The LRA provides:
 - Money paid before the frustrating event can be recovered and that money due before the frustrating event is no longer payable
 - A party who has incurred expenses is permitted to retain an amount up to the value of the expenses out of any money paid by the other party (if the court sees fit)
 - The court may require a party who has gained a valuable benefit to pay a 'just sum' for it.
- Optimal in terms of loss allocation between the parties when performance is prevented.

KERMAN & C^o

© 2020 Kerman & Co. All rights reserved.

12



13



14

Introduction and outline

- Introduction
- Outline
 - The English Litigation Process
 - The Brexit Frustration Case

KERMAN & C^o

© 2020 Kerman & Co. All rights reserved.

15



KERMAN & C^o

© 2020 Kerman & Co. All rights reserved.

16

The English Litigation Process (1)

- Jurisdiction
 - England & The United Kingdom
- The Common Law
- The Adversarial System
- Solicitors & Barristers

KERMAN & C^o

© 2020 Kerman & Co. All rights reserved.

17

The English Litigation Process (2)

- The English Courts
- The Civil Procedure Rules (CPR)
- Active Case Management
- ADR

KERMAN & C^o

© 2020 Kerman & Co. All rights reserved.

18

The English Litigation Process (3)

- Pre-Action Conduct – the ‘Pre-Action Protocols’
- Letter before Action and the Response
- Pleadings/ Statement of Case
 - Limitation
- Disclosure
 - Scope
 - What is a ‘Document’
 - The Duty to Search
 - Reform: The Disclosure Pilot Scheme

KERMAN & C^o

© 2020 Kerman & Co. All rights reserved.

19

The English Litigation Process (4)

- Witness Statements
 - The Statement of Truth
- Expert Witnesses
 - Reports
 - Independence
- Trial
- Injunctions

KERMAN & C^o

© 2020 Kerman & Co. All rights reserved.

20

The English Litigation Process (5)

- Costs
 - Costs 'follow the event'
 - Assessment
- Appeals
 - Court of Appeal
 - Permission to Appeal
 - The Supreme Court

KERMAN & C^o

© 2020 Kerman & Co. All rights reserved.

21

Brexit and Frustration



KERMAN & C^o

© 2020 Kerman & Co. All rights reserved.

22

Brexit and Frustration (1)

- Canary Wharf Group and the European Medicines Agency (Canary Wharf (BP4) T1 Limited and ors v. European Medicines Agency [2019] EWHC 335 (Ch))
- Was Brexit a frustrating event under a 25-year English law-governed lease between the EMA and its Canary Wharf landlords in respect of the premises of the EMA's London headquarters?
- Adoption of the 'multi-factorial approach', involving consideration of:
 - The terms of the contract and context
 - The parties' knowledge, expectations, assumptions and contemplations
 - The nature of the supervening event, and the parties' reasonable and objectively ascertainable calculations as to the possibilities of future performance in the new circumstances.

KERMAN & C^o

© 2020 Kerman & Co. All rights reserved.

23

Brexit and Frustration (2)

- Frustration by:
 - Supervening Illegality
 - Frustration of a Common Purpose
- The Decision
 - Brexit was not relevantly foreseeable in 2011
 - BUT the lease was not frustrated because the parties had expressly catered for the possibility that there might be some event requiring the EMA's involuntary departure from the premises owing to circumstances beyond the EMA's control.
- The EMA's Appeal

KERMAN & C^o

© 2020 Kerman & Co. All rights reserved.

24

Questions ?

KERMAN & C^o

© 2020 Kerman & Co. All rights reserved.

25

Thank you

KERMAN & C^o

© 2020 Kerman & Co. All rights reserved.

26



KERMAN & C^o
200 Strand, London WC2R 1DJ
Tel +44 (0)20 7539 7272
www.kermanco.com

Questions & Answers

Corona Epidemic as Force Majeure

1. How is business and are supply chains affected by the epidemic?

Maria Inês Reis (Portugal):

I think that mostly restaurants/bars/hotels are the main business that are affected because most of online shopping is still running busy.

Iv Fangyuan (China):

Business is greatly affected by the epidemic. Manufacture industries whose products are mostly shipped to foreign countries or whose materials are relying on importing have fallen a cliff in the past four months.

Qiu Shuang (China):

On the one hand, export orders are on the decline, almost all of the world's epidemic has occurred, and the international market demand has shrunk significantly; on the other hand, the global supply chain is blocked, there are difficulties in importing raw materials, and the supply capacity of relevant countries has decreased significantly.

Qiyi Zhang (China):

Business and supply chains have been greatly affected by Corona epidemic. Many businesses, especially the offline service industry, went bankrupt one after another due to the severe decline in business turnover and unbearable operating costs during the epidemic. Because of the epidemic, many companies were unable to resume work and production, leading to supply chain disruptions. The global economic downturn in 2020.

Eduardo Barrera (Mexico):

They were and are affected when we analyze not only the new requirements in specific countries for the transport of goods (for example: sanitation seals are not fully functional because of small working areas etc.) but also because of a regrowth of an epidemic spot that causes delays by a terminate product like at the beginning with

China in January 2020 which caused, among other things, the delay of using a mask as an obligation around the world until months later when their world supply opened again.

Friederike Ammann (Germany):

Reduced demand / reduced production, delivery problems (due to dependency on other countries), low accuracy of planning, due to unpredictable pandemic development, social distance (for businesses which require social interaction)

Arthur Horsfall (UK):

As the epicentre of the Corona virus epidemic moved from China to Europe and then to North and South America different parts of the supply chain have been affected at different times during this Corona virus epidemic.

The manufacturing power of China meant that the initial impact was that the supply of materials or stock may have originally been affected. However, as China's lockdown restrictions began to ease, other parts of the supply chain, such as distribution may have then been affected due to lock down measures being implemented in other countries (including closing borders and quarantine).

As a further result of the lockdowns, footfall and the types of items that customers will prioritise has changed. As a result, many businesses will now be left with large amounts of excess stock.

The Corona virus epidemic has therefore had a long-lasting and wide-ranging impact on supply chains.

Coral Yu (UK):

Almost all industries and businesses suffer from complete or partial disruptions due to the epidemic. Personally, I have come across empty supermarket shelves and shortages of essential home supplies which indicate the negative impact on supply chains to consumer products. There have also been news on the shortage of medical suppliers across the globe. From a work perspective, many clients have been struggling with maintaining their core business activities.

Gary Whitehead (UK):

As supply chains face significant disruption, businesses who have trimmed back their supply chain will find that they do not have the bandwidth to adapt and they may find situations where they are ultimately unable to fulfil orders. Companies will find that they are having to find alternative supply sources and prepare for changes to the labour planning.

Philippa Kwok (UK):

- Public health measures in place, leading to reduction in transportation and manufacturing activities

- Many companies are heavily reliant on certain regions that are particularly affected by the pandemic, for parts and materials.
- Drop in economic activity
- Drop in volume of business
- Impact on labour, movement of goods and provision of services

Julia Krautter and Patrícia Perinazzo (Brazil):

Since the beginning of the year and more strongly since March, our law firm has been following up the strategies of several clients on how to proceed in these challenging months in view of the pandemic that has spread across the globe. In general, the strategies were divided into stages, depending on the financial strength and the profile of each group, among other factors:

- The first stage included directing the entire staff or a substantial part of the staff to work from home, adjusting internal policies and employment contracts accordingly, and renegotiating all other kinds of commercial contracts, whose conditions were impacted by the pandemic.
- Subsequently, some groups required their employees to take their annual leave, both overdue or not yet due, or holiday entitlement as paid time off.
- In a third stage, the suspension of employment contracts and/or the reduction of working hours and wages were options considered. Finally, as a last resort, some groups had to reduce staff and even cease operations locally.

All groups used the first stage. Fortunately, only a few used the two other options.

Alitzel Sánchez Alonso (Mexico):

Unfortunately, here in Mexico and as result of the force majeure most of the business were affected because there was a decrease in their incomes and as result of that, many of such business had the necessity to close, so people got fired or their wages were decreased.

Luis Roberto Moreno Tinoco (Mexico):

The present pandemic has severely affected the Mexican economy, as many of the businesses were paralyzed and forced to close during the quarantine stage. This especially affected companies dedicated to providing entertainment and food services as well as those businesses dedicated to the sale of goods that did not sell their goods over the Internet.

Likewise, the quarantine stage significantly affected the supply chain of goods and services, since the production of basic goods had to be reduced as a consequence of the sanitary measures, which, together with the society's panic purchases, caused that there were shortages in some goods for a short period of time.

It is important to consider that in addition to the above, many people (about 1.1 million people) lost their jobs as a result of the pandemic, which indirectly affected the rest of the economy, as the cash flow was reduced nationally.

Mari Yoli Wulf Sánchez (Mexico):

Travel restrictions and quarantine disrupted supply chains, consumption of products has fallen and therefore countries' economic growth has stopped.

Miguel Ángel Aspe de la Rosa (Mexico):

Business and supply chains have been deeply affected by the epidemic. Certain regulations waivers have been granted to first need commodities such as medical instruments or masks. Despite having these waivers, there is a wide array of goods that have suffered stronger restrictions, such as livestock. In my view, there is still a lack of planning with respect to the adaptation of supply chains.

Addressing the status of businesses, the current situation is mixed. While there are certain industries such as pharmaceuticals or technology businesses (e.g. Zoom) that are thriving due to the epidemic, the majority of other businesses are facing a difficult time that, in many cases, has led to bankruptcy.

Nadieżhda Vázquez Careaga (Mexico):

I consider that a big percentage of the investors in all the world are waiting until the epidemic has finished. Also, I think that the reason is because the need to reconsider if the original plans can continue ones the ordinary course starts again.

Paulina Saldaña Fuentes (Mexico):

Business were affected by two main things:

1. Some were ordered to close, so they stopped generating and
2. others were mandated to operate in a minimum capacity to prevent the virus transmission.

In both cases the income of business was abruptly reduced.

Ricardo Heredia (Mexico):

Everything is related, if suppliers are not able to produce because the government imposed a lockdown, business will not be able to receive such products and later the people. An example could be the supermarket groceries or Lysol products which at the beginning of the pandemic started running low. People should have considered in their agreements special covenants where they are not liable for not meeting certain deadlines or payment obligations due to suppliers or a force majeure.

Fergan Tuğberk İşman (Turkey):

Due to the fast spreading rate of the virus, many countries shut their ports and borders down. Even some countries like Turkey closed some of their metropolitan provinces'

borders. This precautionary measure affected many transportation chains. Most of the maritime and road transportation companies slowed or even halted their operations. With this measure, common food products have spoiled in the farms where they had produced or during the disrupted transportation chain. Even if the demand for those products is increasing, the supply could not meet this demand as efficiently because of the measures and the natural flow of life.

The one who benefits from this measure was supermarkets that sell groceries, undoubtedly. With their high supply chain, they were successful to meet the high demand rate. That achievement was under favour of another important measure which is the closing of social places such as cafes, shopping malls and restaurants.

Measure against social places has not only affected those businesses but also the lessor of the workplaces which is subject to a rental agreement. Some businesses decided to evacuate the places where they were actively working and some of them had to make new deals with their lessors.

2. Which type of force majeure could apply?

Iv Fangyuan (China):

Natural force majeure compared with political force majeure

Qiyi Zhang (China):

On February 10, the Legislative Affairs Committee of the Standing Committee of the National People's Congress declared that Corona epidemic is a force majeure that cannot be foreseen, avoided or overcome. Force majeure events are generally catastrophic events affecting the performance of contracts, including natural forces, such as earthquakes, floods, droughts, blizzards etc., and social anomalies, such as wars and riots. Corona epidemic is a new infectious disease that is sudden, unpredictable and has not yet developed a cure for the epidemic. Of course, if force majeure is to be applied, then the breach must be related to the novel Coronavirus.

Eduardo Barrera (Mexico):

At the beginning, it was discussed in Germany if this normal clause could be enough. In other countries, it is considered as a pandemic situation, too, but the difficulty at the beginning was that the authority needed to declare it officially which caused lots of problems. In Mexico, it was known the UN Law and also this clause normally used by construction or by the oil sector. Now, a specific clause just for Covid-19 is recommended because all contracts being made by now assume the risk we are living already in.

Friederike Ammann (Germany):

None of the standard force majeure types is applicable (war, natural catastrophes etc.).

Arthur Horsfall (UK):

Under the laws of England and Wales force majeure is a concept of contract law, rather than a standalone concept. The type available will therefore entirely depend on the wording of the clause in the contract. It is therefore essential for those wishing to invoke a force majeure clause to assess carefully whether all the requirements are met.

For anyone wishing to rely on a force majeure event it is also crucial, to follow the notification provisions of the contract, including requirements for written notice and specified time periods.

Coral Yu (UK):

English law has no general rule of force majeure. Whether the COVID-19 outbreak is a force majeure event will depend on the drafting and interpretation of each contract. Under many definitions of force majeure, the current pandemic may well trigger the clause.

Gary Whitehead (UK):

Extraordinary event/ pandemic or epidemic (if included in drafting as specific event) or potentially the doctrine of frustration

Philippa Kwok (UK):

- Act of God
- Specific events / references in the force majeure clause to:
 - Epidemics
 - Pandemics
 - Plague
 - Outbreak
 - Crisis
 - Any action taken by government / public authority

Julia Krautter and Patrícia Perinazzo (Brazil):

In Brazil we have an article in the civil code (993) that set forth that: “Art. 393. The debtor is not liable for damages resulting from unforeseeable circumstances or force majeure, unless expressly held responsible for them. Single paragraph. The act of God or force majeure occurs in the necessary fact, the effects of which were not possible to avoid or prevent.”

- The companies have stronger arguments to request and be able to renegotiate their contracts the more of the following items applies:
 - a) they have a long-term contract with their business partners party, with successive and continuous installments;

- b) up to the time of the pandemic they had not faltered any of their obligations;
 - c) they are, in fact, facing an unforeseen and unexpected situation (those that, for example, entered into a contract in early 2020 have less of a case as the threat posed by the coronavirus was already known or likely to be known worldwide);
 - d) they are indeed and evidently facing significant negative impact on their business;
 - e) in respect of their business partner, some of the benefits have become excessively expensive with the changes in the post-pandemic scenario;
 - f) they have taken or are taking all reasonable measures to mitigate their damages (e.g. it is unreasonable to seek renegotiation if they have not yet eliminated unnecessary expenses); and
 - g) the contract to be renegotiated contains clauses providing that events of force majeure and excessive burden are grounds for release of obligations or renegotiation.
- Looking ahead though, among the many lessons that the pandemic has taught us, is the necessity of a more detailed set of clauses about what is force majeure and what are the consequences in this case. It is worthwhile for the parties to invest a few hours drafting and negotiating a substantial clause to avoid long discussions later. Fortuitous event and force majeure clauses, which by default are short and include broad terms such as “acts of nature” or “acts of God” should be better detailed by expressly mentioning, for example, that “pandemic”, “diseases”, “plague”, “epidemic” are or may be events of force majeure and what exactly will happen, should any occur. In addition, the importance of defining dispute resolution procedures has increased and which law will be applicable and the jurisdiction chosen by the parties because the interpretation of what is force majeure varies between cities, states and countries.

Alitzel Sánchez Alonso (Mexico):

Nature, human acts or authority acts that may breach the obligation of one of the parties.

Luis Roberto Moreno Tinoco (Mexico):

Mexican law provides for two different concepts to regulate the cases in which an obligation cannot be complied with due to unexpected events: fortuitous case and force majeure.

According to both Mexican courts and the respected authors, a fortuitous case involves an event of nature that is unpredictable, while force majeure implies a man-made event that is inevitable.

Now, although the new virus could be deemed as a fortuitous case since it is an event of nature that was unpredictable, I consider that its sole existence cannot be deemed as sufficient to justify the failure or delay in the compliance of contractual obligations. Furthermore, I consider that it should be analysed if other circumstances (such as any administrative rule or health measure) affected the economic or technical capacities of the parties involved in the transaction, in which case these circumstances could be argued under the terms of a force majeure.

Mari Yoli Wulf Sánchez (Mexico):

The pandemic is the reason for many people's inability to fulfil their obligations (e.g. to go to work). However, I believe that it could have been prevented through research and be better prepared for this situation.

Miguel Ángel Aspe de la Rosa (Mexico):

In the Mexican legal system there is not a clear-cut division or types of force majeure.

Nadiezhdá Vázquez Careaga (Mexico):

It depends in every case. In my opinion, in Mexico the most relevant sector that is having the actualization of a force majeure is in real estate, with all the lease agreements.

Paulina Saldaña Fuentes (Mexico):

There is a force majeure in Mexican law that refers to the inability of the "thing" to be used, for instance, you cannot use a store in a shopping mall.

Ricardo Heredia (Mexico):

There is not a specific force majeure, it is applied in a general concept. It mainly applies to lease agreements, when the lessee is not able to use the property such as a restaurant. Therefore, Civil Code establishes, the possibility for the lessee for not paying rent and even early terminate the agreement after two months.

Fergan Tuğberk İşman (Turkey):

Force Majeure is a situation that frees the parties from legal obligations under certain circumstances. This situation must be external, inevitable and unpredictable in Turkish law. Covid-19 is a fast spreading virus and it has been declared as an epidemic by WHO. From the perspective of binding contracts, this epidemic is an external, inevitable and unpredictable obstacle.

However, as a consequence of the precautionary measures, some legal agreements have also become impossible to fulfil such as allowing the usage of a workplace through rental agreement, for example restaurants which have been shut down because of the precautions. This legal impossibility may also be counted as a force majeure.

3. Which kind of national or international legal provisions for a post contractual adjustment of obligations exist in your country?

Maria Inês Reis (Portugal):

Most companies applied to “layoff” condition for most of the employees.

Iv Fangyuan (China):

Under PRC General Provisions of the Civil Law (promulgated in March 2017), force majeure is generally recognized as an excuse for not performing civil obligations. If a contract does not include a force majeure provision, it will be implied. If a contract includes a force majeure provision, a party can rely on the force majeure provision or resort to the protection offered by the general law if the scope of the contractual remedy is considered to be limited.

Qiyi Zhang (China):

Contract Law of the People's Republic of China

Eduardo Barrera (Mexico):

As far as I know one of the first modifications was the possibility to postpone the payment of the rent of an apartment for two months in specific states. More developed adjustments occurred with some big companies as I said, to immediately suspend the activities giving a report to the government and the other part (in Oil branches) explaining their reasons, in which the authority had short time to give a reply.

Arthur Horsfall (UK):

Although 'force majeure' is not a recognised legal concept under the laws of England and Wales, the doctrine of frustration is. Frustration can occur where a significant change of circumstances renders performance of a contract radically different from the obligations that were originally undertaken. The change must result from an outside event or change of situation occurring independently from the party seeking to rely on it.

Where frustration applies, the parties are excused from all further performance and are not liable for damages for non-performance.

Relying on frustration is only possible in circumstances where the contract does not already include an express force majeure provision catering to the particular situations. It should also be noted that the threshold for provision frustration is very high and the courts are generally reluctant to hold that a contract has been frustrated. It is normally argued as a last resort.

Coral Yu (UK):

I don't think there are any specific statutes or rules issued in terms of contract law in UK.

Philippa Kwok (UK):

- Break clauses
- Price adjustment clauses
- Variation clauses
- Limitation / Exclusion of liability clauses
- Dispute resolution / Alternative dispute resolution clauses
- Material adverse change clauses

Julia Krautter and Patrícia Perinazzo (Brazil):

It is made it by an amendment duly signed by both parties.

Notwithstanding whatever the angle, we understand that settling the matter out of court between the parties is, in most cases, the best option.

In a renegotiation, the possibilities for a new agreement are many, such as: grace period, postponement and payment in installments, remission of part of the debt overdue or not yet due, reduction of amounts forward with or without subsequent offsetting, request for guarantees and extended contractual term. It is better that the parties themselves, who are well aware of the relationship and the facts, decide what to do and, accordingly, will already know in advance what obligations they will assume.

By taking formal legal action, in addition to a slow and costly process, it will be up to a third-party, who is unfamiliar with the parties or the situation in hand, to decide what the parties must do. A judgment may be better than an out-of-court settlement, it is true. However, it might as well be much worse. It is also true that, unfortunately, some claims are settled only when one party decides to sue the other. This is the last of the alternatives, but please note that it is a good alternative for a party that is entitled and finds the other contractual party unwilling to settle the claim.

Alitzel Sánchez Alonso (Mexico):

According to the applicable law, if during the term of the agreement, an extraordinary act happens that cannot be predicted and, as result of such force majeure the obligations became more onerous for one of the parties, such party may choose "acción pro-forma" which allows the parties having a balance on the obligations they have in terms of the agreement and according to the procedure set forth in the applicable law.

Likewise, the applicable law for leasing, allows the lessee not to pay rent for the term the force majeure lasts (most of the above is applicable for places that are leased for business).

Luis Roberto Moreno Tinoco (Mexico):

In Mexico, as a general rule, the parties must comply with the obligations acquired in the contracts they have entered into, in accordance with the terms and conditions expressly established therein. That is, in Mexico the general principle of law "*pacta sunt servanda*" (what has been agreed must be complied with) applies, except for some exceptional circumstances that may exempt the parties from complying with such obligations (such as fortuitous event or force majeure).

Parties to a contract may agree on the consequences arising from fortuitous cases and force majeure; they are even free to indicate what kind of events may be considered as such, which allows for the possibility of diminishing, to some extent, the adverse effects of such events.

If these circumstances are not expressly agreed upon by the parties, the party that was affected by any of these events can be released of the compliance of some of the obligations (as long as it can be proven), and a post contractual adjustment can be entered into among the parties.

International treaties may include special rules regarding these matters, including the specific assumptions that can be deemed as fortuitous case and force majeure.

Mari Yoli Wulf Sánchez (Mexico):

Whether or not a contracting party can invoke contractual exemption in case of an epidemic depends mainly on whether a corresponding contractual provision has been agreed upon precisely for these cases. In Mexico, the authorities have declared the epidemic in such a way that the pandemic cannot be used as a justification for terminating a contract, which has caused problems.

Miguel Ángel Aspe de la Rosa (Mexico):

The Mexican civil code provides post contractual adjustments of obligations for only domestic transactions. Nonetheless, whether an international transaction is concluded, the set of rules is different and the Mexican legislation is silent on whether these post contractual adjustments could be concluded. The latter is especially relevant for Investor-State agreements, in which the Articles of State Responsibility drafted by the International Law Commission are applicable in case that a dispute arises between the parties.

Nadieżhda Vázquez Careaga (Mexico):

In Mexico the civil law establishes the specific situation for the epidemics and the substantial changes in situations.

Paulina Saldaña Fuentes (Mexico):

In Mexican law there is a post contractual negotiation tool that can be used when the obligation of one of the parties becomes unproportionable to such, in order to renegotiate the terms and conditions to equate such obligations.

Ricardo Heredia (Mexico):

It could be international treaties applied to this case. For example, an international treaty mentioning that borders of the country will not be closed, in order to keep the supply entering, such as medicines.

Fergan Tuğberk Işman (Turkey):

The main principle in the Turkish Law of Obligations is “pacta sunt servanda”. On the ground of this principle, if a contract has been made, the sides have the burden to fulfil the obligation. However, if a situation makes the fulfilment of the obligation intolerable to any of the sides, they may be relieved from the burden due to this situation. This unbearableness must be detected objectively.

The Turkish Code of Obligations article 138 gives two rights to the side who suffers from the unbearable condition. These rights are; rescission from the contract or requesting an adaptation from the judge equal to the unbearableness.

4. Which kind of rules has your country issued with respect to Corona and contractual obligations?

Maria Inês Reis (Portugal):

We have been confined since March but restrictions have been lifted up since end of May, so in Portugal people can go moving around with being strictly at home, with all the hygiene conditions.

Iv Fangyuan (China):

Administrative laws, labor rules

Qiu Shuang (China):

China has formulated the following rules: If the epidemic situation or epidemic prevention and control measures only lead to difficulties in the performance of the contract, the parties may re negotiate; if the performance can be continued, the people's court shall earnestly strengthen the mediation work and actively guide the parties to continue to perform ; the employer cannot terminate the labor contract only because the laborer is infected or takes preventive and control measures.

Eduardo Barrera (Mexico):

Specifically, none of a national importance. Most of them were made up for Labor Law and through a revision of each Contract including a Corona Clause.

Friederike Ammann (Germany):

Reduction of VAT, Insolvency (Aussetzung Insolvenzantragspflicht)

Jannis Ulrich (Germany):

In German law there is a rule that the owner of an estate can cancel the contract of a renter, when the renter doesn't pay two rents in a row. This law is temporally exposed. To support business there is Art. 240 § 1 EGBGB therefore the companies can refuse their service if the service -because of corona- not possible.

Arthur Horsfall (UK):

Since the start of the Epidemic, the government has passed the Corporate Insolvency and Governance Act 2020, which includes the following sections:

- *Creditor Moratorium*
This provides for a 20-business day moratorium to give most types of company experiencing financial difficulties protection from creditors while financial rescue plans are put in place. During that time, no creditor action can be taken against the company.
- *Termination Clauses*
The Act also includes a change to termination clauses in supply contracts. Suppliers will no longer be able to rely on contractual terms to cease to supply or vary the contract terms of supply to companies who have entered into an insolvency or restructuring procedure or obtained a moratorium against creditors.

Coral Yu (UK):

I do not think there are any specific statutes or rules issued in terms of contract law in UK.

Gary Whitehead (UK):

To my knowledge, the UK has not included and 'generic' provisions with Coronavirus Act 2020 except for specific circumstances.

Philippa Kwok (UK):

- Protection of commercial tenants from forfeiture for non-payment of rent
- Non-legally-binding guidance issued by the UK government – encouraging contracting parties to act responsibly and fairly in the national interest in performing and enforcing their contracts

Julia Krautter and Patrícia Perinazzo (Brazil):

None regarding business contracts directly.

The occurrence of the pandemic, however, in itself, is neither a reason nor an excuse for non-compliance with obligations. Nor are the risks inherent in or related to the contract itself, exchange rate changes, inflation, economic crises, an increase in the government

debt and the increase in rates. This is the prevailing understanding of Brazilian court precedents, which was even ratified in Bill No. 1179/20, which provided for the emergency and transitory legal regime of legal relations governed by private law in the period of the pandemic precisely to avoid excessive litigation. It was, however, ultimately vetoed in the final wording of Law No. 14010/20.

Alitzel Sánchez Alonso (Mexico):

The applicable law mentioned above was used during this force majeure, especially for leases and notices that were prepared for loans restructures.

Luis Roberto Moreno Tinoco (Mexico):

Mexican authorities issued several rules that forbid the opening of public spaces (such as restaurants, bars, malls, and, in general, places of social gathering) during the worst stages of the pandemic. Likewise, several rules were issued regarding the development of trials during the quarantine stage.

However, no special rule has been issued whatsoever with respect to the compliance of contractual obligations during this period of time. Thus, the general regime shall be applied should any difference arise.

Mari Yoli Wulf Sánchez (Mexico):

I understand that in Mexico none, simply asked people to stay home, but not as an obligation. For example, with regard to the labour issue, it was not declared as a health emergency so that employers cannot use the pandemic as a reason to dismiss their workers.

Miguel Ángel Aspe de la Rosa (Mexico):

The Mexican government has passed certain waivers in order to comply with contractual obligations related to trade matters. Despite having these measures passed, there are still many industries and sectors that are not covered by these waivers and, thus, the failure to comply with agreements is vast.

Nadieżhda Vázquez Careaga (Mexico):

There are several proposals (real estate, taxes, etc), but nothing official.

Paulina Saldaña Fuentes (Mexico):

The measures adopted by the government were mainly to stop the spreading of the virus, few were issued to support businesses.

Ricardo Heredia (Mexico):

Mainly it has been in connection with lease agreements and operation of businesses. Only a certain group considered as vital and main activities for the country could continue supplying and working, such as telecom services, medical, gas stations, supermarkets and certain financial services, among others. Therefore, if a business

could demonstrate the aforementioned, they could not pay the rent or early terminate the lease agreement after two months.

Fergan Tuğberk İşman (Turkey):

Covid-19 measures halted many business operations. Some of them were social places such as cafes, restaurants and shopping malls. Mandatory closed businesses cannot earn any income during this measure. This precaution did not cease the business' regular outcomes. One of the most important outcomes for many businesses is the renting fee for their business workplace.

With temporary article 2 of Law, numbered 7226, failure to pay the rental fee, processed from 1 March 2020 to 30 June 2020, does not constitute the reason for the termination and evacuation of the rental agreement. With this temporary article, the business owners could keep their workplace even though they could not afford the rent during the precautionary measures.

Labour Law also received some important changes. From 17 April 2020 to 17 July 2020, working agreements cannot be terminated except for the cases like disorderly conducts. Any employer breaching this rule will face administrative fine.

+++

Materials | Compact

Corona and Force Majeure

*Marc-André Delp, Rechtsanwalt, Hanover
Qualified Lawyer for International Commercial Law*

In view of the spread of the Corona virus (Sars-Cov-2) and the associated consequences, many legally relevant questions arise for companies. Short-time work and home office are only two of the issues, albeit particularly urgent ones.

From an economic and contractual point of view, the question of whether the Corona virus automatically removes the contractual obligation to perform for affected companies, whether there is still an obligation to perform, or whether special regulations are required is particularly important. It is precisely in supply chains that the effects of the Corona virus can become noticeable, either through restricted production or through delivery problems.

Fulfilment of contract

In principle, contracts must be fulfilled by the contracting parties. Contracting parties are not per se entitled to terminate contracts unilaterally and may also be subject to claims for damages in the event of non-performance or delays in performance. To counteract and prevent this principle, force majeure clauses should be included in contracts. These clauses stipulate that non-fulfilment due to an unforeseen or uncontrollable event (force majeure) can lead to certain consequences. These consequences must be defined in the contract. The consequences include, e.g., an exclusion of liability for events of force majeure. Furthermore, contracts must be considered in which such clauses are not included.

Force majeure

Many companies use the phrase "the seller is not liable in cases of force majeure". This clause may not be sufficiently precise in all cases.

What constitutes a case of force majeure should be clearly defined in the contract in case of doubt. This prevents subsequent disputes between the parties on the scope of the force majeure. The precise definition helps to create clarity between the parties

about the scope of force majeure. This is because the parties to the contract may naturally have different ideas about the scope. Clear regulations help in this respect. A list of examples of force majeure helps to clarify the situation.

However, this list should not be conclusive, as there may be other, new and unexpected cases which also constitute force majeure, and which should be taken into account. The wording could thus be supplemented to "The seller is not liable in cases of force majeure. This includes in particular, but not conclusively, the following examples: ...". In these formulations, standard terms such as war, business interruptions, natural disasters, traffic disruptions, industrial disputes, disruptions in the operations of carriers and subcontractors and so on will be listed.

Corona as force majeure

Whether the Corona virus has to be regarded as force majeure depends strongly on the wording of force majeure.

With regard to the current developments concerning the Corona virus, the terms epidemic/pandemic and infectious diseases should be listed from a health perspective. Since the Corona virus is an infectious disease and now even a pandemic according to the World Health Organisation (WHO), the Corona virus and its consequences may fall under the aforementioned examples and thus constitute force majeure. The mere formulation *disease* would probably not have been sufficient here, because a disease in itself is not necessarily to be regarded as force majeure.

In view of the current developments, it would also make sense to define certain standards, e.g., when an event should occur. Only when such thresholds are exceeded the event has actually occurred. Thus, with regard to the term "epidemic", reference could be made to a corresponding classification by the WHO, possibly also to warnings of a corresponding health ministry of a certain country.

This shows especially that the regulations concerning force majeure should be made with caution.

It should be examined in each individual case whether a company can rely on force majeure caused by the Corona virus.

Time of the conclusion of the contract

However, despite a corresponding clause, the Corona virus is not always to be regarded as a force majeure. It must be noted that the circumstance of force majeure must have arisen after the conclusion of the contract. If the circumstance was already present at the time the contract was concluded and was therefore known to the parties to the contract, neither party can subsequently invoke force majeure, as this circumstance no

longer constitutes an unforeseen event in this case. If a company therefore concludes a contract in March 2020, it must be assumed that the risk of Corona virus and the associated consequences was known when the contract was concluded and no longer constitutes an unforeseen event. In this case, it would not be possible to invoke force majeure retroactively with the associated exclusion of liability.

Further requirements

If a party wishes to invoke the circumstance of force majeure, further obligations must be complied with, which usually also result from the force majeure regulations. Thus, the other party to the contract must be informed of the occurrence of the case of force majeure. For this purpose, contracts usually contain a provision that the party invoking force majeure must inform the other party without delay about the circumstance and the end of force majeure. This should be documented accordingly.

Furthermore, it is usually contractually agreed that a party must do everything possible to minimise the consequences of the case of force majeure (damage minimisation).

It must then be considered whether there are any further contractual restrictions regarding force majeure, for example that each party must bear the financial consequences of force majeure on its own side. A party may also have reserved the right to dissolve the entire agreement if the force majeure lasts longer than, e.g., 100 days.

And, as a general rule, the party invoking force majeure must prove it in case of doubt and in case of dispute by the other party. This may be less problematic with the current Corona virus, but here too, the circumstances should be documented why a specific service obligation cannot be fulfilled or that the service cannot be fulfilled at this point due to the Corona virus, for example if the business has been closed down or supply chains are interrupted due to the virus. A blanket reference to the Corona virus will not suffice to release the contractor from its obligation to perform.

Contractual regulation

If there is no possibility of recourse to force majeure, in such a case and when new contracts are concluded, only an express contractual provision, which, e.g., expressly provides for an exclusion of liability for the Corona virus and the associated aftereffect, can release from the obligation to perform. This contractual regulation would apply irrespective of the concept of force majeure. However, such a clause must be negotiated by the contracting parties and must be included in the contract accordingly.

This possibility is suitable for future contracts which are to be concluded during Corona. However, they are only effective for the future and thus do not cure contracts which did not contain such a clause but were nevertheless already concluded with knowledge of the Corona virus.

Missing contractual clause

If a contract does not contain an express exclusion of liability for specific events (such as the Corona virus) or a provision on force majeure, the statutory provisions of the applicable law to which the contract is subject shall apply to the possibility of exemption from the obligation to perform. This law may vary from case to case and each legal system contains different regulations.

a) UN Convention on Contracts for the International Sale of Goods

The UN Convention on the International Sale of Goods (CISG) is applicable to international sales contracts. The buyer and seller must be domiciled in two different member states. If the CISG is applicable, it contains a force majeure clause. According to Article 79 of the CISG, "A party shall not be liable for the non-performance of any of its obligations if it proves that the non-performance is due to a cause beyond its control and that it could not reasonably have been expected to take the cause of non-performance into account when entering into the contract or to avoid or overcome the cause of non-performance or its consequences." This provision releases a party from liability for non-performance for reasons beyond its control. On this basis, claims for damages against this party can be excluded. If the Corona virus thus still constitutes force majeure, an exclusion of liability would be possible under the CISG.

If the CISG is not applicable, the provisions of the respective applicable national legal system shall apply.

b) German law

The German Civil Code (BGB) does not contain any express regulation on the concept of force majeure regarding deliveries. Therefore, the general legal regulations must be resorted to. Here, the basis is the inability to perform the contractual obligations. In its case law, the German Federal Court of Justice considers force majeure to be "an external event that has no operational connection and cannot be averted even by exercising the utmost care that can reasonably be expected".

Recommended course of action

With regard to the current developments and the spread of the Corona virus, companies are advised to review their existing contracts and terms and conditions regarding the force majeure clause. The scope of the clause in question should be taken into account.

Any ambiguities in the force majeure clause or loopholes in existing contracts should be resolved by the contracting parties, preferably together, as both parties may be affected by the effects of the Corona virus and its consequences. This must be agreed and documented accordingly.

It is also advisable to take the results of the review as an opportunity to make appropriate contractual adjustments for future contracts. If necessary, clauses for the future must be adapted and revised. Clear regulations help to prevent disputes.

Regardless of this, companies should check their insurance policies to see whether they cover the consequences of the Corona virus.

Emergency measures in civil law

In March, the German government presented a draft for a temporary amendment of certain provisions in civil law. For example, certain deadlines are to be frozen if payments and other contractual obligations cannot be met on time due to the Corona epidemic. However, payments must be made at a later date, no exemption is provided for, nor is an adjustment of contracts on the legal basis of the "doctrine of frustration". Nevertheless, in individual cases, a court may come to the conclusion that the circumstances presented when the contract was concluded do not (no longer) exist and therefore the contract had to be amended or even cancelled.

Due to the unclear development, the contracting parties must therefore closely follow the legal requirements and amendments of the legislator and, if necessary, react appropriately.

+++

Chapter Two

Work from Home



ALLIURIS SUMMER SCHOOL | JULY 2020

- WORK FROM HOME (Open Discussion)
 - Program:
 - Short introduction of participants and moderator;
 - Open discussion;
 - End.

ALLIURIS

MARREE+
DIJXHOORN
ADVOCATEN

Introduction

- Please introduce yourself;
 - name;
 - country/firm;
 - brief description of your firm (one per firm);
 - legal expertise;
 - motivation to attend the Summer School.

ALLIURIS

MARREE+
DIJXHOORN
ADVOCATEN

Topics of open discussion

General information:

1. How did your firms handle the work from home issue during lock down?
2. What was/is your personal experience while working at home?

In your jurisdiction:

3. Can an employer force employees to work from home?
4. Can an employee refuse to work at the office being afraid to be contaminated?
5. Can an employer force its employees to be tested?
6. Does an employer need to pay extra compensation, or less?

ALLIURIS

MARREE+
DIJXHOORN
ADVOCATEN

7. Do we need to take measures regarding cybersecurity, GDPR, privacy?
 8. Who is responsible for a safe and healthy working environment?
 9. Can one be liable for contaminating others?
- Future developments:
10. Should we keep working from home?
 11. Biggest advantage and biggest disadvantage of working from home?
 12. Will sustainability be a driver for prolonging work from home?

End

ALLIURIS

MARREE+
DIJXHOORN
ADVOCATEN



herfurth.partner

Home Office Agreement

Antonia Herfurth
Attorney at Law in Munich and Hanover
21 July 2020

herfurth.partner

Structure of Home Office Agreement – Art. 1 to 7

- Preliminary note
- Art. 1 Subject of the Additional Agreement
- Art. 2 Commencement of Work
- Art. 3 Place of Work
- Art. 4 Working Hours and Working Hours Recording
- Art. 5 Structure and Control
- Art. 6 Remuneration
- Art. 7 Equipment of Home Office

herfurth.partner

Structure of Home Office Agreement – Art. 8 to 15

- Art. 8 Use of Company Equipment
- Art. 9 Expenses and Disbursements
- Art. 10 Communication
- Art. 11 Data Protection and Secrecy Protection
- Art. 12 Access to Home Office for Control Purposes
- Art. 13 Extraordinary Circumstances
- Art. 14 Home Office Accidents and Damage
- Art. 15 Holiday

herfurth.partner

Structure of Home Office Agreement – Art. 16 to 23

- Art. 16 Duty of Confidentiality
- Art. 17 Withdrawal and Termination of Home Office
- Art. 18 Obligation to Return Property Belonging to the Employer
- Art. 19 Contractual Penalties
- Art. 20 Limitation Periods
- Art. 21 Amendment of Agreement
- Art. 22 Saving Provisions
- Art. 23 Clarification and Receipt of Agreement

Working Hours



Working Hours

- Same working hours rule like in office
 - 8 hours/working day or 10 hours if average of 8 hours/day not exceeded within six calendar month (GER)
- Breaks and rest periods
 - After 6 hours 30 min break, after 9 hours 45 min (GER)
 - Rest period 11 hours (GER)
 - Availability in certain time slots
- Tracking working hours by working hours recording (start, break times, end)

herfurth.partner

Structure and Control

Task	Mon 05/19	Tue 06/19	Wed 07/19	Thu 08/19	Fri 09/19
08:00					
09:00					
10:00					
11:00					
12:00					
13:00					
14:00					
15:00					
16:00					
17:00					
18:00					
19:00					
20:00					

herfurth.partner

Structure and Control

- Calender of activities and expectations (digital tools)
- Reporting system
- Appraisal system
- Managing and measuring of performance (taken into account employee's circumstances)

herfurth.partner

HOME OFFICE ERGONOMIE

Equipment of Home Office


herfurth.partner

Equipment of Home Office

- Safety and health standards apply as well in home office → technical, organisational and personal measures
- Ergonomic equipment (e.g. chair, desk), laptop, printer, office supplies
- Exclusive use of operating equipment and exclusion of private use
- (P) Control?
 1. Employer visits employee's home office
 2. Sending photos of workspace to employer
 3. Partially exemption of employer of workspace regulations

herfurth.partner

Expenses



The slide features a blue header with the text 'herfurth.partner'. Below the header, the word 'Expenses' is written in a black sans-serif font. To the right of the text are three square icons: a yellow one with a white electrical plug, a light blue one with a white water drop, and an orange one with a white radiator. A thin horizontal line is positioned below the text and icons.

herfurth.partner

Expenses and Disbursements

- Reimbursement of necessary expenses (electricity, water, heating e.g.)
- Laid down in writing which costs employer will bear and in what amount (flat rate recommended)
- Reimbursement of rent?
 - Only partly
 - If private use is considerably restricted which means flat is partly „useless“

herfurth.partner

Communication



herfurth.partner

Communication

- How employer and employee will keep in touch
- Availability in certain time slot
- Response in certain time (e.g. during regular work time)
- Supervisors contactable at a set period each week/fortnight
- Frequent company-wide meetings
- Guidelines for videoconferences

Data & Secrecy Protection



Data Protection and Secrecy Protection

- Information and guidance of employee
- Appropriate secrecy measures:
 - No use of private devices, only company equipment
 - Computer software and antivirus software up to date
 - No storage of sensitive data on external devices
 - Use of secure passwords and not passing them on
 - Confidential documents stored in lockable room in lockable cupboard
 - Data protection conform destroying of documents
 - And more...



Accidents and Damage

Home Office Accidents and Damage

- Office: statutory accident insurance or liability insurance taken out by employer
- Home office: statutory accident insurance
- Damage during work-related activity → (P)
 - Injured in office on way to coffee machine → work accident
 - Injured in home office on way to coffee machine → **no** work accident
- Evidences that accident occurred during work-related activity
- Self insurance: occupational disability insurance or private accident insurance

Withdrawal and Termination



Withdrawal and Termination of Home Office

- Termination of employment agreement
- Withdrawal
- On expiry of time
- Right to recall of employer when safety and health standards not met
- Lapse of the extraordinary event (e.g. Covid-19)



herfurth.partner

COPYRIGHT BY
HERFURTH & PARTNER
RECHTSANWALTSGESELLSCHAFT MBH
HANNOVER · GÖTTINGEN · BRÜSSEL

MEMBER OF
ALLIURIS GROUP
ALLIANCE OF INTERNATIONAL BUSINESS LAWYERS

BRUSSELS · PARIS · LONDON · AMSTERDAM
AMERSFOORT · LYON · MADRID · BARCELONA · LISBON
MILAN · DUBLIN · COPENHAGEN · HANOVER · ZUG · VIENNA
MOSCOW · MINSK · BUCHAREST · ATHENS · NICOSIA
ISTANBUL
BEIJING · SHANGHAI · NEW DELHI
NEW YORK · SAO PAULO · RIO DE JANEIRO · BRASILIA

LUISENSTR. 5 info@herfurth.de
30159 HANNOVER www.herfurth.de
FON 0511 307 56-0
FAX 0511 307 56-10

herfurth.partner

COPYRIGHT BY
Herfurth & Partner
RECHTSANWALTS
GESELLSCHAFT MBH

MEMBER OF
ALLIURIS
ALLIANCE OF
INTERNATIONAL
BUSINESS
LAWYERS

HANNOVER
GÖTTINGEN
BRÜSSEL

BRUSSELS
LONDON
PARIS
AMSTERDAM
AMERSFOORT
LYON
MADRID
BARCELONA
LISBON
MILAN
DUBLIN
COPENHAGEN
HANOVER
GÖTTINGEN
ZUG
VIENNA
SALZBURG

MOSCOW
MINSK
ATHENS
ISTANBUL

BEIJING
SHANGHAI
GUANGZHOU
WUHU
NEW DELHI
MUMBAI

NEW YORK
CHICAGO
SAN FRANCISCO
LOS ANGELES
ORANGE COUNTY
SAO PAULO
RIO DE JANEIRO
BRASILIA

LUISENSTR. 5
30159 HANNOVER
FON 0511 307 56-0
FAX 0511 307 56-10

info@herfurth.de
www.herfurth.de

Question & Answers

Work from Home

1. Which practical problems exist in the “work from home“ mode?

Maria Inês Reis (Portugal):

Well I had to buy a printer because I could not print at home and schools were shut down so having children in the house was quite challenging, but I noticed that I work a lot more hours and manage family time and work time better.

Iv Fangyuan (China):

This work mode does not apply to workshop workers.

Qiu Shuang (China):

- Interpersonal communication is blocked and information is blocked. I am not familiar with my colleagues and cannot keep abreast of the latest strategy and business adjustment of the company.
- It is easy to fall behind in business. Working at home cannot participate in group meetings, training, technical seminars.
- Work at home is easy to cause work procrastination and cannot be completed in time.

Qiyi Zhang (China):

Home working mode has become a common and safe working mode during the Corona Epidemic. The sudden attack of the epidemic has caught people by surprise and forced them to work from home. However, home-based work also brings a lot of problems. For example, the employer cannot remotely supervise whether the employees work on time according to the rules and regulations, and the employees' work efficiency is low due to the lack of supervision. Not all jobs are suited to working from home. In the final analysis, telecommuting at home is suitable for a small number of jobs and groups, such as new media practitioners, e-commerce, sales and other groups. Their work itself relies heavily on the Internet and has low requirements for the working environment and office equipment. But for more collaborative work is

also not suitable at home. If there is a procedural upstream and downstream relationship between each other's work, it is better to be able to work together to discuss the work. From the legal point of view, because the home office, employers cannot supervise the behaviour of employees, employees if out during office hours, there are accidents, whether should be handled according to the injury. For example, employees working from home lead to longer working hours but cannot calculate overtime costs.

2. Which laws exist in your country that affect work from home?

Maria Inês Reis (Portugal):

None really. We can actually work from home because we have a platform called Citius, that is used online, so we can work from home and still manage to get things done, in litigation area I mean.

Qiu Shuang (China):

Chinese law stipulates that "if a worker claims overtime pay, he / she shall bear the burden of proof for the existence of overtime. However, if the laborer has evidence to prove the existence of the employer's knowledge of overtime work, and the employer fails to provide such evidence, the employer shall bear the adverse consequences. " Under the traditional working mode, the working hours of employees can be controlled, while in the new working mode of working from home, enterprises can hardly measure or control the working hours of employees.

Qiyi Zhang (China):

Suggestions on novel Coronavirus Disease Prevention and Control to Stabilize Labour Relations and Support enterprises to resume work and Production

Notice on novel Corona virus infection pneumonia epidemic and work related to labour Relations

Notice of Guangdong Provincial Department of Human Resources and Social Security

State Administration of Taxation concerning the payment and treatment of social Insurance during the novel Coronavirus epidemic prevention and control

A number of policy measures to increase support for smes in response to the impact of the epidemic and so on.

3. Which rules would you provide when drafting a “work from home”-agreement with employees?

Iv Fangyuan (China):
Labor Contract Law

Qiyi Zhang (China):
Employees can be on time to work, through the network platform clocking records. The enterprise should also keep a good record of the working hours, confirm the overtime work in time and pay the workers in full when the salary is paid.

Home Office Agreement

Additional agreement to the existing employment contract

Between

(Employer)

- Employer -

and

(Employee)

- Employee -

Preliminary note

(Information about already existing employment contract)

Art. 1

Subject of the Additional Agreement

Art. 2

Commencement of Home Office

Art. 3

Place of Work

Art. 4

Working Hours and Working Hours Recording

- Flexible working arrangement, e.g. for employees who need to provide childcare.
- Availability in a certain time slot.
- Confirming overtime work in time.
- A guarantee provision of the employer for underworking (establish right to compensatory work), overworking has to be determined as well (forbidden without written notice by employer).
- How work-life balance will be managed.
- Voluntary specific computer programs which monitor the activity of the worker on the PC.

Art. 5
Structure and Control

- Concrete calendar of activities and expectations + tools that are available for it (digital).
- Establishing work schedule
- Suitable reporting system
- Suitable appraisal system
- How performance will be managed and measured - taking into account people's circumstances where necessary.

Art. 6
Remuneration

- Pay the workers in full when salary is paid.

Art. 7
Equipment of Home Office

- The minimum hardware which the employer will provide if required.
- An internet policy to provide faster broadband if required.
- Confirmation of suitability of home-working environment.
- Who employees should contact if they have any problems or their circumstances change.

Art. 8
Use of Company Equipment

Art. 9
Expenses and Disbursements

- Expenses the employee may claim back due to having to work from home.

Art. 10
Communication

- How the employer and the employee will keep in touch.
- Availability in a certain time slot.
- Response in a certain time (e.g. 24h).
- Supervisors/line managers contactable at a set period each week/fortnight.
- Company-wide meeting at least once a month.
- How the employees will communicate with other staff and managers.
- Guideline for video calls.

Art. 11

Data Protection and Secrecy Protection

- Rules around storing information and data protection.
- Use of a given communication program to transfer work-based data to colleagues.
- Who employees should contact if they have any problems or their circumstances change.

Art. 12

Access to Home Office for Control Purposes

- Confirmation of suitability of home-working environment.

Art. 13

Extraordinary Circumstances

- Organisation of teams that attend the office during the week.
- Right to enter for work related purposes, e.g. health and safety matters.
- Asking of the use of the Corona App if they work with vulnerable groups.

Art. 14

Home Office Accidents and Damage

Art. 15

Holiday

- Voluntary holiday arrangements

Materials | Compact

Work from Home

*Antonia Herfurth, Rechtsanwältin in Munich and Hanover
April 2020*

For reasons of secrecy and data protection - more on this at once - the employee should work in the home office with operating equipment provided by the employer. The use of private PCs, notebooks and also smartphones (*bring your own device / BYOD*) would require considerable additional security measures. For PCs and laptops, the software must always be up-to-date and an anti-virus program must be installed. The internet must be sufficiently fast to allow videoconferences, for example. Otherwise, the employee must order a tariff with a higher bandwidth at the employer's expense.

The set-up and equipment of the home office should be agreed in writing between the employer and the employee. In reality, however, implementation and control often fail. The employer cannot control whether the employee always sits in the ergonomically equipped home office or on the sofa. Furthermore, the ownership of the purchased items should be recorded and the private use of equipment purchased by the employer should be excluded.

The employee has a duty to cooperate in ensuring his safety and health at work. The employer, for his part, must inform the employee in detail about the correct setup of the home office. In addition, the employer should offer to visit the employee's home office and assess whether the required standards have been met or need to be improved. One problem is that the employer has no right to visit the employee's home office. The German constitution protects spatial privacy. However, the employee should be cooperative. If he denies access, photos of the workplace can be sent to the employer. If the employee also refuses to do so, the workplace regulations may be partially exempted in favour of the employer.

Protection of secrets and data protection

Companies are subject to increased due diligence obligations with regard to the protection of trade secrets. If companies do not protect confidential information by taking appropriate secrecy measures, this information may lose its legal protection as a

trade secret. As a result, companies are not entitled to any legal claims if third parties obtain information against the company's will.

When working from home, there is an increased risk that unauthorized third parties may gain access to confidential data and documents. This can happen by connecting private devices, which may not comply with data and secrecy protection requirements, to professionally used and protected devices or by listening to business calls by other people living in the household or voice assistants such as Google Home, Siri or Alexa.

Since secrecy and data protection is extremely sensitive, a written agreement is required. This agreement regulates which measures the employee has to take in the home office in order to guarantee the increased protection standards.

In order to meet the standards, an employee in the home office may not use his private devices for reasons of secrecy protection - legally, he does not have to. For this reason too, the employer should provide company equipment and keep its software up to date.

The employee may not store sensitive data on external devices, but only on the company server, and he may only use VPN connections. The hard disk of the company PC or laptop should be encrypted. The employee is obliged to set up secure passwords and not to pass them on. Professional e-mails may not be forwarded to the private mailbox. If the employee does not live alone in the household, he must activate the screen lock when leaving the workplace. Confidential documents must be stored in a lockable room in a lockable cupboard; and he must prevent family and friends from accessing the documents. If documents are no longer required and can be destroyed, he must dispose of them in accordance with data protection regulations, for example by using an appropriate shredder with particle cut or by tearing them into very small pieces (confetti).

Reimbursement of expenses for resources of the employee

The employee can basically demand reimbursement of the - necessary - expenses incurred by the home office from the employer. For this purpose, it should be laid down in writing whether and if so, which costs the employer will bear. The employee must provide evidence of the costs incurred. These are likely to be mainly electricity and working materials such as paper or toner. If an internet flat rate exists, the employee cannot demand reimbursement from the employer due to increased internet use, as the costs for the flat rate would have been incurred anyway.

Since it can be difficult to break down the expenses incurred (especially for electricity, water, heating), a monthly flat rate is recommended, e.g. EUR 50.00. The employee can only demand reimbursement of a part of the rent from the employer if the private use

of the own flat during home office is considerably restricted and the flat is therefore partly "useless".

Working time recording

The employee is also subject to the same working time rules in the home office as in the office. For this purpose, the employer should set fixed working hours, similar to those in the office.

To enable the employer to track the working hours, the employee must document the start of the workday, break times and the end of work. In principle, the employer must also provide the employee with remote access to the company's legally compliant time recording system. The employer cannot check whether the employee actually works as specified. He must trust the employee. Similarly, the employee must trust the employer to ensure that he is not monitored, for example by webcam or keyloggers that record the employee's keystrokes. For monitoring purposes, the employer should therefore not only have time statements presented to him, but also, at certain intervals, proof of performance.

Compliance with rest periods required by law

The scope of the working time to be performed results from the employment contract or collective bargaining agreement. In the home office, the German Working Hours Act (*Arbeitszeitgesetz*) applies just as in the office.

The employee may not work more than eight hours per day or ten hours if the average working time of eight hours per working day is not exceeded within six calendar months. The employee must also observe breaks and rest periods as in the office: After six hours of work, the employee is entitled to a 30-minute break, after nine hours to a 45-minute break. Between the end of work and the start of work the next day, there must be at least eleven hours without interruption. As with daily working hours, the rest period can be shorter on some days. Therefore, it must be at least twelve hours on another day - and this within a calendar month or within four weeks.

Particularly problematic when working from home is an interruption of the rest period, usually due to communication. This is because the interruption of the rest period causes the eleven hours to start again.

It is controversial and not clearly clarified in court whether there is an interruption if the employee gives a short information by telephone or sends e-mails in the evening. It is argued that every interruption is working time because the rest period is for recreation. Other opinions weight the activity and assume an interruption only if a certain threshold

is exceeded. This can easily be the case if a supervisor becomes active and requires the employee to answer technical questions, for example.

It is advisable to define times in which the employee must be available. This helps to ensure that rest periods are observed. The working time recording not only helps as a control instrument for the employer, but also for the employee himself. It is hardly possible to ensure that rest periods are observed. As an extreme measure, the employer can prohibit work during the rest period. A North German automobile company has even switched off its mail server at night to ensure that rest periods are observed.

Incidentally, the employee himself is responsible for observing the rest periods. Working from home requires more self-discipline and self-organization than work in the office.

Insurance cover in the home office

If the employee suffers a damage in the office or otherwise in connection with his professional activity, this is a case for the statutory accident insurance or the liability insurance taken out by the employer.

The employee is also subject to the statutory accident insurance in the home office. The decisive factor is that the damage occurs during an activity that is factually related to work. This is where things get complicated because there are considerable differences between home office and office work: The statutory accident insurance applies if the employee is injured in the office on the way to the coffee machine, but it does not apply in the home office when getting a coffee from the own kitchen. Accident-insured activities in the home office are, for example, accepting a parcel with office supplies needed for work and fetching company documents from the printer. Accepting a private parcel or getting a drink from the kitchen during working hours is not covered by accident insurance.

In the event of damage, the employee should gather precise evidence as quickly as possible that the accident occurred in connection with his professional activity. If he cannot prove this, the statutory accident insurance will not pay in case of doubt and the employee must pay for the damage himself. Therefore, he could document when he is working on which document, save his call lists or take screenshots.

If an employee wants to make sure that he is fully insured, he should take out insurance himself. In addition to occupational disability insurance, private accident insurance can also be considered.

Conclusion

There are three points to consider when working from home:

- Information
- Written agreement
- Trust

In the home office, the employer has fewer possibilities to control compliance with data protection, technical and health requirements. Therefore, a precise education of the employee is indispensable by information meetings or information brochures, in which employees are sensitized for questions, problems and obligations around home office. A written home office agreement with detailed regulations is also important. Such regulations impose increased duties of care on the employee. Apart from that, employer and employee must trust each other.

It is important that all measures and regulations are not limited to the current Corona pandemic but are always applicable when employees work from home. The current Corona crisis is the cause, but not the reason, for the need to regulate the work of employees in the home office.


In fact, to the surprise of many, it turns out that the remote work for the company works better than expected: The systems and networks withstand the strain, the processes are inevitably more structured, digital document management more disciplined. And it turns out that many time-intensive and cost-intensive business trips can be replaced by video conferencing. But new perspectives are also opening up for employees: They can better organize family care, such as the distances and background to day-care centres or school.

Experts not only see the Corona crisis as a boost for further digitization, but also expect a new mix of work arrangements in the future based on this experience. Employers should prepare for this in good time.

+++

Chapter Three

Data Protection Update International



**HAMMURABI
& SOLOMON
PARTNERS**

**INDIA 2020: DATA PROTECTION, PRIVACY &
DIGITALIZATION COMPLIANCE FOR
BUSINESSES**

(An Outline on Data Protection Regime in India)

**Dr. Manoj Kumar
Founder & Managing Partner**

22/07/2020
©hammurabisolomonpartners

AGENDA



- Historical Context of Data Protection Laws in India
 - Legislative and Judicial Timeline
- Introduction to the Present and Proposed Indian Data Protection Laws through the EU GDPR Lens
 - Scope of Application
 - Key Definitions
 - Grounds for Data Processing
 - Key Obligations of Data Controllers/Data Fiduciaries
 - Key Rights of Data Subjects
- Cross-border transfers of Data and Data Localization

Historical Context of Data Protection Laws in India



Timeline

- **Information Technology Act, 2000**
 - 1997 UNCITRAL Model Law on E-Commerce
 - Electronic Communications and Information Storage
- **Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.**
 - Scope of Application: data of individuals located in India.
 - Privacy Policy and Disclosures
 - Collection and Reasonable Security Practices
- **2012 Report of the Group of Experts on Privacy – 9 principles**
 - (a) Notice; (b) Choice & Consent; (c) Collection Limitation; (d) Purpose Limitation; (e) Access & Correction; (f) Disclosure; (g) Security; (h) Openness; and (i) Accountability
- **Information Technology (the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules of 2013**
 - Data Breach Reporting and Compliance Mechanism

2

Historical Context of Data Protection Laws in India



Timeline

- **Justice K.S. Puttaswamy (Retd.) v. Union of India – 2017
Supreme Court of India**
 - Whether Privacy is a constitutionally protected value?
Answer:
“Privacy is a constitutionally protected right which emerges primarily from the guarantee of life and personal liberty in Article 21 of the Constitution. Elements of privacy also arise in varying contexts from the other facets of freedom and dignity recognised and guaranteed by the fundamental rights”
 - Informational Privacy is a facet of Right to Privacy
 - “The challenges which big data poses to privacy interests emanate from State and non-State entities.”
 - “Yet, it is now a universally accepted fact that information and data flow are “increasingly central to social and economic ordering”

3

Historical Context of Data Protection Laws in India



Timeline

- **Justice BN Srikrishna Committee Report**
 “A Free and Fair Digital Economy Protecting Privacy, Empowering Indians”

- **Draft Personal Data Protection Bill, 2018**
 - Normative foundation - Supreme Court Privacy Judgment

- **Personal Data Protection Bill, 2019**
 - December 2019 – Introduced in Indian Parliament
 - Joint Parliamentary Committee
 - 3rd February 2020 to 24th February 2020 – comments invited
 - JPC Report expected in next Parliamentary Session

Indian Data Protection Laws through EU GDPR Lens



- **Scope of Application - Territorial**

GDPR	Present Indian Law	PDP Bill
<p>Organizations that have an establishment in the European Union and process personal data “in the context of” the EU establishment.</p> <p>Organizations that are not established in the EU but process personal data in relation to either (a) offering goods or services in the EU; or (b) monitoring the behavior of individuals in the EU.</p>	<p>Body corporates Body Corporate (Definition): -any company -a firm -sole proprietorship other association of individuals engaged in commercial or professional activities; FOR -collection -disclosure -transfer of personal information and sensitive personal data.</p> <p>However, the IT Rules only apply to processing of data of individuals located in India, limiting their scope.</p>	<p>Processing personal data that has been collected, disclosed, shared or otherwise processed within the territory of India</p> <p>Entities: -Indian companies -Indian citizens, and -Any other persons or bodies incorporated or created under Indian law</p> <p>Organizations that are not present in India, but nexus: 1. business carried out in India 2. any systematic offering of goods or services to individuals in India; 3. an activity that involves profiling individuals in India</p>

Indian Data Protection Laws through EU GDPR Lens



• Scope of Application – Subject Matter

GDPR	Present Indian Law	PDP Bill
i. Personal data — anonymous data is out of scope ii. Automated processing or non-automated processing where personal data forms part of a filing system. EXCLUDING: -Personal data processed by natural persons for purely personal or household purposes. -Processing by law enforcement and national security agencies.	The obligations under the IT Rules only apply to companies collecting personal data from an individual, for the purpose of directly providing a service to that individual. Several sectoral laws address data confidentiality: -healthcare -telecommunications -banking -other financial services	Processing personal data that has been collected, disclosed, shared or otherwise processed within the territory of India Entities: -Indian companies -Indian citizens, and -Any other persons or bodies incorporated or created under Indian law Organizations that are not present in India, but nexus: 1. business carried out in India 2. any systematic offering of goods or services to individuals in India; 3. an activity that involves profiling individuals in India

6

Indian Data Protection Laws through EU GDPR Lens



• Key Definitions – Personal Data

EU GDPR	Indian Law (Present)	PERSONAL DATA PROTECTION BILL
Personal Data any information relating to: -an identified or identifiable -natural person	Personal Information "any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate , is capable of identifying such person.	Personal Data relating to a natural person - directly or indirectly identifiable -characteristic, trait, attribute or any other feature -combination of features with any other information, -whether online or offline, -- shall include any inference drawn from such data for the purpose of profiling

7

Indian Data Protection Laws through EU GDPR Lens



• Key Definitions – Sensitive Personal Data

EU GDPR	Indian Law (Present)	PERSONAL DATA PROTECTION BILL
Special Categories of Personal Data	Personal Information	Sensitive Personal Data
Personal Data revealing: Racial or ethnic origin. • Political opinions, religious or philosophical beliefs. • Trade union membership. • Genetic data. • Biometric data • Health. • Sex life or sexual orientation.	-passwords; -financial information such as bank account or credit card or debit card or other payment instrument details; -physical, physiological and mental health condition; -sexual orientation; -medical records and history; -biometric information	-Financial data -Health -Official identified -Sex Life and Sexual Orientation -Transgender or intersex status -Biometric Data -Genetic Data -Caste or Tribe Religious or Political Belief or affiliation

8

Indian Data Protection Laws through EU GDPR Lens



• Key Definitions - Controller

EU GDPR	Indian Law (Present)	PERSONAL DATA PROTECTION BILL
Controller	Not defined specifically	Data Fiduciary
The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data	The Indian Information Technology Act, 2000 and the Rules thereunder do not identify the Client, Data Controller, or Data Processor as distinct entities.	Any person, including the state, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data.

9

Indian Data Protection Laws through EU GDPR Lens



- Key Definitions – Processor and Data Subject

EU GDPR	Indian Law (Present)	PERSONAL DATA PROTECTION BILL
Processor A natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller	Not defined The Indian Information Technology Act, 2000 and the Rules thereunder do not identify the Client, Data Controller, or Data Processor as distinct entities.	Data Processor Any person, including the state, a company, any juristic entity or any individual, who processes personal data on behalf of a data fiduciary.
Data Subject identified or identifiable natural person	Not defined	Data Principal the natural person to whom the personal data relates

10

Indian Data Protection Laws through EU GDPR Lens



- Key Definitions – Data Processing

EU GDPR	Indian Law (Present)	PERSONAL DATA PROTECTION BILL
Processing Operation (or sets) performed on personal data (or sets), whether or not by automated means , such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation , use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.	Not defined	Processing An operation or set of operations performed on personal data May include collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing , disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction

11

Indian Data Protection Laws through EU GDPR Lens



- Key Definitions – De-Identification

EU GDPR	Indian Law (Present)	PERSONAL DATA PROTECTION BILL
Pseudonymisation	Not defined	De-identification + Anonymisation
Operation or set of operations performed on personal data or sets of personal data, whether or not by automated means , such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.		<p>De-identification: remove, or mask identifiers from personal data, or replace them with such other fictitious name or code that is unique to an individual but does not, on its own, directly identify the data principal</p> <p>Anonymisation: irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified.</p>

12

Indian Data Protection Laws through EU GDPR Lens



- Key Definitions – De-Identification

EU GDPR	Indian Law (Present)	PERSONAL DATA PROTECTION BILL
Pseudonymisation	Not defined	De-identification + Anonymisation
<p>“the data can no longer be attributed to a specific data subject without the use of additional information, [...] such additional information is kept separately”</p> <p>Anonymisation: “personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.”</p>		<p>De-identification: remove, or mask identifiers from personal data, or replace them with such other fictitious name or code that is unique to an individual but does not, on its own, directly identify the data principal</p> <p>Anonymisation: irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified.</p>

13

Indian Data Protection Laws through EU GDPR Lens



• Key Definitions – Consent

EU GDPR	Indian Law (Present)	PERSONAL DATA PROTECTION BILL
Consent	Section 14 – Indian Contract, 1872	Consent
'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;	Consent is said to be free when it is not caused by: a. Coercion b. Undue influence c. Fraud d. Misrepresentation e. Mistake <u>IT Rules:</u> -Personal Information – no consent -Sensitive Personal Data: consent is required	Valid consent is: (a) Free (as per Section 14 (b) Informed, (c) Specific, (d) Clear, (e) Capable of withdrawal. In respect of Sensitive Personal Data, consent has to be explicitly obtained : 1) After informing the purpose 2) In clear terms 3) After giving choice of separately consenting to purposes of operations.

14

Indian Data Protection Laws through EU GDPR Lens



• GROUNDS FOR DATA PROCESSING

• GDPR

- Consent
- Contract
- Legal Obligation
- Vital Interests
- Public Task
- Legitimate Interests

15

Indian Data Protection Laws through EU GDPR Lens



GROUNDNS FOR DATA PROCESSING

Present Indian Law

- Consent: Only for Sensitive Personal Data
- Notice Obligations:
 - The fact that the data is being collected
 - The purpose for which the data is being collected
 - The intended recipients of the data
 - The name and address of the agency collecting the information and the agency that will retain the information

16

Indian Data Protection Laws through EU GDPR Lens



GROUNDNS FOR DATA PROCESSING

- PDP Bill
 - Consent
 - State Functions
 - Nature of Function
 - Nature of Entity
 - Extent to which Personal Data can be processed
 - In compliance with law: To ensure the Data Protection does not hinder course of law
 - Prompt action: such as health emergency
 - For purposes related to employment
 - Recruitment/Employment Relationship
 - Reasonable purposes

17

Indian Data Protection Laws through EU GDPR Lens



Key Obligations of Data Controllers/Fiduciaries

GDPR	OBLIGATION	INDIAN LAW (PRESENT & PDP)
<p>Article 5 read with Recital 39: Data must be Processed in manner which is lawful, fair and transparent.</p> <p>Information shared must be: -concise -transparent, -intelligible and in easily accessible form, using clear and plain language.</p> <p>Notice must be provided at of before the time of collection (If Indirectly collected: within one month; Unless- impossible/disproportionate effort</p> <p>Content of Disclosure: -Obligation to provide Data or not -Purpose -Third Party Sharing</p>	<p>LAWFULNESS, FAIRNESS, & TRANSPARENCY</p>	<p>PRESENT: CONSENT AND NOTICE PDP: Sections 4 &5: specific, clear, lawful purpose, fair and reasonable , ensure privacy of data principal</p> <p>Notices: clear, concise and easily comprehensible to a reasonable person. Translation, if required.</p> <p>Notice at time of collection. (If indirectly collected – As soon as reasonably practicable) UNLESS “substantially prejudice the purpose of processing”</p> <p>Contents of Notices: -Disclosure: parties with whom data shared (esp. cross-border) -Grievance procedure -Rating/Data Trust Score</p>

Indian Data Protection Laws through EU GDPR Lens



Key Obligations of Data Controllers/Fiduciaries

GDPR	OBLIGATION	INDIAN LAW (PRESENT & PDP)
<p>Data collected for specified, explicit and legitimate purposes</p> <p>Adequate, Relevant, and Limited</p>	<p>Purpose Limitation</p> <p>Data Minimization</p>	<p>Only to the extent that is necessary for the purposes of processing of personal data</p> <p>Undertake periodic review to determine whether it is necessary to retain the personal data in its possession</p>
<p>Data is accurate, up to date, erased or rectified without delay</p>	<p>Accurate</p>	<p>Ensure: complete, accurate, not misleading and updated, having regard to the purpose for which it is processed</p>
<p>Required that the period for which the personal data are stored is limited to a strict minimum.</p>	<p>Minimal Period</p>	<p>Data fiduciaries may “not retain any personal data beyond the period necessary to satisfy the purpose for which it is processed and shall delete the personal data at the end of the processing”. Unless explicitly consented</p>

Indian Data Protection Laws through EU GDPR Lens



Key Obligations of Data Controllers/Fiduciaries

GDPR	OBLIGATION	INDIAN LAW (PRESENT & PDP)
Take account of: -Potential risks -Interest and Rights of Data Subject -Prevent Discriminatory Effect	Security (Applicable to Data Processors under GDPR AND PDP)	PRESENT: -REASONABLE SECURITY PRACTICES AND PROCEDURES -INTERNATIONAL STANDARD REQUIREMENTS PDP: Data Fiduciary and Processor, regard to: Nature , Scope, Purpose, Risks associated, Likelihood and severity of harm
-Minimization -Pseudonymisation -Monitoring by Data Subject -Create and Improve Security Features	Necessary Safeguards	Necessary Security Safeguards: -De-identification and encryption -Protect Integrity of Personal Data -Prevent: Misuse, Unauthorised Access, Modification, Disclosure, Destruction
Measures to be reviewed and updated where necessary	Review	Both Data Fiduciary and Data Processor -in such manner as may be specified

20

Indian Data Protection Laws through EU GDPR Lens



Key Obligations of Data Controllers/Fiduciaries

GDPR	OBLIGATION	INDIAN LAW (PRESENT & PDP)
-Requirement to implement appropriate compliance processes through the lifecycle of any product, service or activity. -By default, only the personal data necessary for a purpose should be processed and personal data should not be publicly disclosed without an individual's affirmative action	PRIVACY BY DESIGN	PRESENT: Privacy Policy but not specific Privacy by Design -Data fiduciaries must "prepare a privacy by design policy" and may seek certification from the DPA for the privacy-by-design policies. Benefits: -participate in the regulatory sandbox -which provides some shelter from enforcement around the use of new technologies
<u>Controllers:</u> -notify DPA within 72 hours; unless unlikely risk to individuals -Notify Individuals without undue delay only if "high risk" <u>Processors:</u> notify controllers without undue delay	BREACH NOTIFICATION	Fiduciaries: -notify DPA "as soon as possible" if likely to cause harm to data principal -time period may be prescribed -time period make account for time required to adopt urgent measures DPA may direct publication of breach

21

Indian Data Protection Laws through EU GDPR Lens



Key Obligations of Data Controllers/Fiduciaries

GDPR	OBLIGATION	INDIAN LAW (PRESENT & PDP)
Retain Detailed Records -Written Form (and Electronic) -Purpose of Processing -Description of Categories -Categories of Recipient -Transmissions to: (a)Third Country (b)International Organization -Time limit for erasure of data -General and Organizational Security	RECORD OF PROCESSING (Also applicable to Data Processors)	PDP: Significant data fiduciaries shall maintain accurate and updated records of: 1. Important operations in the date life-cycle – -collection -transfers and -erasure of personal data 2.Periodic review of security safeguards 3. Data Protection Impact Assessment 4. Any other aspect of processing. The above also applies to the state.

22

Indian Data Protection Laws through EU GDPR Lens



Key Obligations of Data Controllers/Fiduciaries

GDPR	OBLIGATION	INDIAN LAW (PRESENT & PDP)
DPIA for HIGH RISK ACTIVITIES: - systematic and extensive profiling - processing sensitive data on a large scale; and - systematic monitoring of a publicly accessible area on a large scale. Where the risks cannot be mitigated, controller must consult DPA before engaging in processing EXCEPTIONS: -Legal basis in Union/State Law -DPIA part of General Assessment -Processing under Specific Law	DATA PROTECTION IMPACT ASSESSMENT	PRESENT: NO SUCH REQUIREMENT PDP: Applies only to significant data fiduciaries , where processing involves: 1. new technologies; 2.large-scale profiling or use of sensitive data; or 3.any other activities that carry a significant risk of harm as may be specified by regulations. All DPIAs must be submitted to the DPA for review, and the DPA may direct the data fiduciary to cease processing.

23

Indian Data Protection Laws through EU GDPR Lens



Key Obligations of Data Controllers/Fiduciaries

GDPR	OBLIGATION	INDIAN LAW (PRESENT & PDP)
<p>Required for private entities only where a “core activity” of the controller or processor involves:</p> <p>(a) the regular and systematic monitoring of data subjects on a large scale; or</p> <p>(b) the large-scale processing of sensitive data.</p> <p>The DPO must have sufficient independence and skill to carry out its functions and must be able to report to the highest levels of management within the organization.</p> <p>DPOs may be outsourced.</p>	<p>DATA PROTECTION OFFICERS</p>	<p>PRESENT: NO SUCH REQUIREMENT</p> <p>PDP:</p> <ul style="list-style-type: none"> • Appointment of a DPO is required for all significant data fiduciaries. • There are no express independence or skill requirements, but further guidance may be provided by regulations. • The DPO must be based in India. • The DPO must “represent the data fiduciary under this Act.”

Indian Data Protection Laws through EU GDPR Lens



RIGHTS OF DATA SUBJECTS

GDPR	RIGHTS	INDIAN LAW (PRESENT & PDP)
<p>Article 15 of GDPR</p> <p>Right to obtain confirmation on processing personal data from the controller.</p> <p><u>Exceptions</u>: Providing information that affect the rights and freedom of others, including intellectual rights.</p>	<p>RIGHT TO ACCESS</p>	<p>PRESENT: Rule 4 of SPDI Rules, 2011 - Policy for privacy and disclosure</p> <p>Section 17 of PDP Bill :Data Principal has the right to obtain:</p> <ol style="list-style-type: none"> 1. confirmation about the processing 2. brief summary of processing activities 3. identities of data fiduciaries and category of personal data shared. <p><u>Exception (Clause 21(5))</u>: No entertaining request, which harms the personal data.</p> <p>The exception provided under PDP Bill – may not permit withholding personal data on intellectual property grounds.</p>

Indian Data Protection Laws through EU GDPR Lens

RIGHTS OF DATA SUBJECTS



GDPR	RIGHTS	INDIAN LAW (PRESENT & PDP)
<p>Article 12</p> <p>Transparent information, communication and modalities</p> <p>Article 13</p> <p>Information to be provided where personal data is collected from the data subject</p> <p>Article 14</p> <p>Information to be provided where personal data is collected from the data subject</p>	<p>RIGHT TO BE INFORMED</p>	<p>PRESENT: Rule 6 of SPDI Rules Disclosure of information</p> <p>PDP: Section 7 read with Section 11(b) Requirement of notice for collection or processing of personal data.</p> <p>The PDP <u>does include additional disclosure requirements that may not already be included in a privacy notice drafted for GDPR.</u></p> <p>Under PDPB, requirement for more specific disclosures of data processors.</p>

Indian Data Protection Laws through EU GDPR Lens

RIGHTS OF DATA SUBJECTS



GDPR	RIGHTS	INDIAN LAW (PRESENT & PDP)
<p>Article 17 of GDPR</p> <p>Grounds to obtain right of erasure:</p> <ol style="list-style-type: none"> 1. Personal data no longer necessary 2. Data subject withdraws consent 3. Data subject objects to the processing 4. Personal data processed unlawfully. 5. For compliance with a legal obligation in Union or Member State law to which the controller is subject 6. To offer of information security services. 	<p>RIGHT TO BE FORGOTTEN</p>	<p>PRESENT: Rule 5(6) & 5(7) of the SPDI Rules 2011: These rules permit body corporate:</p> <ol style="list-style-type: none"> 1. To amend the data, if any inaccuracies 2. To not authenticate data 3. To provide an option to the provider to not to provide the data or information sought to be collected. 4. To provide goods or services for which the said information was sought if withdrawal not given in writing. <p><u>But the said Rules do not emphasise clearly on the 'right to be forgotten'.</u></p>

Indian Data Protection Laws through EU GDPR Lens RIGHTS OF DATA SUBJECTS



GDPR	RIGHTS	INDIAN LAW (PRESENT & PDP)
<p>Where controller has made personal data public, controller is obliged to:</p> <ol style="list-style-type: none"> 1. erase the personal data 2. Inform controllers which are processing the personal about the request of erasure. <p>The above stated shall not apply –</p> <ol style="list-style-type: none"> 1. To right of freedom of expression and information; compliance with a legal obligation 2. For reasons of public interest in area of public health; In the public interest, scientific or historical research or statistical purposes 3. For establishment, exercise or defense of legal claims. 	<p>RIGHT TO BE FORGOTTEN</p>	<p>Section 18 of PDP Bill – Right to correction and erasure: Data Principal has the right to –</p> <ol style="list-style-type: none"> 1. Correct inaccurate or misleading personal data; 2. To complete incomplete personal data; 3. To update personal data that is out-of-date; 4. To erase personal data which is no longer necessary for the purpose of which it was processed. <p>Section 20 of PDP Bill - Right to Freedom Data principal has the right to restrict or prevent the continuing disclosure of personal data <u>once the purpose is served; consent has been withdrawn or is contrary to this Act or any other law in force</u></p> <p>Can be enforced only by an order of an Adjudicating Officer</p>

Indian Data Protection Laws through EU GDPR Lens RIGHTS OF DATA SUBJECTS



COMPARISON OF THE RIGHT TO BE FORGOTTEN UNDER GDPR AND PDP BILL

1. The PDP distinguishes between two separate rights — one for erasure and one for restricting the disclosure of personal data (i.e., the right to be forgotten).
2. Unlike the GDPR, the PDP places responsibility for determining the scope of application of the right to be forgotten on adjudicating officers appointed by the DPA, rather than the controller.
3. Since, the adjudicating officer has to consider a number of contextual factors, the interpretation of the right to be forgotten will be narrower than then corresponding right provided under GDPR right.

Indian Data Protection Laws through EU GDPR Lens



Cross-border transfers of Data and Data Localization

GDPR	OBLIGATION	INDIAN LAW (PRESENT & PDP)
Localization is not required unless International Data Transfer requirements are not met.	LOCALIZATION OF CRITICAL DATA AND SENSITIVE PERSONAL DATA	<p>PRESENT: NO LAW ON LOCALIZATION IT RULES 2011 -Personal Data: transfer to any other body corporate or individual located in any other country, provided: same level of data protections is adhered to as provided under 2011 Rules.</p> <p>PDP BILL: •"Critical Personal Data" (to be defined by Central Government of India) shall only be processed in India.</p> <p>•"Sensitive Personal Data" may be transferred but will continue to be stored in India.</p>

Indian Data Protection Laws through EU GDPR Lens



Cross-border transfers of Data and Data Localization

GDPR	OBLIGATION	INDIAN LAW (PRESENT & PDP)
Localization is not required unless International Data Transfer requirements are not met.	LOCALIZATION OF CRITICAL DATA AND SENSITIVE PERSONAL DATA	<p>PRESENT: NO LAW ON LOCALIZATION</p> <p>PDP BILL: •"Critical Personal Data" (to be defined by Central Government of India) shall only be processed in India.</p> <p>•"Sensitive Personal Data" may be transferred but will continue to be stored in India.</p>

Indian Data Protection Laws through EU GDPR Lens



Cross-border transfers of Data and Data Localization

GDPR	OBLIGATION	INDIAN LAW (PRESENT & PDP)
Localization is not required unless International Data Transfer requirements are not met.	CONDITIONS FOR TRANSFER OF SENSITIVE PERSONAL DATA	IT RULES 2011 -Personal Data: transfer to any other body corporate or individual located in any other country, provided: same level of data protections is adhered to as provided under 2011 Rules. PDP BILL: •"Sensitive Personal Data": -Explicit Consent A-Under a DPA approved Contract or intra-group scheme (protection & liability) B-Central Govt. and DPA determine: (i) Adequate protection (ii) Jurisdictional Enforcement unaffected D-DPA allows specific purpose transfer

Indian Data Protection Laws through EU GDPR Lens



Cross-border transfers of Data and Data Localization

GDPR	OBLIGATION	INDIAN LAW (PRESENT & PDP)
GDPR doesn't require a serving copy to be maintained within the territory of the Member State.	CONDITIONS FOR TRANSFER OF CRITICAL DATA	PDP BILL: •"Critical Data": -Health Services -Emergency Services -Prompt Action To be notified by DPA -Central Government opines that such transfer does not prejudicially affect the security and strategic interest of the State

Indian Data Protection Laws through EU GDPR Lens



Cross-border transfers of Data and Data Localization

Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems

1. On 16th July 2020, in a decision that will have widespread ramifications for Data Controllers and Data Processors transmitting Personal Data from EU to the US, the Court of Justice of the European Union has ruled that:
 - a. Where the adequacy decision is not in place and the Data Protection Authority determines that the third-country cannot ensure adherence with GDPR and EU Law, the Data Protection Authority must suspend or prohibit the transfer, unless, the suspension has been given effect by the Data Controller or the Data Processor.

AND

 - b. EU Data Subjects did not have access to courts against US authorities and that the Privacy Shield Ombudsperson “cannot remedy the deficiencies” concerning judicial protection of Data Subjects. Thereby, invalidating the EU-US Privacy Shield Framework.

34



HAMMURABI & SOLOMON PARTNERS

Head Office:
405A & 405B,
Rectangle One - 4th Floor
Saket District Centre,
Saket, New Delhi - 110017

Other Locations:
GURUGRAM | MUMBAI
BENGALURU | PATNA | RANCHI

www.hammurabisolomon.com

EVERSHEDS
SUTHERLAND

International Data Transfers under the GDPR

22. July 2020

Constantin Herfurth

Associate

Data Protection & Cybersecurity



Bigger picture

GDPR

GDPR - Overview

- GDPR = General Data Protection Regulation
- Key legislation of EU data protection law
- Came into force 25 May 2016
- Applicable from 25 May 2018
- Objectives:
 - Protection of natural persons with regard to the processing of personal data
 - Free movement of personal data

GDPR - Scope

- Material scope: Processing of personal data
- Territorial scope:
 - Establishment in the EU: Processing of personal data in the context of an establishment's activities
 - No establishment in the EU: Processing of personal data relating to the offering goods or services to data subjects in the EU or to the monitoring of data subjects in the EU
- Personal scope:
 - Controllers (compliance with all obligations from GDPR)
 - Processors (compliance with fewer, specific obligations from the GDPR)

GDPR – Principles for data processing

GDPR sets out seven key principles:

- Lawfulness
- Transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (i.e. data security)
- Accountability

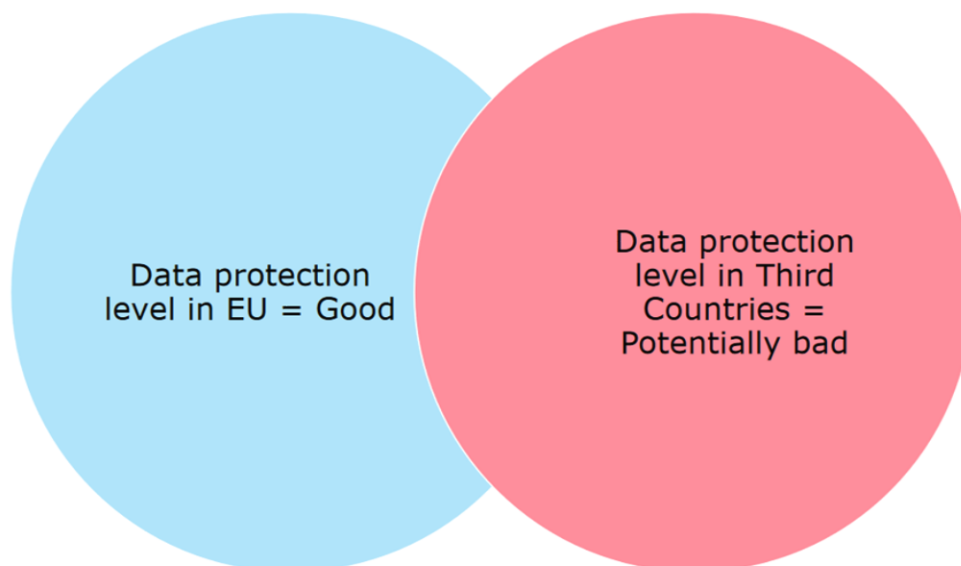
Zoom in
International Data Transfers

International Data Transfers – General principle

Art. 44 GDPR:

*"Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. **All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.**"*

International Data Transfers – General principle



Mechanism

Data protection level must „travel“ with the personal data

International Data Transfers – Mechanism

Transfers on the basis of an adequacy decision

Transfers subject to appropriate safeguards

Transfers subject to derogations for specific situations

Transfers on the basis of an adequacy decision

- European Commission has the power to determine whether a country outside the EU offers an adequate level of data protection
- Think of it as "GDPR and friends"
- Effect: Personal data can flow from the EU to that third country without any further safeguard being necessary.
- In others words: Transfers to the country in question will be treated as an transfer within EU.

List of countries with adequate data protection level

- Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay.
- Until last week: United States of America (limited to the Privacy Shield framework). CJEU has ruled that the Privacy Shield is invalid.
- Available under: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

Transfers subject to appropriate safeguards

- List of different safeguards in Art. 46 GDPR
- Most important: standard contractual clauses
- European Commission can decide that standard contractual clauses offer sufficient safeguards on data protection for the data to be transferred internationally.
- Think of "ready-to-use contracts" which cannot be amended
- So far issued two sets of standard contractual clauses
 - EU controller to non-EU or EEA controller
 - EU controller to non-EU or EEA processor
- Available under: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

Transfers subject to derogations for specific situations

- Final exception:
 - No adequacy decision applicable
 - No other appropriate safeguard applicable
- List of derogations, e.g.
 - Consent of data subject
 - Necessary for the performance of a contract
 - Necessary for the establishment, exercise or defence of legal claims
- In depth guidance on derogations:
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf

Summary

Summary

- What: Ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined.
- How:
 - Transfers on the basis of an adequacy decision
 - Transfers subject to appropriate safeguards
 - Transfers subject to derogations for specific situations
- New developments for data transfers to the US as Privacy Shield was declared invalid.



**EVERSHEDS
SUTHERLAND**

Associate, Commercial

Constantin Herfurth
constantinherfurth@eversheds-sutherland.com

www.eversheds-sutherland.com/constantinherfurth

eversheds-sutherland.com

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

© Eversheds Sutherland 2018. All rights reserved.



INDIA 2020:

**DATA PROTECTION, PRIVACY &
DIGITALIZATION COMPLIANCE FOR
BUSINESSES**

(An Outline on Data Protection Regime in India)

22/07/2020

PRIVILEGED ATTORNEY CLIENT COMMUNICATION

©hammurabisolomonpartners



INDIA 2020: DATA PROTECTION, PRIVACY & DIGITALIZATION COMPLIANCE FOR BUSINESSES

INDEX

Chapter Number	CHAPTERS	Page Number
1.	SCOPE OF APPLICATION OF LAW	2.
2.	KEY LEGAL DEFINITIONS	5.
3.	GROUND S FOR PROCESSING OF PERSONAL DATA	12.
4.	KEY OBLIGATIONS OF DATA CONTROLLERS/DATA FIDUCIARIES	15.
5.	KEY RIGHTS OF DATA SUBJECTS	26.
6.	CROSS BORDER DATA TRANSFERS AND DATA LOCALIZATION	31.



CHAPTER 1: SCOPE OF APPLICATION OF LAW

I. TERRITORIAL SCOPE OF APPLICATION OF LAW

GDPR

- i. Organizations having an establishment in the European Union and processing personal data “in the context of” the said European Union establishment.
- ii. Organizations not established in the European Union but processing personal data related to:
 1. Goods/services in European Union; or
 2. Monitoring behaviour of individuals in European Union.

PRESENT INDIAN LAW

- i. Body corporates that are related to the collection, disclosure, and transfer of personal information and sensitive personal data.
Body Corporate (Definition):
 - any company
 - a firm
 - sole proprietorshipother association of individuals engaged in commercial or professional activities;
- ii. However, the scope of the present Indian law (comprising the Information Technology Act, 2000 and the Rules thereunder) is limited as it only applies to data processing operations of individuals located in India.

The obligations under the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (“IT Rules, 2011”) are limited in application as they apply only to body corporates collecting personal data from individuals for providing services to the said individuals.

- iii. **Clarification on the Privacy Rules, issued by the former Ministry of Communications and Information in 2011:**
EXCLUDES: Indian outsourcing service providers who provide services related to personal information for:



1. collection,
2. storage or
3. handling
4. If they are under contractual obligation with any legal entity located within or outside India.

PERSONAL DATA PROTECTION BILL (PDP BILL)

- i. Processing personal data collected, disclosed, shared or otherwise processed within the territory of India
- ii. Indian companies, Indian citizens, and any other persons or bodies incorporated or created under Indian law
- iii. Organizations that are not present in India, but have a nexus with:
 1. businesses in India
 2. any systemic offering of goods/services to individuals in India;
 3. activities involving profiling of individuals in India

II. MATERIAL SCOPE OF APPLICATION OF LAW

GDPR

- i. Personal data — anonymous data is out of the scope of GDPR
- ii. Automated processing or non-automated processing where a filing system comprises personal data.

EXCLUDING:

-Processing of Personal Data by natural persons for:

- a. purely personal
- or
- b. household purposes.

-Data Processing by law enforcement agencies and national security agencies.

PRESENT INDIAN LAW

The obligations under the IT Rules 2011 only apply to companies collecting data from individuals, for the purpose of directly providing a service to that individual.

Sector and industry specific laws prescribe confidentiality of data, such as: telecommunications, healthcare, banking and financial services.



PDP BILL

Personal Data (including Sensitive Personal Data and Critical Data)

1. Anonymous data is out of the scope of PDP
2. Exception: the Central Government is empowered to direct disclosure of “anonymized” personal and “non-personal data.”

EXCLUDING

1. Processing of Personal Data by natural persons for:
 - a. purely personal.
 - b. household purposes.
 - c. journalistic purposes (as per the concerned code of ethics)

Data security principles will however apply to data processing by natural persons.

2. Law enforcement agencies and national security agencies.
3. Courts and Tribunals (in exercise of judicial functions).
4. Crime prevention, investigations and prosecutions of offenses or for violation of laws.

The scope of application of PDP Bill (which is subject of Government Regulations) exceeds that of GDPR by virtue of an entity being subjected to the same by the nexus of processing personal data in India.



CHAPTER 2: KEY LEGAL DEFINITIONS

Sr. No.	Definition	GDPR	PRESENT INDIAN LAW	PDP Bill 2019 (As Introduced in Indian Parliament)	Observations/ Remarks
1.	Personal Data	Art. 4(1) “‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); 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;”	Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 Rule 2(i) “‘Personal information’ means any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.”	Section 3 (11) “data” includes a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by humans or by automated means; Section 3(28) “personal data” means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling;	The definition of personal data under the GDPR is tied to identification of the concerned individual, however the definition of personal data under the PDP Bill is much wider PDP Bill is subject to interpretations as may be expressly encompassed by the scope of the definition of personal data. On the other hand, the interpretations of Personal Data under the GDPR seem restricted to the identification of the concerned individual; thereby restricting the scope of most interpretations.



					In terms of anonymised data the PDP Bill empowers the Data Protection Authority to define the anonymisation processes from time to time (as per the advances in technology) and the same effectively excludes such data from its ambit.
2.	Sensitive Personal Data	<p>Article 9(1) Processing of Special Categories of Personal Data</p> <p>“Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or 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 [...]”</p>	<p>Rule 3, IT Rules 2011 Sensitive personal data or information.— Sensitive personal data or information of a person means <u>such personal information</u> which consists of information relating to;— (i) password; (ii) financial information such as Bank account or credit card or debit card or other payment instrument details ; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; (vi) Biometric</p>	<p>"sensitive personal data" means such personal data, which may reveal, may relate to, or may constitute— (i) financial data; (ii) health data; (iii) official identifier; (iv) sex life; (v) sexual orientation; (vi) biometric data; (vii) genetic data; (viii) transgender status; (ix) intersex status; (x) caste or tribe; (xi) religious or political belief or affiliation; or (xii) any other data categorised as sensitive personal data under section 15.</p> <p>Explanation.— For the purposes of this clause, the expressions,— (a) "intersex status" means the condition of a data principal who is— (i) a</p>	<p>The definitions of sensitive personal data in GDPR and the PDP Bill are similar in terms of the elements comprising such data. However, the inclusion of “financial data” within the definition of sensitive personal data in the PDP Bill significantly broadens the same.</p> <p>Additionally, the PDP Bill empowers the Government to define further types of sensitive data, unlike the GDPR.</p>



			<p>information; (vii) any detail relating to the above clauses as provided to body corporate for providing service; and (viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise: provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.</p>	<p>combination of female or male; (ii) neither wholly female nor wholly male; or (iii) neither female nor male; (b) "transgender status" means the condition of a data principal whose sense of gender does not match with the gender assigned to that data principal at birth, whether or not they have undergone sex reassignment surgery, hormone therapy, laser therapy, or any other similar medical procedure;</p>	<p>Another elemental difference is in respect of GDPR uniquely providing for rules pertaining to processing of data of criminal convictions and offenses, unlike the PDP Bill.</p>
3.	Controller	<p>Controller: The natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of the</p>	NA	<p>Data Fiduciary: Any person, including the state, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data.</p>	<p>Although the definition under the PDP Bill uses the term "fiduciary" the Bill does not specifically identify any specific obligations arising out of such a legal relationship.</p>



		processing of personal data.			
4.	Processor	A natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller	NA	Any person, including the state, a company, any juristic entity or any individual, who processes personal data on behalf of a data fiduciary	The definitions are identical in nature.
5.	Data Subject	An identified or identifiable natural person		Data principal: The natural person to whom the personal data relates.	The definitions are identical in nature.
6.	Processing	Article 4(2) ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;	NA	Article 3(41) “processing” in relation to personal data, means an operation or set of operations performed on personal data, and may include operations such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction;	The only elemental difference in the definitions concerns the usage of the word “consultation” in GDPR.



7.	Pseudonymisation/De-identification¹	'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or	NA	"de-identification" means the process by which a data fiduciary or data processor may remove, or mask identifiers from personal data, or replace them with such other fictitious name or code that is unique to an individual but does not, on its own, directly identify the data principal; Anonymisation: "anonymisation" in relation to personal data, means such irreversible process of transforming or converting personal	The PDP Bill does not define pseudonymisation, leave alone mention it. The Bill however identifies the de-identification of data which can be achieved by pseudonymisation and other such technological means and leaves it upon the Data Protection Authority to identify such methods from time to time to keep pace with the
----	---	---	----	--	--

¹ See the 2018 "A Free and Fair Digital Economy Protecting Privacy, Empowering Indians" (Justice BN Sri Krishna Committee Report), available at: https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

"A slightly different approach may be adopted with respect to de-identification, pseudonymisation and anonymisation. It must be acknowledged that there is no consensus on the meanings of these terms and commenters have noted that policy makers and on occasion, legislators have been imprecise in their use of these terms.⁹⁷ Polonetsky et al bring about a measure of clarity to these terms by analysing a spectrum of identifiability that has data that is obviously personal on one end and anonymised data on the other.⁹⁸ Pseudonymised data and de-identified data are inflection points on the spectrum nearer to anonymisation. Anonymisation requires the use of mathematical and technical methods to distort data to irreversibly ensure that identification is not possible. In this aspect, anonymisation is distinct from de-identification which involves the masking or removal of identifiers from data sets to make identification more difficult. Given the pace of technological advancement, it is desirable not to precisely define or prescribe standards which anonymisation must meet in the law. It is appropriate to leave it to the DPA to specify standards for anonymisation and data sets that meet these standards need not be governed by the law because they cease to be personal data."



		<p>identifiable natural person;</p> <p>Anonymisation: “personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.”</p>		<p>data to a form in which a data principal cannot be identified, which meets the standards of irreversibility specified by the Authority;</p>	<p>advent of technology.</p> <p>Interestingly, however the Bill defines Anonymisation, and it even specifies that except for as may be prescribed by the government in consultation with the Data Protection Authority, the anonymised data will be exempt from the scope of application of the PDP Bill.</p>
8.	Consent	<p>‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;</p>	<p>Indian Contract Act, 1872</p> <p>14. ‘Free consent’ defined.—Consent is said to be free when it is not caused by— — Consent is said to be free when it is not caused by— 1. coercion, as defined in section 15, or 2. undue influence, as defined in section 16, or 3. fraud, as defined in section 17, or</p>	<p>Section 11(2) The consent of the data principal shall not be valid, unless such consent is— (a) free, having regard to whether it complies with the standard specified under section 14 of the Indian Contract Act, 1872; (b) informed, having regard to whether the data principal has been provided with the information required under section 7; (c) specific, having regard to whether the data principal can determine the scope of consent in</p>	<p>By virtue of incorporating reference to free consent under the Indian Contract Act, 1872, the PDP Bill offers a much more stringent definition of consent as compared to the GDPR.</p>



			<p>4. misrepresentation, as defined in section 18, or</p> <p>5. mistake, subject to the provisions of sections 20, 21 and 22. Consent is said to be so caused when it would not have been given but for the existence of such coercion, undue influence, fraud, misrepresentation or mistake.</p>	<p>respect of the purpose of processing; (d) clear, having regard to whether it is indicated through an affirmative action that is meaningful in a given context; and (e) capable of being withdrawn, having regard to whether the ease of such withdrawal is comparable to the ease with which consent may be given.</p>	
--	--	--	---	---	--



CHAPTER 3: GROUNDS FOR PROCESSING OF PERSONAL DATA

GDPR

- a. **CONSENT:** Under the GDPR, consent is one of six lawful bases for processing personal data.
 - i. The GDPR defines consent as, “any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.”
 - ii. The definition of consent under the GDPR is a continuing one, which requires the controller to manage and update the same from time-to-time as the data cycle develops, giving rise to the requirement of seeking consent for the actions and purposes from the data subject at varying points. The exclusion of the opt-out mode of obtaining consent is critical to the functional aspects of GDPR.

- b. **NON-CONSENSUAL:** The other five lawful bases for processing set out in Article 6(1) GDPR are:
 - i. **Contract:** When the purpose of processing data arises from a contractual obligation on part of the controller to fulfil its contractual obligations towards the data subject.
 - ii. **Legal obligation:** When processing is mandated by virtue of legal obligation emanating from EU or member state law.
 - iii. **Vital interests:** When processing is essential for safeguarding the vital interests.
 - iv. **Public task:** When processing is necessary for performing a task in public interest or while exercising state functions by virtue of the authority as may be vested in the data controller.
 - v. **Legitimate interests:** When processing of data is necessitated for the legitimate interests of the controller/third party. The exception to the same being that the rights of the data subject interests take precedence over the legitimate interests. Processing data in legitimate interests is not a ground available to state/official authorities.

- c. **SENSITIVE DATA PROCESSING:** GDPR employs a negative permission to sensitive data processing by specifying that unless the sensitive data is processed on a lawful



basis derived from the below grounds, the same is prohibited. The lawful bases identified under Article 9, GDPR are as below:

- i. **Explicit Consent**
- ii. **Employment or social security and social protection law**
- iii. **Vital interests**
- iv. **Foundation, association or not-for-profit**
- v. **Public Data (Data available publicly)**
- vi. **Legal Claims**
- vii. **Public Interest**
- viii. **Healthcare**
- ix. **Public health (element of Public Interest)**
- x. **Archiving, Research or Statistical Purposes in Public Interest**

PRESENT INDIAN LAW

- a. Lawful basis for processing Personal Information:
 - i. Presently Indian Law does not mandate obtaining consent to collect data, or for disclosing the same to a third party.
 - ii. The law mandates there being a privacy policy and the same must specify the data that is sought to be collected and the purpose thereof.
- b. Lawful basis for processing Sensitive Personal Data:
 - i. Consent; defined as "in writing, through letter or Fax or email"; and
 - ii. Disclosing the following information at the time of sensitive data collection:
 1. The fact that the data is being collected
 2. Purpose of data collection
 3. Intended recipients of data
 4. Name and address of the collecting agency and retaining agency
- c. Notably, the present Indian Law on data protections does not apply to:
 - i. Personal information or data stored in a non-electronic format.
 - ii. Freely available information which is accessible in public domain.
 - iii. Information furnished under a law which in force at the time of collection.
- d. Purpose:
 - i. The information is restricted from being used for any purpose other than the one for which it is collected and upon exhaustion of the purpose the information ought not to be retained, unless the requirement emanates from legal obligations.
 - ii. Sensitive personal data can be collected only if necessary for the lawful purpose associated with the activities of a body corporate.



PDP BILL

- a. The PDP Bill exhibits much more stringency with regard to grounds for data processing.
- b. PDP Bill prescribes separate standards of consent for personal data and sensitive personal data
- c. Personal data can only be processed, on the following basis:
 1. Consent
 2. State Functions, with emphasis on:
 - i. the entity performing the function,
 - ii. the nature of the function,
 - iii. the extent of processing of data.
 3. Legal Compliance: Legal obligations can range from:
 - i. Complying with the requirements of outlined in law; or
 - ii. Complying with court or tribunal orders.
These grounds essentially ensure that the legal process is not hindered by the data protections laws.
 4. Prompt Action, such as emergencies arising out of health and safety conditions, where only ex-post consent can be obtained.
 5. Employment; such as for recruitment purposes or during the course of employment for necessary functions such as disbursal of remuneration, or disciplinary actions, attendance, and medical records.
 6. Reasonable Purposes; such as for prevention and detection of unlawful activities.



CHAPTER 4: KEY OBLIGATIONS OF DATA CONTROLLERS/DATA FIDUCIARIES

GDPR – OBLIGATIONS OF DATA CONTROLLERS

i. PROCESSING OBLIGATIONS

Article 5 read with Recital 39 of GDPR- Principles of Personal Data shall be:

a. LAWFULNESS, FAIRNESS, TRANSPARENCY:

- i. Information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
- ii. Where personal data is collected directly from the individual, notice must be provided at or before the time of collection.
- iii. For personal data collected indirectly notice must be provided within one month (or upon first contact with the individual, if earlier), unless providing notice would be impossible or would require disproportionate effort. The notice must necessarily provide information such as purpose and parties with whom the data will be shared, and consent must be explicitly sought for sharing the data with cross-border parties.
- iv. Controllers and processors, subject to GDPR, but not established in the European Union are required to appoint a representative in the European Union. Exception: when processing is rare and occasional and not involving large scale processing of sensitive data.

b. Collected for specified, explicit and legitimate purposes ('Purpose Limitation').

c. Adequate, relevant, limited ('Data Minimization').

d. Accurate - Data is required to be maintained in an accurate and up to date manner and it is required to be erased or rectified without any delay.

e. Storage Limitation



- i. Data ought not to be stored in a way that allows the data subject to be identified after for purpose of processing is satisfied.
- ii. EXCEPTION: Data storage for longer periods can be allowed only when processed in public interest, scientific research, historical research or statistical purposes.
- iii. Proper technical and organizational measures are essential to safeguard rights of Data Subjects.

f. Integrity and Confidentiality

- i. Ensuring security of data through manner of processing.
- ii. Unlawful processing, accidental losses, and destruction or damage of data needs to be prevented.

g. Accountability of the Controller

- i. Controller ought to comply with all of the above.

ii. DATA PROTECTION OFFICERS

1. Required for private entities only where a “core activity” of the controller or processor involves either
 - a. the regular and systematic monitoring of data subjects on a large scale; or
 - b. the large-scale processing of sensitive data.
2. The Data Protection Officer must be sufficiently independent and functionally skilled and must be able to report to the highest levels of management.
3. Data Protection Officers can be outsourced.
4. Data Protection Officers should be EU-based.

iii. RECORD OF PROCESSING: Controllers and processors are obliged to retain records of processing activities.

Article 30: All Data Controllers and Processors are responsible for the maintenance of the record of processing activities in written form including electronic form, containing information of:

1. Details of the Controller/Processor
2. Purpose of Processing
3. Description of Categories of Personal Data and of Data Subjects
4. Categories of Recipient
5. Transmission of third country / international organization, if applicable
6. Time limit for erasure of data
7. Description of general and organizational security measures.



Exception – obligation mentioned above shall not apply to the enterprises or an organization employing fewer than 250 persons unless the intended processing is likely to result in a risk to the rights and freedoms of the data subject.

Application of Law to Data Processors Under GDPR

- I. Processors and controllers, both, are obligated to maintain records of personal data and processing activities.
- II. Data Controllers are obligated to ensure that the Processor is GDPR compliant and responsibly ensures security of the data.
- III. Obligations of the controller while electing the Processor are as below:
 - a. Choose a data processor that provides “sufficient guarantees” about its security measures;
 - b. Execute a contract obliging the processor, among other obligations, to undertake to implement the same security measures that the controller would have taken for data processing;
 - c. Ensure that the processor shares all requisite information to enable the controller to ensure compliance, including convening of audits and inspections;
- IV. In case the Controller lacks the ability to ensure implementation of requisite measures the Processors can help the Controller ensure compliance with security obligations pertaining to data processing.

PRESENT INDIAN LAW

- i. **REASONABLE SECURITY:** Any “body corporate” handling sensitive personal data is obligated to implement “reasonable security practices and procedures” with respect to sensitive personal data commensurate with protecting the information assets.
- ii. **INTERNATIONAL STANDARD REQUIREMENTS:** Such requirements can be agreed upon by the parties, or in absence thereof, the Rules recommend employing International Standards or a code established by trade associations and approved by the Central Government.
- iii. **DATA BREACH:** Upon the occurrence of a data breach the body corporate may be called upon to demonstrate that the standards have been followed.



PDP BILL - OBLIGATIONS OF DATA FIDUCIARIES

I. KEY PRINCIPLES

- i. Processing Obligations **Clauses 4-10 of PDP Bill** - deals with the Principles of Data Protection, which are similar to the principles under GDPR.
 1. Personal data may not be processed by any person “except for any specific, clear and lawful purpose”.
 2. Personal data must be processed “in a fair and reasonable manner and ensure the privacy of the data principal.”
 3. Personal data must be processed “for the purpose consented to by the data principal or which is incidental to or connected with such purpose, and which the data principal would reasonably expect that such personal data shall be used for, having regard to the purpose, and in the context and circumstances in which the personal data was collected”.
 4. Personal data must be “collected only to the extent that is necessary for the purposes of processing of such personal data.”
 5. Data Fiduciaries are obligated to “take necessary steps to ensure that the personal data processed is complete, accurate, not misleading and updated, having regard to the purpose for which it is processed,” taking into account whether:
 - a. the data is likely to be used to make a decision about the data principal;
 - b. the data is likely to be disclosed; or
 - c. the data is kept in a form that distinguishes facts from opinions or personal assessments.
 6. Data fiduciaries are “responsible for complying with the provisions of this Act in respect of any processing undertaken by it or on its behalf.”
- ii. Purpose Limitation and Data Minimisation
 1. Data Fiduciaries may “not retain any personal data beyond the period necessary to satisfy the purpose for which it is processed and shall delete the personal data at the end of the processing” in the manner as may be specified under regulations, unless the data principal explicitly consents or so is required by law.
 2. Data Fiduciaries are obligated to “undertake periodic review to determine whether it is necessary to retain the personal data in its possession.”
- iii. Transparency
 1. Notices must be clear, concise and easily comprehensible to a reasonable person.



2. There is a requirement to translate notices to multiple languages where necessary and practicable.
3. Notice must be provided at the time of collection, or, if not collected directly from the individual, as soon as reasonably practicable, unless providing notice would “substantially prejudice the purpose of processing.”
4. Detailed requirements for the contents of notices, including:
 - a. Detailed disclosures of the “individuals or entities including other data fiduciaries or data processors, with whom such personal data may be shared.”
 - b. The procedure for redressing grievances (in addition to responding to rights requests).
 - c. Any rating of data trust score assigned to the data fiduciary.
 - d. Any other information specified by regulations.

II. DATA PROTECTION (SECURITY)

- a. **Encryption – Precautionary Data Protection and post-facto Legal Protection**
 - i. **General Perceptions:**
 1. The process of protecting data through encryption is an accepted method of data protection.
 2. Encryption Policies add value to compliance with data protection laws
 3. The requisite level of encryption is directly proportional to the sensitivity of the data.
 - ii. **Safeguard against Liability in the event of Data Breach**
 1. Encryption prevents data stealth from qualifying as a data breach.
 2. Encryption safeguards organizations from liabilities arising from instances of data breach
 3. Encryption pays a key in reporting compliances to Data Protection Authorities.
 - iii. **Encryption in Indian law and Jurisprudence:**
 1. It is noteworthy, that the Hon’ble Supreme Court of India in the landmark judgment of Justice K. Puttaswamy v. Union of India, while deciding upon the vires of Aadhar, the Indian social security equivalent, determined that encryption was key to determining that the Central Identities Data Repository was not a soft target.
 2. The Supreme Court of India even noted in Justice K. Puttaswamy v. Union of India that end to end encryption qualifies as a protected system under the Indian Information Technology law; and even when the data is lost or stolen it need not result in a breach provided the same remains inaccessible.



- b. Privacy by Design (PBD)**
- i. Technological designs resulting in protection of privacy include:
 - 1. Implementation of Technical and Organisational Measures, such as pseudonymisation.
 - 2. Data minimization.
 - 3. Processing only essential data.
 - 4. Period of storage.
 - 5. Restricted accessibility.
 - ii. Benefits: PBD ensures cost-effective protection for personal data and provides ensures higher quality of data for business functions.
 - iii. Developments in Indian laws:
 - 1. PDP Bill mandates PBD as part of transparency and accountability measures. Each organisation that collects data is required to prepare a Privacy by Design Policy.
 - 2. The PDP Bill also states that an organisation “may submit its privacy by design policy to [the proposed Data Protection] Authority for certification within such period and in such manner as may be specified by regulations”, after which the policy would be “published on the website of the [organisation] and the Authority”.
- c. Security Safeguards** - The PDP Bill identifies the obligation of Data Fiduciary and Data Processor to implement Security Safeguards having regard to:
- i. nature,
 - ii. scope; and
 - iii. purpose of processing personal data undertaken,
- AND
- iv. the risks associated with such processing,
and
 - v. the likelihood and severity of the harm that may result from such processing,
- The Bill further prescribes:
- a. use of methods such as de-identification and encryption
 - b. steps necessary to protect the integrity of personal data;
 - c. steps necessary to prevent misuse, unauthorised access to, modification, disclosure or destruction of personal data.



d. Periodical Review

Data Fiduciaries and Data Processors shall review security safeguards periodically.

e. Registration Obligations

1. "Significant data fiduciaries" are required to register with the Data Protection Authority in accordance with procedures that will be set out in regulations (S. 26(2)).
2. The DPA is required to notify data fiduciaries or classes of data fiduciaries as significant taking into account the following factors:
 - a. The volume and sensitivity of data processed.
 - b. Company revenue.
 - c. Risk of harm.
 - d. Use of new technologies

f. Record of Processing Activities

Significant data fiduciaries shall maintain accurate and updated records of:

1. Important operations in the data life-cycle – collection, transfers and erasure of personal data
2. Periodic review of security safeguards
3. DPIA
4. Any other aspect of processing.

The above also apply to the state.

The Record of Processing obligations under PDP Bill are more relaxed in comparison with GDPR and are likely to apply to a fewer companies that are subject PDP Bill.

Application of law to Data Processors under PDP BILL

Section 24. (1) Every data fiduciary and the data processor shall, having regard to the nature, scope and purpose of processing personal data, the risks associated with such processing, and the likelihood and severity of the harm that may result from such processing, implement necessary security safeguards, including—

- (a) use of methods such as de-identification and encryption;
- (b) steps necessary to protect the integrity of personal data; and



(c) steps necessary to prevent misuse, unauthorised access to, modification, disclosure or destruction of personal data.

(2) Every data fiduciary and data processor shall undertake a review of its security safeguards periodically in such manner as may be specified by regulations and take appropriate measures accordingly.

Section 31. (1) The data fiduciary shall not engage, appoint, use or involve a data processor to process personal data on its behalf without a contract entered into by the data fiduciary and such data processor.

(2) The data processor referred to in sub-section (1) shall not engage, appoint, use, or involve another data processor in the processing on its behalf, except with the authorisation of the data fiduciary and unless permitted in the contract referred to in sub-section (1).

(3) The data processor, and any employee of the data fiduciary or the data processor, shall only process personal data in accordance with the instructions of the data fiduciary and treat it confidential.

The PDP Bill prescribes much more specific storage limitations than GDPR:

1. Unlike GDPR, which allows data retention in a form that no longer identifies an individual, the PDP Bill mandates data deletion.
2. The PDP Bill mandates data fiduciaries to conduct periodic reviews of personal data retention.

DATA PROTECTION IMPACT ASSESSMENT

GDPR

- i. The GDPR requires controllers to conduct a Data Protection Impact Assessment for "high risk" activities, including
 1. Systematic and extensive profiling;
 2. Large scale sensitive data processing; and
 3. Large scale systematic monitoring of a publicly accessible area.
- ii. The controller must consult with the Data Protection Authority before engaging in the processing where high risks are mitigated.

iii. EXCEPTIONS:



1. Where the relevant Union law or member state law prescribes a legal basis.
2. Where sectoral/specific laws regulate specific processing operations or set of operations.
3. Data Protection Impact Assessment forms part of a general impact assessment.

PRESENT INDIAN LAW:

No such express law under the existing laws in India.

PDP BILL

DPIA provisions apply to significant data fiduciaries only, where processing involves:

- new technologies;
- large-scale profiling or use of sensitive data; or
- any other activities that carry a significant risk of harm as may be specified by regulations.

All Data Protection Impact Assessments must be submitted to the Data Protection Authority for review, and the Data Protection Authority may direct the data fiduciary to cease processing.

COMMENT: Unlike under the GDPR, the PDP Bill mandates all Data Protection Impact Assessments to be reviewed by the Data Protection Authority.

KEY POINTS OF DIFFERENCE BETWEEN GDPR AND PDP BILL:

- a. GDPR obligates all Data Collectors to undertake Data Protection Impact Assessments and maintain records of the same. The PDP Bill, however, mandates 'Significant Data Fiduciaries' only to carry out Data Protection Impact Assessments.
- b. The grounds for determining the necessity of Data Protection Impact Assessments are wider under the GDPR.
- c. Details to be provided in the Data Protection Impact Assessments are narrower under PDP Bill as compared to GDPR.



DATA PROTECTION OFFICER (DPO)

GDPR

- a. Essential Qualifications:
 1. Expert knowledge of data protection law and practices
 2. Knowledge of relevant regulations applicable within the field in which the controller or processor carry out activities
 3. Detailed knowledge of data processing processes and technologies employed by the controller or processor
- b. Tasks:
 1. Data Protection Officer essentially is an extended arm of the Data Protection Authority.
 2. Data Protection Impact Assessment: Consult with Data Protection authority in case of high risk.
 3. Point of contact for Data Subjects
- c. Challenge: Conflict of Interest:
 1. The Data Protection Officer cannot have other duties conflicting with monitoring obligations of the Data Protection Officer.
 2. Such conflicts of interest crop up if the Data Protection Officer is the head of other departments that process personal data.
 3. Why Legal? If the legal counsel may represent the company in a legal proceeding (especially with regard to legal actions against employees or customers, which may include data privacy related aspects), the legal counsel is subject to conflict of interest and, therefore, not independent.
- d. Solution: Positioning Data Protection Officer as a secondary defence mechanism
 1. The primary tasks of Impact Assessments and related compliances need to be handled through an expert who is not a designated Data Protection Officer.
 2. Conducting regular Internal Audits by the experts who can then guide the Data Protection Officer to the compliances to be performed.
- e. Point of Contact
 1. The Data Protection Officer is the point of contact for Data Subjects. However, the Data Protection Officer need not be designated with responding to or resolving concerns and complaints.



2. It is essential for experts to maintain active communication channels with Data Protection Officer and resolve and respond to Data Subjects.
3. Documenting processes through experts to demonstrate compliance and have the same accessible to the DPO will thereby give the DPO the onus to review the compliances rather than be compelled to conduct a full-fledged audit

PRESENT INDIAN LAW

The existent Indian law does not provide for Data Protection Officers.

PDP BILL

- a. The PDP Bill identifies Significant Data Fiduciaries (a subset of the Data Fiduciary, equivalent of Data Controller in GDPR) as full-fledged regulated entities required to appoint Data Protection Officers.
- b. The Bill even mandates offshore entities qualifying as Significant Data Fiduciaries to appoint Data Protection Officers based in India.



CHAPTER 5: KEY RIGHTS OF DATA SUBJECTS

Sr. No.	Right	GDPR	PRESENT INDIAN LAW	PDP BILL	OBSERVATIONS
1.	Right to Access	<p><u>Article 15 of GDPR</u></p> <p>Data Subject have the right to obtain confirmation from the controller – concerning the processing of his/her personal data.</p> <p><u>Exceptions apply where providing information, would adversely affect the rights and freedom of others, including intellectual rights.</u></p>	<p><u>Rule 4 of SPDI Rules, 2011</u></p> <p>Body corporate to provide policy for privacy and disclosure of information</p>	<p><u>Clause 17 of PDP Bill</u></p> <p>Data Principal have the right to obtain:</p> <ul style="list-style-type: none"> • confirmation about the processing of his personal data • a brief summary of processing activities • identities of data fiduciaries with whom his personal data had been shared. • category of personal data shared. <p><u>Exception (Clause 21(5)):</u> Data fiduciary</p>	<p>Broadly similar under GDPR and PDP Bill</p> <p>Burden of identifying all the data fiduciaries with whom personal data has been shared.</p> <p>The exception provided under PDP Bill – protecting other data principals may not permit <u>withholding personal data on intellectual property grounds.</u></p>



				shall not entertain any such request, which may harm the personal data of any other data principal.	
2.	Right to be forgotten	<p><u>Article 17 of GDPR</u></p> <p><u>Right to erasure ('right to be forgotten')</u></p> <ul style="list-style-type: none"> • Data subject have the right to obtain erasure of his/her personal data without undue delay and the controller shall be obliged to do so without undue delay – on the following grounds: <ul style="list-style-type: none"> ○ Personal data no longer necessary ○ Data subject withdraws consent ○ Data subject objects to the processing ○ Personal data processed unlawfully. ○ the personal data have to be 	<p><u>Rule 5(6)</u></p> <p>Body corporate or any person on its behalf permit the providers of information, as and when requested by them, to review the information they had provided and ensure that any personal information or sensitive personal data or information found to be inaccurate or deficient shall be corrected or amended as feasible:</p> <p>Provided that a body corporate shall not be responsible for the authenticity of the personal information or sensitive</p>	<p><u>Clause 18 of PBP Bill – Right to correction and erasure</u></p> <ul style="list-style-type: none"> • Data Principal have the right to – <ul style="list-style-type: none"> ○ the correction of inaccurate or misleading personal data; ○ the completion of incomplete personal data; ○ the updating of personal data that is out-of-date; ○ the erasure of personal data which 	<p>The PDP distinguishes between two separate rights – one for erasure and one for restricting the disclosure of personal data (i.e., the right to be forgotten).</p> <p>Unlike the GDPR, the PDP places responsibility for determining the scope of application of the right to be forgotten on adjudicating officers appointed by the DPA, rather than the controller.</p> <p>Since, the adjudicating officer have to consider a number of contextual factors, the interpretation of the right to be forgotten will be</p>



		<p>erased for compliance with a legal obligation in Union or Member State law to which the controller is subject</p> <ul style="list-style-type: none"> o personal data collected in relation to offer of information security services. • Where controller has made personal data public, controller is obliged to: <ul style="list-style-type: none"> o erase the personal data o shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data. 	<p>personal data or information supplied by the provider of information to such body corporate or any other person acting on behalf of such body corporate.</p> <p>Rule 5(7)</p> <p>Body corporate or any person on its behalf shall, prior to the collection of information including sensitive personal data or information, provide an option to the provider of the information to not to provide the data or information sought to be collected. The provider of information shall, at any time while availing the services or otherwise, also have an option to withdraw its consent given</p>	<p>is no longer necessary for the purpose of which it was processed.</p> <ul style="list-style-type: none"> • Data fiduciary can reject the application of data principal, giving written justification for the same. <p>Clause 20 of PDP Bill - Right to Freedom</p> <ul style="list-style-type: none"> • Data principal have the right to restrict or prevent the continuing disclosure of his personal data by a data fiduciary where such disclosure – <ul style="list-style-type: none"> o has served the purpose for which it was 	<p>narrower than then corresponding right provided under GDPR right.</p>
--	--	---	---	--	--



		<ul style="list-style-type: none"> • The above stated shall not apply – <ul style="list-style-type: none"> ○ For exercising the right of freedom of expression and information; ○ For compliance with a legal obligation ○ For reasons of public interest in area of public health ○ In the public interest, scientific or historical research or statistical purposes ○ For establishment, exercise or defense of legal claims. 	<p>earlier to the body corporate. Such withdrawal of the consent shall be sent in writing to the body corporate. In the case of provider of information not providing or later on withdrawing his consent, the body corporate shall have the option not to provide goods or services for which the said information was sought.</p>	<p>collected or is no longer necessary</p> <ul style="list-style-type: none"> ○ consent has been withdrawn ○ was made contrary to the provisions of this Act or any other law for the time being in force. <ul style="list-style-type: none"> • Above right to freedom can be enforced only by an order of an Adjudicating Officer – on an application filed by the Data Principal. 	
3.	Right to be informed	<p>Article 12 Transparent information, communication and modalities</p> <p>Article 13 Information to be provided where</p>	<p>Rule 6 of SPDI Rules</p> <p>Disclosure of information</p>	<p>Clause 7 read with Clause 11(b)</p> <p>Requirement of notice for collection or processing of personal data.</p>	<p>There is significant overlap between the transparency requirements of both frameworks.</p> <p>However, the PDPB does include additional</p>



		<p>personal data are collected from the data subject</p> <p>Article 14 Information to be provided where personal data are collected from the data subject</p>		<p>disclosure requirements that may not already be included in a privacy notice drafted for GDPR, such as details on the procedure for handling individual requests and grievances, and, if applicable, a data trust score assigned by a data auditor pursuant to the PDPB's audit provisions (discussed below).</p> <p>In addition, requirements to provide the contact details of the data protection officer, and to provide notice in multiple languages, may require the localization of global privacy notices.</p> <p>Finally, the requirements for disclosing recipients under the PDPB may require more specific disclosures of data processors than is required under the GDPR.</p>
--	--	---	--	---



CHAPTER 6: CROSS-BORDER DATA TRANSFERS AND DATA LOCALIZATION

GDPR

Localization is not required unless international data transfer requirements are not met.

PRESENT INDIAN LAW

Rule 7 of IT Rules 2011

Transfer of information

"A body corporate or any person on its behalf may transfer sensitive personal data or information including any information, to any other body corporate or a person in India, or located in any other country, that ensures the same level of data protection that is adhered to by the body corporate as provided for under these Rules.

The transfer may be allowed only if it is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and provider of information or where such person has consented to data transfer.

PDP BILL

CHAPTER VII RESTRICTION ON TRANSFER OF PERSONAL DATA OUTSIDE INDIA

Section 33. Prohibition of processing of sensitive personal data and critical personal data outside India.

(1) Subject to the conditions in sub-section (1) of section 34, the sensitive personal data may be transferred outside India, but such sensitive personal data shall continue to be stored in India.

(2) The critical personal data shall only be processed in India.

Explanation.—For the purposes of sub-section (2), the expression "critical personal data" means such personal data as may be notified by the Central Government to be the critical personal data

Section 34. Conditions for transfer of sensitive personal data and critical personal data.



(1) The sensitive personal data may only be transferred outside India for the purpose of processing, when explicit consent is given by the data principal for such transfer, and where—

(a) the transfer is made pursuant to a contract or intra-group scheme approved by the Authority: Provided that such contract or intra-group scheme shall not be approved, unless it makes the provisions for—

(i) effective protection of the rights of the data principal under this Act, including in relation to further transfer to any other person; and

(ii) liability of the data fiduciary for harm caused due to non-compliance of the provisions of such contract or intra-group scheme by such transfer; or

(b) the Central Government, after consultation with the Authority, has allowed the transfer to a country or, such entity or class of entity in a country or, an international organisation on the basis of its finding that—

(i) such sensitive personal data shall be subject to an adequate level of protection, having regard to the applicable laws and international agreements; and

(ii) such transfer shall not prejudicially affect the enforcement of relevant laws by authorities with appropriate jurisdiction: Provided that any finding under this clause shall be reviewed periodically in such manner as may be prescribed;

(c) the Authority has allowed transfer of any sensitive personal data or class of sensitive personal data necessary for any specific purpose.

(2) Notwithstanding anything contained in sub-section (2) of section 33, any critical personal data may be transferred outside India, only where such transfer is—

(a) to a person or entity engaged in the provision of health services or emergency services where such transfer is necessary for prompt action under section 12; or

(b) to a country or, any entity or class of entity in a country or, to an international organisation, where the Central Government has deemed such transfer to be permissible under clause (b) of sub-section (1) and where such transfer in the opinion of the Central Government does not prejudicially affect the security and strategic interest of the State.

(3) Any transfer under clause (a) of sub-section (2) shall be notified to the Authority within such period as may be specified by regulations.

RECOMMENDATIONS OF JUSTICE BN SRIKRISHNA COMMITTEE:

a. Cross border data transfers of personal data, other than critical personal data, will be through model contract clauses containing key obligations with the transferor



- being liable for harms caused to the principal due to any violations committed by the transferee.
- b. Intra-group schemes will be applicable for cross-border transfers within group entities.
 - c. The Central Government may have the option to green-light transfers to certain jurisdictions in consultation with the DPA.
 - d. Personal data determined to be critical will be subject to the requirement to process only in India (there will be a prohibition against cross border transfer for such data). The Central Government should determine categories of sensitive personal data which are critical to the nation having regard to strategic interests and enforcement.
 - e. Personal data relating to health will however permitted to be transferred for reasons of prompt action or emergency. Other such personal data may additionally be transferred on the basis of Central Government approval.
 - f. Other types of personal data (non-critical) will be subject to the requirement to store at least one serving copy in India.

STANDARD CONTRACTUAL CLAUSES AND INVALIDATION OF EU-U.S. PRIVACY SHIELD.

Case No. C-311/18, *Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems*²

1. Validity of Standard Contractual Clauses

- a. In an investigation led by the Irish Data Processing Commission it was provisionally found that the processing of personal data of citizens of the European Union by the U.S. authorities was not in conformity with Article 7 – “Respect for private and family life” and Article 8 – “Protection of personal data” of the Charter of Fundamental Rights of the European Union.
- b. The Irish Data Processing Commission also preliminarily opined that citizens of the European Union were not provided with legal remedies in conformity with Article 47 – “Right to an effective remedy and to a fair trial” of the Charter of Fundamental Rights of the European Union.

In view of the above the Court of Justice of the European Union ruled that:

² Judgment of the Court of Justice of the European Union (Grand Chamber), 16th July 2020, Case C- 311/18, titled ‘*Data Protection Commissioner v. Facebook Ireland Ltd. and Maximillian Schrems*’. Available at: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=9793916>



- i. If the European Commission has made an adequacy decision, a Data Protection Authority cannot conclude that a jurisdiction does not offer adequate protection.
- ii. For all the other third countries where the European Commission has not made an adequacy decision a Data Protection Authority may decide that the Standard Contractual Clauses cannot be complied with and that requirements of the GDPR for the protection of the data of the Data Principal in European Union cannot be ensured by other means.

RULING: The Court of Justice of the European Union ruled that where the adequacy decision is not in place and the Data Protection Authority determines that the third-country cannot ensure adherence with GDPR and EU Law, the Data Protection Authority must suspend or prohibit the transfer, unless, the suspension has been given effect by the Data Controller or the Data Processor.

2. Invalidity of EU-US Privacy Shield

- a. The European Commission had acknowledged that the Privacy Shield Framework needs to be complied with to the *"extent necessary to meet the national security, public interest, or law enforcement requirements."*
- b. The limitations within the Privacy Shield Framework on data processing on the grounds of national security, public interest or law enforcement requirements were not in consonance with the GDPR and could allow processing of data in contravention with the GDPR and EU Law on the basis of the domestic law of the US in addition to grounds of national security and public interest.

RULING: The Court of Justice of the European Union ruled that Article 47 of the Charter were not honoured as Data Subjects did not have access to courts against US authorities and that the Privacy Shield Ombudsperson "cannot remedy the deficiencies" concerning judicial protection of Data Subjects, specifically on grounds of lack of Independence of the Privacy Shield Ombudsperson from the US Executive as the same directly reported to the US Secretary of State. Moreover, the Privacy Shield Framework did not ensure that the Ombudsperson could issue decision binding on US intelligence services.

.....




Hammurabi & Solomon Partners was founded in the early 2001 and is ranked amongst the top #15 law firms in India. Our journey has been marked by stellar growth and recognition over the past 2 decades with over 16 partners handpicked from the top of their fields. Paving our way into the Indian legal landscape we believe in providing complete client satisfaction with a result driven approach.

We have always aimed at being the change-maker for a newer India and the world around us. With our portfolio of services - law, public policy, regulation and justice converge to enable solutions to our client needs within the legal framework to operate in India with ease and predictability.

Our main aim is to provide world-class legal services with a unique client-centric approach. We aim at providing the utmost quality and result-oriented solutions with our out of the box thinking and teamwork. We focus on being very approachable and highly reliable legal advice with a practical and relevant approach, we tailor solutions with each client's needs.

Our firm implements a holistic approach towards client satisfaction by offering higher level of services, in-time solutions and exercising greater insights to understand the clients' sectors.

H&S Partners offices are located in New Delhi (HQ) // Mumbai // Bengaluru // Gurugram // Patna // Ranchi



herfurth.partner

Videoconferences and Data Protection


Antonia Herfurth
Attorney at Law in Munich and Hanover
22 July 2020

herfurth.partner

Introduction

- Increase of videoconferences
- Requirements for videoconferences:
 - Technical possibilities, e.g. for screen presentations, conferences with many participants etc.
 - Smooth running
 - Videoconference tools have to be in accordance with GDPR
- Every videoconference tool processes personal data of users

herfurth.partner


Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

R	T	Dienst	URL	Version der Dokumente	Rechtliche Mängel bzgl. Auftragsverarbeitung	Ort der Verarbeitung nach Vertrag auf EU/EWR beschränkt
●	●	Blizz	https://www.blizz.com/de/	Blizz Auftragsverarbeitungsvertrag (https://www.blizz.com/de/auftragsverarbeitungsvertrag/), Endnutzer-Lizenzvereinbarung – Blizz (https://www.blizz.com/de/eula/), jeweils ohne Datum, letzter Abruf 28.5.2020 [Deutsch]	ja, siehe Anmerkung Anbieter hat Änderungen angekündigt	nein
●	●	Cisco WebEx	https://www.webex.com/de	Universelle Cloud-Vereinbarung Version 9.3 vom 15.4.2020 [Deutsch]; Master Data Protection Agreement, December 2019 [Englisch]; Digital River Ireland Ltd. Allgemeine Geschäftsbedingungen und Verbraucherinformationen Deutschland vom 24.7.2017 [Deutsch]	ja, siehe Anmerkung	nein
●	●	Cisco WebEx über Telekom	https://konferenzen.telekom.de/produkte-und-preise/telefon-und-web/cisco-webex/	Auftragsverarbeitungsvertrag zum Vertrag über Cisco Webex (Webex Standard) Version 1.0 vom 15.01.2020 [Deutsch], Anhang AVV zum Vertrag über Telekommunikationsleistungen Version 2.2 vom 16.04.2020 [Deutsch]	ja, siehe Anmerkung Anbieter hat Änderungen angekündigt	nein, siehe Anmerkung
●	●	frei verfügbare Jitsi-Angebote			in der Regel ja, da kein Auftragsverarbeitungsvertrag	

Source: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Hinweise_Berliner_Verantwortliche_zu_Anbietern_Videokonferenz-Dienste.pdf

herfurth.partner

●	●	Google Meet (als Teil der G Suite unter Geltung des G Suite (Online) Agreement und des Data Processing Amendment to G Suite and/or Complimentary Product Agreement)	https://apps.google.com/meet/	G Suite (Online) Agreement Version 8 April 2020; Data Processing Amendment to G Suite and/or Complimentary Product Agreement, Version 2.2 [Englisch]	ja, siehe Anmerkung	nein
●	●	Google Meet (kostenlos)	https://apps.google.com/meet/	Google-Nutzungsbedingungen, wirksam ab dem 31. März 2020, Google-Datenschutzerklärung, wirksam ab dem 31. März 2020 [Deutsch]	ja, kein Auftragsverarbeitungsvertrag	nein
●	●	GoToMeeting	https://www.getomeeting.com/de-de	Datenverarbeitungsnachtrag vom 26. Dezember 2019 [Deutsch]	ja, siehe Anmerkung	nein
●	●	Microsoft Teams (als Teil von Microsoft 365 unter Gültigkeit der Online Service Terms)	https://www.microsoft.com/de-de/microsoft-365/microsoft-teams/group-chat-software	Anhang zu den Datenschutzbestimmungen für Microsoft-Onlinedienste Januar 2020 [Deutsch] – Dateiversionen (laut Metadaten) vom 3.1.2020 und 9.6.2020 (Version ist im Dokument selbst nicht ersichtlich)	ja, siehe Anmerkung	nein
●	●	Microsoft Teams (kostenlose Version)	https://www.microsoft.com/de-de/microsoft-365/microsoft-teams/group-chat-software	Microsoft-Servicevertrag gültig ab 30. August 2019, Datenschutzerklärung von Microsoft April 2020 [Deutsch]	ja, kein Auftragsverarbeitungsvertrag	nein
●	●	NETWAYS Web Services Jitsi	https://mws.netways.de/de/apps/jitsi/	AVV v1.7 [Deutsch]	keine gefunden	ja

Source: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Hinweise_Berliner_Verantwortliche_zu_Anbietern_Videokonferenz-Dienste.pdf

herfurth.partner						
		sichere-videokonferenz.de	https://sichere-videokonferenz.de/	Vertrag über die Auftragsverarbeitung personenbezogener Daten nach EU Datenschutz-Grundverordnung Stand 06/2020 [Deutsch]	keine gefunden	ja
		Skype	https://www.skype.com/de/	Microsoft-Servicevertrag gültig ab 30. August 2019. Datenschutzerklärung von Microsoft April 2020 [Deutsch]	ja, kein Auftragsverarbeitungsvertrag	nein
		Skype for Business Online (zustehend, unter Gültigkeit der Online Service Terms)		Anhang zu den Datenschutzbestimmungen für Microsoft-Onlinedienste Januar 2020 [Deutsch] – Dateiversionen (laut Metadaten) vom 3.1.2020 und 9.6.2020 (Version ist im Dokument selbst nicht ersichtlich)	ja, siehe Anmerkung zu Microsoft Teams (als Teil von Microsoft 365 unter Gültigkeit der Online Service Terms)	nein
		TixeoCloud	https://www.tixeo.com	Vertrag zur Auftragsverarbeitung Version 20200608 [Deutsch]	keine gefunden	ja
		Werk21 BigBlueButton	https://www.werk21.de/produkte/co_workingbigbluebutton/index.html	Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DSGVO, Version 1.2.1., 06/2020 [Deutsch]	keine gefunden	ja
		Wire	https://wire.com/de/	Datenverarbeitungszusatz Juni 2020 [Deutsch]	keine gefunden	nein, auch Schweiz
		Zoom	https://zoom.us	Global Data Processing Addendum December 2019 [Englisch]	ja, siehe Anmerkung	nein

Source: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BinBDI-Hinweise_Berliner_Verantwortliche_zu_Anbietern_Videokonferenz-Dienste.pdf

herfurth.partner	
<h3 style="color: #4F81BD;">Videoconference providers compliant with GDPR</h3> <ol style="list-style-type: none"> 1. Data processing agreement <ul style="list-style-type: none"> – Clear wording and no doubt about compliance with GDPR requirements – Must meet the requirements of Art. 28 GDPR: <ul style="list-style-type: none"> processors processes data only on instructions, deletes or returns data after end of services, makes information available necessary to demonstrate compliance with GDPR, e.g. 2. Provider based in the EU/EEA 	



Videoconference providers compliant with GDPR

1. Data processing agreement
2. Third country *but*
comparable level of data protection recognised by adequacy decisions of EU Commission:
 - Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay
 - Adequacy talks with South Korea
 - Notable: no longer US since European Court of Justice overturned Privacy Shield last week

Videoconference providers compliant with GDPR



1. Data processing agreement
2. Third country *but*
use of appropriate guarantees, most popular Standard Contractual Clauses approved by EU Commission:
<https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32010D0087>

herfurth.partner

Examples: Zoom  vs Wire 

- Zoom
 - Legal defecits regarding processing activities:
 1. Defecits concerning data processing agreement
 2. Impermissible limitation of the obligation to delete data
 3. Impermissible export of data
 4. Doubts on the reliability of the provider
 - Place of processing not limited to EU/EEA

herfurth.partner

Examples: Zoom  vs Wire 

- Wire
 - No legal defecits regarding processing activities
 - Place of processing limited to EU/EEA and Switzerland
 - Less technical possibilities, e.g. no moderation of videoconference, every user has control over his camera and microphone


herfurth.partner

Checklist

1. Conference call or e-mails instead of videoconference
2. Provide own service in source code with publicly available (open source) or commercially available software
3. Provider with headquarters and processing location, in particular server location, within the EU/EEA
4. Provider with headquarters and processing location in third country **but** with an equivalent level of data protection **or** use of appropriate guarantees (e.g. Standard Contractual Clauses approved by the EU Commission)

herfurth.partner

Thank you



herfurth.partner

COPYRIGHT BY
HERFURTH & PARTNER
RECHTSANWALTSGESELLSCHAFT MBH
HANNOVER · GÖTTINGEN · BRÜSSEL

MEMBER OF
ALLIURIS GROUP
ALLIANCE OF INTERNATIONAL BUSINESS LAWYERS

BRUSSELS · PARIS · LONDON · AMSTERDAM
AMERSFOORT · LYON · MADRID · BARCELONA · LISBON
MILAN · DUBLIN · COPENHAGEN · HANOVER · ZUG · VIENNA
MOSCOW · MINSK · BUCHAREST · ATHENS · NICOSIA
ISTANBUL
BEIJING · SHANGHAI · NEW DELHI
NEW YORK · SAO PAULO · RIO DE JANEIRO · BRASILIA

LUISENSTR. 5
30159 HANNOVER
FON 0511 307 56-0
FAX 0511 307 56-10

info@herfurth.de
www.herfurth.de

herfurth.partner

COPYRIGHT BY
Herfurth & Partner
RECHTSANWALTS
GESELLSCHAFT MBH

MEMBER OF
ALLIURIS
ALLIANCE OF
INTERNATIONAL
BUSINESS
LAWYERS

HANNOVER
GÖTTINGEN
BRÜSSEL

BRUSSELS
LONDON
PARIS
AMSTERDAM
AMERSFOORT
LYON
MADRID
BARCELONA
LISBON
MILAN
DUBLIN
COPENHAGEN
HANOVER
GÖTTINGEN
ZUG
VIENNA
SALZBURG

MOSCOW
MINSK
ATHENS
ISTANBUL

BEIJING
SHANGHAI
GUANGZHOU
WUHU
NEW DELHI
MUMBAI

NEW YORK
CHICAGO
SAN FRANCISCO
LOS ANGELES
ORANGE COUNTY

SAO PAULO
RIO DE JANEIRO
BRASILIA

LUISENSTR. 5
30159 HANNOVER
FON 0511 307 56-0
FAX 0511 307 56-10

info@herfurth.de
www.herfurth.de

Question & Answers

Data Protection

- 1. Which kind of technical / practical problems about data protection exist in your country?**

Maria Inês Reis (Portugal):

I think since data protection exists, people are aware of most internet problems and some telecommunications companies are reducing some publicity phone calls because people now know their rights. It has been in discussion the right to be forgotten on the internet because of all google and facebook problems (Cambridge analytica).

Iv Fangyuan (China):

Many Apps steal private data and this situation is difficult to supervise.

Qiu Shuang (China):

Lack of special legislation.

Qiyi Zhang (China):

Now, data protection has become the intangible wealth and assets of enterprises or individuals. Maybe these problems are not paid enough attention to by enterprises or individuals, but it doesn't matter, we hand them over to website hosting, professional website hosting experts, website updating, Internet brand promotion, we-media operation, website security and so on. So what are the problems with enterprise data protection today? 1. Insufficient attention; 2. The limit of the budget; 3. The lack of relevant professional or information.

Eduardo Barrera (Mexico):

Data protection is a topic reserved in practice just to big companies and for specific areas of the government and of course for taxes. Normally a small business has a lack of knowledge on this topic when it has to do with deleting this data or being able to give an answer where this data was at the end stored.

Friederike Ammann (Germany):

- Encryption
- Digital footprint
- Too simple password (too easy to guess)
-

Jannis Ulrich (Germany):

The weak choose of good alternative. If you want to communicate with others you have to use programs from Google and Facebook. Companies don't know how to execute the DSGVO. The "good will" to protect data, because people think data protection is not important.

Arthur Horsfall (UK):

Balancing the need to obtain people's information for legitimate needs with the unessential obtaining and storing of data under the GDPR.

Understanding the difference between processors and controllers and how this impacts on how personal data can be used and stored.

Coral Yu (UK):

In the context of M&A transactions, there is often a tension between what lawyers are obliged to advise clients in terms of the technical compliance with data protection legislation and the overriding objective to complete a transaction quickly and in a cost-efficient manner. We are often asked by clients to weigh up the practical implications of a technical breach of data protection legislations.

Gary Whitehead (UK):

Not understanding what constitutes sensitive data at a basic level

Philippa Kwok (UK):

- Specific procedures laid down by legislation that must be adhered to
- Data security
- Effective data encryption
- Erasure of data upon request

Julia Krautter and Patrícia Perinazzo (Brazil):

The companies are still in the adaptation period since the data protection law is not in place yet. Thus, the problems we face at the moment are those related to the behavioural change.

Alitzel Sánchez Alonso (Mexico):

Not all the people respect data and some of the people who have personal data do not use them in a correct way.

Luis Roberto Moreno Tinoco (Mexico):

Mexican law provides for a complete regime regarding data protection, including special rules in our constitution, laws and its regulations. These provisions are binding for Mexican entities that receive personal data from individuals, which are obliged to treat personal data with strict confidentiality.

However, practical problems may arise when the entities who receive the data are not deemed as Mexican for legal purposes, since their domestic laws may differ with Mexican regulations.

Mari Yoli Wulf Sánchez (Mexico):

All, most companies do not take care of personal information.

Miguel Ángel Aspe de la Rosa (Mexico):

Social engineering poses a great threat and jeopardizes almost every industry. Big firms often experience cyber attacks through phishing emails or identity-theft software.

Nadieżda Vázquez Careaga (Mexico):

In Mexico there is just a few regulation about this subject, and I think we should impose punishments that motivate not to perform criminal acts.

Paulina Saldaña Fuentes (Mexico):

Lately government internet sites have been hacked a lot. Mexican system has a Data Protection Law that distinguishes different types of confidential information, depending on the breach, the sanctions can go from paying damages to a felony.

Ricardo Heredia (Mexico):

The legal regulation is not very clear and precise in certain cases; such as when it will not apply with international companies. For example a European company with an international web page, which has a particular Mexican site, where citizens can register. It is not very clear sometimes if it should comply also with Mexican regulation, or is enough with international law.

Fergan Tuğberk Işman (Turkey):

Data protector has many responsibilities within the scope of data protection regulations. Some of those responsibilities are having an informative text about the data they are going to process, taking explicit consent from the users on processing of sensitive information and keeping obligatory log records in order to prevent cyber crimes.

Those responsibilities bring some problems with them. Some practical problems are not having a proper informative text. Without an informative text, users cannot see which personal data about them is getting processed and for what purpose it is going to be processed.

Another and maybe the most important problem is not taking an explicit consent. Explicit consent is absolutely necessary on sensitive data processing and without a proper consent; the data protector may face serious consequences.

Technical problems mainly arise from software such as log recording programs and data loss protection software. If that software were not prepared or installed properly they may cause serious legal problems to the data protector.

2. Which modules shall be used for the establishment of a data protection management system?

Qiyi Zhang (China):

Starting from the function of database management system, the data is protected by modules such as data schema definition, physical construction of data access, data manipulation, data integrity, security definition and inspection, concurrent control and fault recovery of database, and data service.

Eduardo Barrera (Mexico):

Document store, Vulnerabilities, Tracking, Data Protection Policy, among others.

Arthur Horsfall (UK):

- Records of data processing activities;
- GDPR compliance assessment gap analyses;
- Compliance reports;
- Customisation of data protection impact assessment method;
- Analysis of data protection threats and vulnerabilities;
- Analysis of data protection impacts;
- Data protection risk reports; and
- Continual treatment of compliance findings and data protection risks.

Coral Yu (UK):

Assuming GDPR applies to the business, then the business should carry out the following to establish a data protection management system:

- Designate a person or group to lead the effort within the business.
- Educate the businesses' senior decision makers about the GDPR's risk-based compliance approach; and the potential effects of non-compliance.
- Empower the governance program to establish or change systems and processes within the business to demonstrate compliance with the GDPR's requirements and provide accountability.
- Build support for the program across the organization.

- Meet with key stakeholders who collect and use personal data for the business to educate them about the GDPR's requirements; and learn more about how those requirements might affect their core business needs.
- Conduct a GDPR compliance assessment.
- Establish a reasonable GDPR implementation and compliance budget based on the business's size, locations, and means; and the processing activity's complexity and sensitivity.

Philippa Kwok (UK):

- Data collection
- Data storage
- Data destruction
- Application of security processes
- Case management to handle requests and complaints from data subjects
- Incident management
- Identification of data protection risks and fault in database system

Julia Krautter and Patrícia Perinazzo (Brazil):

Identify records of data and of data processing activities; data protection assessment and gap analyses; analysis of data protection threats and vulnerabilities; map data protection policies to operational practices; improvement of privacy policies; review and manage processor contracts; employee training; appointing a DPO; manage consent withdrawal and/or refresh.

Alitzel Sánchez Alonso (Mexico):

Privacy notice is used as a system to protect personal data.

Luis Roberto Moreno Tinoco (Mexico):

I am not aware of any training module regarding data protection that is currently being implemented in Mexico. It is my understanding that this is one of the requirements set forth by European legislation regarding this matter, but it has not yet been adopted by Mexican law.

However, it is important to note that I do not consider myself an expert in data protection law, since my practice area is focused in tax law.

Mari Yoli Wulf Sánchez (Mexico):

Contracts.

Miguel Ángel Aspe de la Rosa (Mexico):

In my perspective a diligent firewall system which includes not only a virtual but a human firewall protection is clearly a way to reduce the impact of cyber attacks related to identity-theft issues. The integrity of information is a serious problem in Mexico.

Paulina Saldaña Fuentes (Mexico):

First data site's encryption so the information provided by such is fully protected.
Second I would suggest an intercompany platform for sharing documents in a secure way.

Ricardo Heredia (Mexico):

Proper software protection mechanisms.

Fergan Tuğberk İşman (Turkey):

The most important modules are data loss protection software and log recording programs. Log recording programs help detecting ill intended users and prevent them from doing any criminal activity. Data loss protection software neglects the bad outcome of a cyber attack that targets an online platforms archive. With the help of this software any lost data from the cyber attack can be retrieved.

Data protection management is not limited to those systems. Operators can create systems that block any transfer of processed personal data without other security checks. Those systems automatically block any personal data and allow the data protector to check if this transfer is necessary to prevent any personal information infringement.

3. Which advice would you give to your client for cross border relations?

Maria Inês Reis (Portugal):

To read every single line of the whole contract and be careful about what they consent the other part.

Iv Fangyuan (China):

Investigate the trading party, pay by letter of credit.

Qiu Shuang (China):

Focus on communication, information and cultural differences.

Qiyi Zhang (China):

Set up archives, agree confidentiality agreement in the agreement, grasp the legal provisions of the cross-border other country involved in this transaction, etc.

Eduardo Barrera (Mexico):

To be informed about EU Law in this field and thinking into hiring a Data Protection Officer.

Jannis Ulrich (Germany):

- Ask how the cross-border company execute data protection.

- Don't send private Data with insecure communicators like "WhatsApp"
- Try to reduce the generation of personal data (example: no-third-Party cookies on the homepage)

Arthur Horsfall (UK):

Understand both the data protection laws in both countries as if there are data processing facilities in both countries, they will be subject to the regulations of both legislation.

Also, for EU and UK countries to try to limit the impact that Brexit may have on their data transfers, adopt Standard Contractual Clauses (**SCCs**) in their agreements. These are provisions which have been approved by the EU as a legal basis to safeguard the transfer of personal data to third countries. Whilst not a total safeguard it is something that can be done now in preparation.

Coral Yu (UK):

As a first step, it is necessary to identify those processes that involve non-EU data transfers, as sanctions of breach of data protection rules in such cases can be quite severe (up to € 20 million or 4% of the annual global turnover). Thereafter it is essential to adopt the right transfer mechanism for such transfers - in the absence of an adequacy decision, the client would need to consider and provide for appropriate safeguards (Standard Contractual Clauses or Binding Corporate Rules). The client should also consider whether certification schemes and codes of conduct can be possible transfer mechanisms. Lastly, derogations may be possible under exceptional circumstances, only when appropriate safeguards are put in place.

Gary Whitehead (UK):

Fully get to grips with the intricacies of the laws of the country where data will be stored – as an example, California Privacy Act quite different to GDPR

Philippa Kwok (UK):

- Data protection regimes differ across jurisdictions (although there are common elements, emphasis may be placed on different elements) – data processors / controllers may subject to different forms of obligations.
- There may be restrictions on the transfer of personal data to countries whose data protection regime lack robust / appropriate safeguards of personal information.

Julia Krautter and Patrícia Perinazzo (Brazil):

Attention to the level of security of the country which data origin provides, if it's an adequate degree of protection of personal data as provided for in the Brazilian Law.

Alitzel Sánchez Alonso (Mexico):

Before executing any document or agreement, review if there is some privacy notice that answers to the following questions:

1. which information are they requesting;
2. what is the purpose of requesting such information;
3. who will have access to review his/her personal data and for how long;
4. who would be responsible of the protection of the data; and
5. which actions are taken to protect the personal data.

Luis Roberto Moreno Tinoco (Mexico):

It is important to determine the scopes of the domestic legislation of the foreign entities that are going to be involved in the transaction, since their rules may differ from the ones established by Mexican law, which may lead to practical problems if there is not an international treaty that rules this matter.

Mari Yoli Wulf Sánchez (Mexico):

Establish good contact and be very clear about the laws of your country and the other country, and establish a clear contractual relationship.

Miguel Ángel Aspe de la Rosa (Mexico):

Whether my client is planning to make business in Mexico, I would suggest not to take data protection as a minor problem. This would include contracting an independent firewall system and to share information only through encrypted channels, which implies avoid to share information in open or prone-hacking sites such as Google Drive or Dropbox.

Nadiezhdá Vázquez Careaga (Mexico):

Have an advisor who knows the laws of the places involved.

Paulina Saldaña Fuentes (Mexico):

To ensure that the client he is treating with in a cross border business is ethical and compliant by requesting few references.

Ricardo Heredia (Mexico):

It all depends if you have a Mexican incorporated legal entity, and if such entity obtains and addresses personal data, or if it is another international subsidiary.

Fergan Tuğberk İşman (Turkey):

Personal Data Protection Law article 9 is an imperative provision. Personal data shall not be transferred without explicit consent of the data subject. But the Binding Corporate Rules (BCR) created by European Union Article 29, Working Party allows international organizations to transfer personal data in compliance with EU data protection law.

In order to benefit from BCR, the rules created by the companies are required to be approved by the data protection authority in each country. By means of the approval of each country's data protection authority, personal data may be shared between the companies.

Materials | Compact

Data Protection in Foreign Business

*Marc-André Delp, M.L.E., Rechtsanwalt in Hanover,
Qualified Lawyer for International Commercial Law
December 2018*

The introduction of the General Data Protection Regulation (GDPR) has kept companies very busy in recent months. Internal implementation processes have been set in motion, but there are still uncertainties in dealing with the GDPR

For internationally active companies, there is another aspect of the GDPR that needs to be observed: The transfer of personal data beyond the borders of the EU. This is referred to as data transfer to third countries and is regulated in Articles 44 to 49 of the GDPR. The transfer refers to the disclosure of personal data to a recipient in a third country; the type of disclosure or the disclosure to the third party is irrelevant. The aim is to ensure that the level of data protection under the GDPR is maintained even when data is transferred to third countries.

Two-stage check

This data transfer initially requires that the fundamental and generally known requirements of the GDPR are complied with. If this is not the case, there is no need for further examination regarding cross-border transfer of personal data. Only in a second step the requirements for data transfer to third countries are to be examined.

Data transfer to third countries

For data transfers to third countries, the GDPR provides for three rules:

- determination of the adequacy of the level of data protection in the third country by the EU Commission (Article 45),
- the existence of appropriate guarantees (Article 46), and
- exceptions for certain cases (Article 49).

Decision on adequacy

The adequacy of the level of data protection in the third country can only be determined by the EU Commission, not by the individual member states. If third countries offer an adequate level of data protection comparable to the level of the GDPR, the EU Commission determines this by decision. Personal data may then be transferred to these countries without further approval. The adequacy decisions are reviewed by the Commission at least every four years. Adequacy decisions that were adopted before the GDPR was applicable will initially remain valid until the next review. Adequacy decisions exist for Andorra, Argentina, Canada (Commercial Organisation), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, USA (limited to the Privacy Shield). Since 5 September 2018, it has been decided that a decision on adequacy will also be made for Japan. Additionally, talks are underway with South Korea; dialogues with India, Brazil and Paraguay are planned.

The advantages of the adequacy decisions are the high level of legal certainty and the suitability for mass use. The disadvantage is that there is no permanent guarantee of transmission since the EU Commission reviews the decision at least every four years.

Appropriate guarantees

Without a decision on adequacy, personal data can only be transferred on the basis of appropriate guarantees provided by the controller or processor. The guarantees must ensure an appropriate level of protection. These include:

- binding internal data protection regulations (binding corporate rules),
- standard data protection clauses of the EU Commission or a supervisory authority,
- approved codes of conduct and approved certification mechanism, and
- individually negotiated contractual clauses.

The guarantees must provide data subjects with enforceable rights and remedies.

Binding Corporate Rules (BCR) are rules that company groups or groups of companies can impose on themselves when carrying out a common economic activity and which then apply to all the companies involved. The appropriate BCR must be approved by the competent national supervisory authority. Once approved, the BCR may be used as a basis for the transfer of personal data without the need for further approval in individual cases. The prerequisites for approval are a legally binding nature for the companies involved, enforceable rights for the persons concerned and compliance with the minimum requirements under Article 47 paragraph 2 GDPR. BCR are suitable for groups of companies consisting of a controlling company and companies dependent on it. The advantage is the high level of legal certainty and transparency as well as suitability for mass use. In addition, the BCR are also tailored to companies/company groups and their practices. Furthermore, a uniform internal level of data protection (also externally) is

guaranteed. A disadvantage is the complex approval procedure and the associated high time expenditure.

Standard contract clauses are defined by national supervisory authorities and subsequently approved by the EU Commission or directly enacted by the EU Commission. Thereafter, the standard contractual clauses can be used without further approval. Here too, no further approval is required for data transfer. This only applies, however, if the clauses are not changed. If clauses are added or existing clauses are changed and contradict the approved regulations, the approval is no longer given. The advantage over the BCR is that the clauses are already fully developed and only need to be adopted. In addition, the standard contract clauses can be used not only internally within the company group, but also in relation to third parties. The EU Commission has already issued three packages of clauses: EU Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses, EU Commission Decision 2004/915/EC of 15 June 2001 on the introduction of alternative standard contractual clauses for the transfer of data from an EU controller to a controller in a third country and EU Commission Decision 2010/087/EU of 5 February 2010 on standard contractual clauses for transfers to processors in third countries. These clauses contain formulations that companies can use. The advantage of the standard contract clauses is that they can be used at short notice, as the pre-formulated clauses only have to be adopted. In addition, no separate approvals are required for individual data transfers. The disadvantage is that the standard contract clauses cannot be adapted to the concrete needs of the companies/company groups. Company groups in third countries are subject to EU law through the standard contractual clauses. It is also possible that the EU Commission will subsequently amend the standard contractual clauses and that the companies will have to react immediately and adapt the clauses they use.

Approved codes of conduct are industry-, sector- or association-specific guidelines. They therefore apply to certain industry sectors or certain organisations that can create their own rules of conduct for their industry for the processing of personal data. The approved codes of conduct must contain legally binding and enforceable obligations of the controller or processor. The rules of conduct are published by the national supervisory authority and the EU Data Protection Committee. Another advantage of the approved code of conduct is that no separate approval is required for the transfer of personal data. Disadvantage is the necessary willingness of the responsible association to cooperate as well as a considerable effort.

Additional guarantees can be achieved through certification mechanisms. The certification must be carried out by national supervisory authorities or accredited certification bodies; the certification mechanism must be approved in advance (certification, seal, test mark). The advantage of certification mechanisms is a high degree of legal certainty and transparency, the disadvantage is the complex certification procedure.

Approved contract clauses, self-designed contract clauses or modified standard data protection clauses may constitute suitable guarantees if they have been examined and approved by a national supervisory authority. The advantage is that they can be individually designed and provide a high degree of legal certainty, but the disadvantage is that they require a complex test procedure.

Exceptions for certain cases

In the absence of an adequacy decision or guarantees, there may be exceptions for the transfer of personal data. However, the exceptions listed in Article 49 can only be applied within a narrow interpretation, due to the tiered nature of the assessment. In addition, the cases listed in Article 49 are explicitly and exhaustively regulated.

The exceptions include consent, necessity for the performance of the contract, important reasons of public interest, pursuit of legal claims, protection of vital interests and protection of mandatory legitimate interests.

The consent is an explicit consent of the data subject to the transfer of personal data to a third country in a specific case. In advance, the person must be adequately informed, including specific purpose and risk information. The data subject must be aware that an adequate level of data protection may not be guaranteed in the third country, and that the enforcement of data subjects' rights may be difficult. The data subject must also be granted a right of withdrawal. Consent as the basis for repeated, permanent and mass transfers to third countries is viewed critically by supervisory authorities.

The exception in the context of contract performance may only be made occasionally and is subject to strict necessity. The transfer of data to the third country must be necessary for the performance of a contract with the data subject or for the conclusion or performance of a contract in the interest of the data subject.

An important public interest must be recognised in EU law or in the law of the member state to which the controller is subject.

Data may be transferred to a third country for the purpose of pursuing legal claims if this is necessary, but only occasionally.

The protection of vital interests means that a data subject cannot give consent for physical or legal reasons. In this case, data may be transferred to the third country if it is necessary to protect the vital interests of the data subject or another person.

The exceptions to the mandatory legitimate interest are the catchall element among the exceptions. It represents the very last possibility of justification. The transfer of data may not be repeated, only a limited number of persons may be affected. An overriding

(compelling) interest must arise for the controller, an overall assessment of the controller must be made and suitable guarantees must protect the personal data. The transfer must be absolutely necessary for the exercise of the legitimate interest. In addition, the competent supervisory authority and the data subject must be informed.

Transmission of employee data within the company group

There is no group privilege for company groups. This means that the transfer of personal data to companies in third countries is always a transfer to third parties.

Special case Brexit

When the United Kingdom leaves the EU on 29 March 2019, it will be considered a third country from the data protection perspective. This can be prevented by agreements between the EU and the UK. For this reason, German companies should take the precaution of entering into contractual arrangements with service providers in the UK.

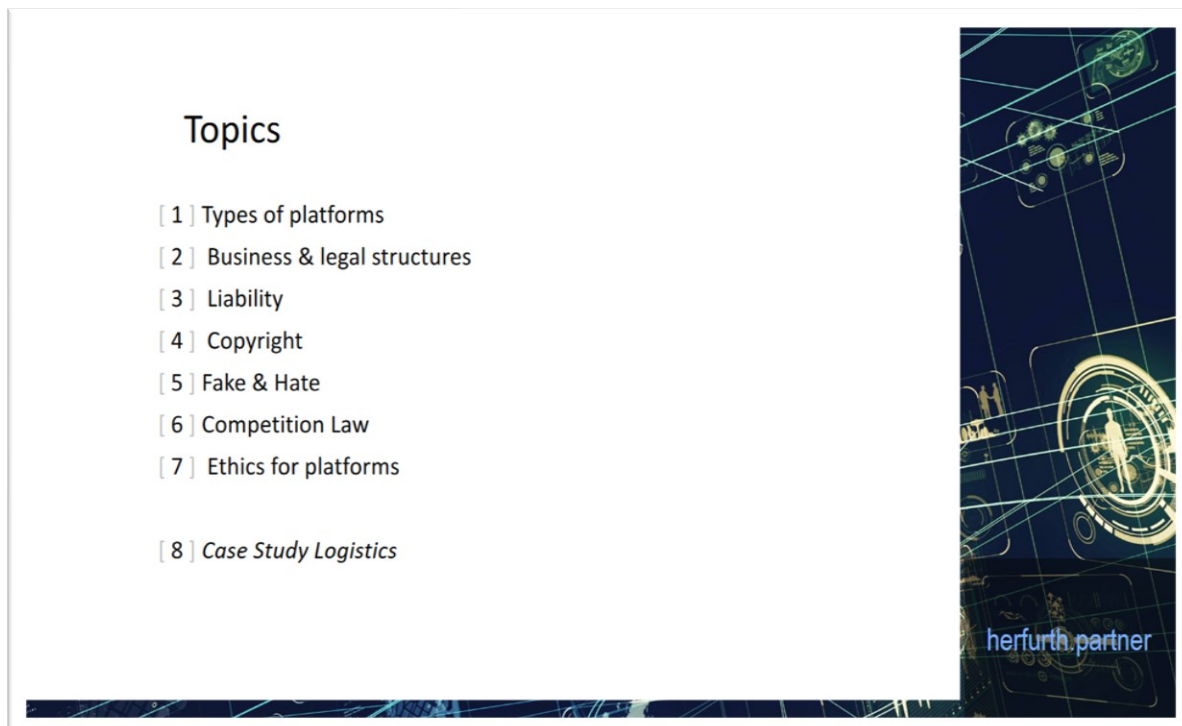
Conclusion

The GDPR provides for special requirements for the transfer of personal data to third countries. The aim is to guarantee the high level of data protection under the GDPR also in relation to third countries. First of all, the basic requirements of the GDPR must be complied with. Only in a second step is it to be checked whether the additional requirements for data transfer to the third country are also fulfilled. For internationally positioned companies, these regulations mean an additional examination effort.

+++

Chapter Four

Business Platforms

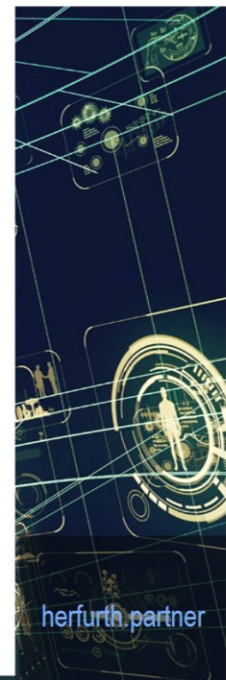


[1] Types of platforms



Types of platforms

- Social media (facebook & Co, contact markets)
- Information (wikipedia, compare portals, consumer info)
- Services (payment, ticketing, booking)
- Trade markets (ebay, amazon, travel, auto24, real estate, sourcing & supply)
- Resources management (tourist, finance, transportation, workforce, services)
- Technical management (routing systems, maintenance systems)
- Other



Types of platforms

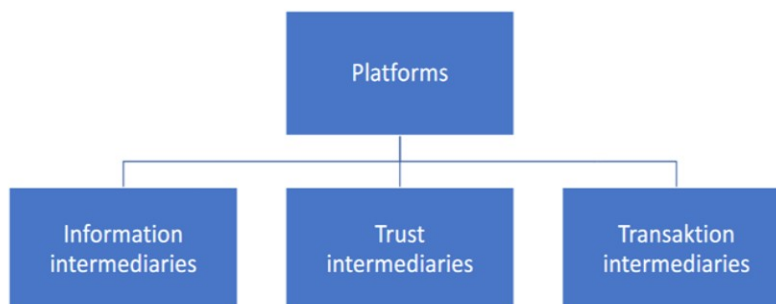
“ Platforms perform different functions in digital markets. The main focus of their activity is on the role as **intermediaries** providing **information**, promoting **trust** and facilitating **transactions**.

In many cases several of these functions are combined ("hybrid platforms").

Effective consumer protection in e-commerce – responsibility and liability of platforms in the internet
Federal Association of Consumer Central / Bundesverband Verbraucherzentralen, Report 2020

herfurth partner

Types of platforms



herfurth partner

Systematisierung von Plattform
Geschäftsmodellen

Information intermediaries

- make it easier for consumers to make choices about products or transaction partners
- Information media can be: search engines, comparison portals but also booking portals
- For example Google, Booking.com, Idealo, Trivago

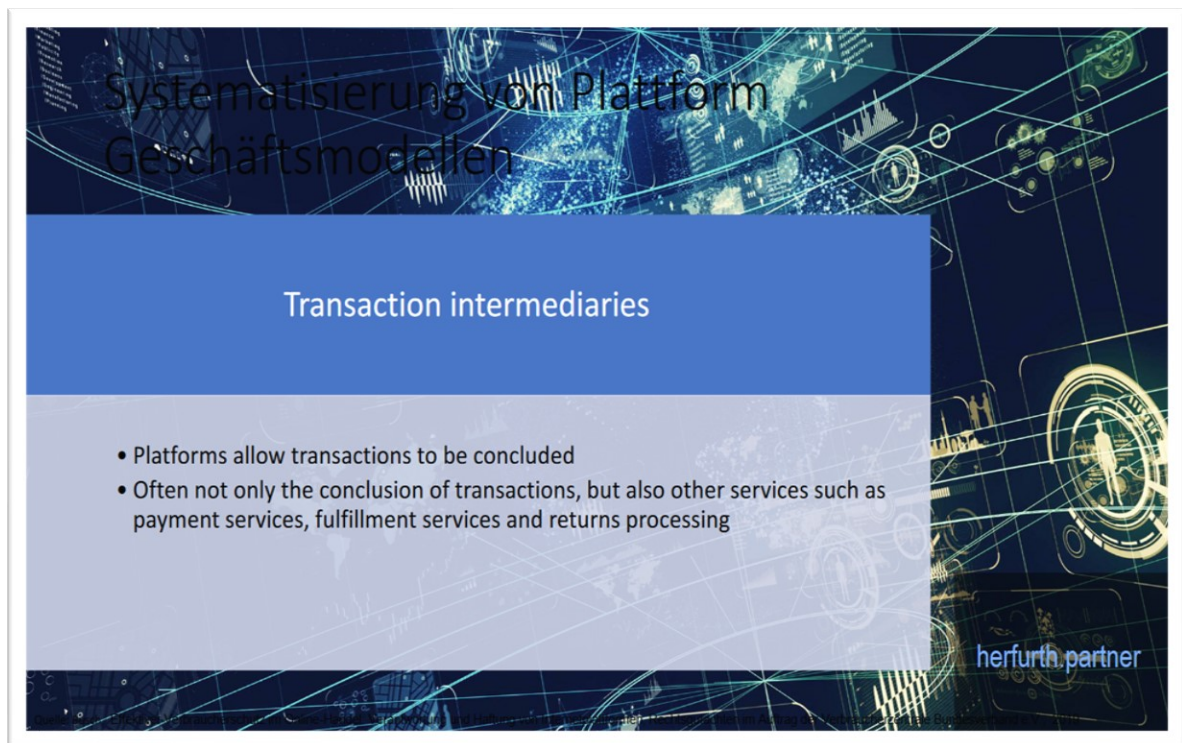
herfurth.partner

Systematisierung von Plattform
Geschäftsmodellen

Trust intermediaries

- Trust between market participants is essential in online trading, as transactions often fail because trust cannot be established between market participants
- Therefore, platform operators offer rating systems so that consumers can evaluate the suppliers or the products offered
- Examples - "pure" evaluation platforms: Yelp, jameda
- Central importance of ratings but also at amazon, ebay or google

herfurth.partner



Systematisierung von Plattform
Geschäftsmodellen

Transaction intermediaries

- Platforms allow transactions to be concluded
- Often not only the conclusion of transactions, but also other services such as payment services, fulfillment services and returns processing

herfurth.partner



[2] Business &
legal structure

herfurth.partner

Business & legal structure

- Platform provider
- Users, customers (users for free, advertisers)
- Contractual relationships / parties (bilateral models)
- Payment flow (if users pay)
- personal data (collected on platform)
- Ownership on collected data
- Taxation of services (*Digital Tax*)

herfurth.partner

Functions

“ *The **combination of different intermediary functions** has consequences for the contractual and non-contractual liability of the platform operator.*

The more comprehensive the involvement of the platform operator in the initiation, conclusion and execution of a transaction, the more extensive are the legitimate consumer expectations and, accordingly, the legal responsibilities of the platform operator.

Effective consumer protection in e-commerce – responsibility and liability of platforms in the internet
Federal Association of Consumer Central / Bundesverband Verbraucherzentralen, Report 2020

herfurth.partner

Legal basis

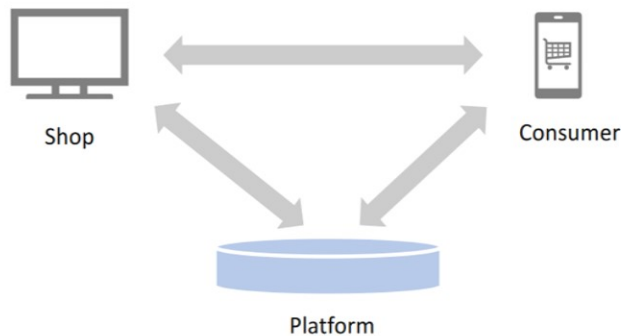
“ So far, there are hardly any **specific regulations** regarding online platforms in German contract and consumer law. The German Civil Code does not contain a specific set of rules for "platform contracts".

Therefore, in case of a dispute it is necessary to apply the general rules and principles of contract law to platform transactions.

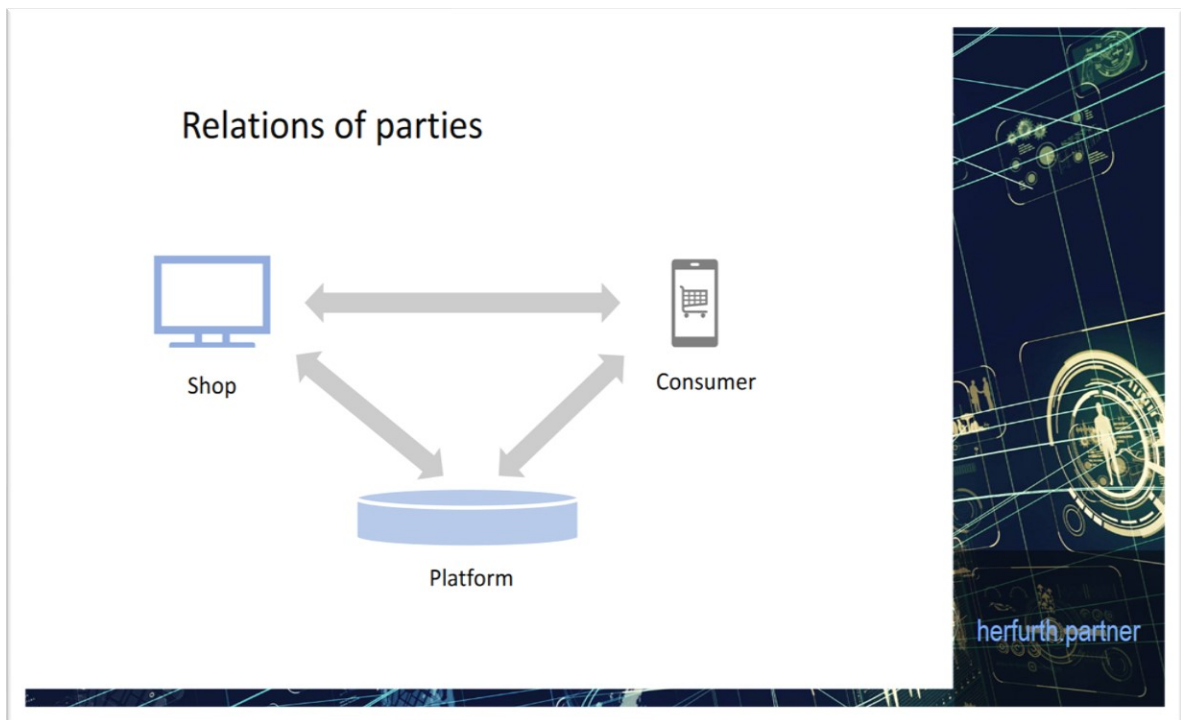
Effective consumer protection in e-commerce – responsibility and liability of platforms in the internet
Federal Association of Consumer Central / Bundesverband Verbraucherzentralen, Report 2020

herfurth partner

Relations of parties



herfurth partner



Relations of parties

“ In most cases, platform transactions involve **three interlocking legal relationships** which form the so-called "**platform triangle**". However, there are also cases in which the platform operator is not only an intermediary but actually the provider of goods or services.

In many cases, it is not sufficiently clear from the consumer's point of view who is responsible for fulfilling the contract concluded via the platform.

Effective consumer protection in e-commerce – responsibility and liability of platforms in the internet
Federal Association of Consumer Central / Bundesverband Verbraucherzentralen, Report 2020

herfurth.partner

Type of contrasts

“ It is a matter of controversy how the contractual relationship between platform operators and consumers can be categorized within the system of contract types under the German Civil Code. According to a widely held view such contracts can be considered as **brokerage contracts** or **agency agreements**.

As the German Civil Code does not provide very detailed rules for these contract types, there is no sufficiently concrete legal framework for platform contracts.

Effective consumer protection in e-commerce – responsibility and liability of platforms in the internet
Federal Association of Consumer Central / Bundesverband Verbraucherzentralen, Report 2020



herfurth partner

Platform contracts

“ The **platform contract** between the consumer and the platform operator is the most important basis for establishing a liability of the platform operator towards consumers.

However, as a result of the absence of statutory rules the concrete content of the platform operator's contractual obligations remains **unclear**. This is true in particular with regard to the scope of **information duties and fiduciary duties**.

Effective consumer protection in e-commerce – responsibility and liability of platforms in the internet
Federal Association of Consumer Central / Bundesverband Verbraucherzentralen, Report 2020



herfurth partner

Duties of platforms

“ It is a matter of **dispute** to what extent the **information duties and organisational obligations** regarding consumer contracts under Section 312 et seq. of the German Civil Code are applicable to platform operators.

*In particular, it is unclear whether platform operators are subject to these provisions also with regard to contracts that have been concluded between **consumers and third parties** via the platform.*

Effective consumer protection in e-commerce – responsibility and liability of platforms in the internet
Federal Association of Consumer Central / Bundesverband Verbraucherzentralen, Report 2020

herfurth partner

Data protection

In principle the platform is subject to the provisions of the data protection regime, in Europe the *General Data Protection Regulation / GDPR*:

- acceptance by the consumer, or
- necessary for the fulfilment of a contract, or
- specific interest of the provider in the data

Question, which data are collected, saved and processed by the platform and which by the shop on the platform.

herfurth partner

Taxation

In principle the platform is subject to taxation for its own business – and in the jurisdiction where it earns its profits.

But with respect to the massive sourcing of data as a basis for its business in a country where the platform generates no income and profit, the respective countries (in Europe) are considering a “*Digital Tax*” on data resources as a kind of source tax/withholding tax.

This concept follows the idea that the providing of data for free could be considered as an equivalent to cash payments for “free” services of the platform.



[3] Liability of platforms



Liability of platforms

- Provider / supplier / shop owner
- Functionality of platform
- Product warranties
- Product liability
- Data protection infringements
- Copyright infringements
- Fake & hate news
- Tax liability (VAT on sales from third countries)
- Legal proceedings, injunctions, information rights

herfurth.partner

Liability of platforms

“ One of the most controversial issues is the question of whether the **platform operator** can be held **liable for a transaction** concluded via the platform, e.g. in the case of a breach of contract by a third-party supplier.

A possible basis for such liability could be Section 311(2) sentence 2 of the German Civil Code, under which a third party can be held liable if, by laying claim to being given a particularly high degree of trust, the third party substantially influences the contract negotiations or the conclusion of the contract.

Effective consumer protection in e-commerce – responsibility and liability of platforms in the internet
Federal Association of Consumer Central / Bundesverband Verbraucherzentralen, Report 2020

herfurth.partner

Product Liability

“ An issue which so far has received rather little attention is the question to which extent platform operators and providers of fulfillment services can be held liable under the German **Product Liability Act**.

Both a liability as an importer (Section 4(2) Product Liability Act) and a subsidiary liability as a supplier (Section 4(3) Product Liability Act) could be envisaged. The study of the consumer federation shows, however, that the Product Liability Act currently does not sufficiently take into account the changing distribution structures created by the rise of the platform economy.

Effective consumer protection in e-commerce – responsibility and liability of platforms in the internet
Federal Association of Consumer Central / Bundesverband Verbraucherzentralen, Report 2020

herfurth partner

Tax liability

Often Online-Shops from third countries sell their goods online without charging German VAT to the consumer. And they don't pay VAT, that should have been collected from its customers, to the state, although the amounts later can be recollected by the Seller from the state.

herfurth partner

Tax liability

Since January 2019, the operator of electronic marketplaces (provider) under certain circumstances has been liable for the VAT obligations of online shops in order to avoid losses of VAT when trading goods on the Internet. The operator does not have to "actively research" the shops operating on his platform. If, however, he becomes aware of facts that indicate a breach of duty by an online shop with regard to VAT, he should request the shop to remedy the breach of duty and block the relevant account if the shop does not comply with this. In addition, he should inform the tax authorities in these cases. The operator is not liable if the shop has presented him with a "certificate of registration as a *taxable person*".

herfurth.partner

[4] Copyright

herfurth.partner

Copyright

Directive on Copyright and Related Rights in the Digital Single Market (2019/790).

The Directive must be transposed into national law by 07.06.2021 (Art. 29 I). The aim of this Copyright Directive: adapting copyright law to the digital age.

Art. 15 and Art. 17 of the Directive are particularly under controversial discussion.



Copyright

Article 15 of the Directive

According to Art. 15 I, press publishers are granted the exclusive right to reproduce and make available to the public the online use of press articles (Articles 2 and 3(2) of Directive 2001/29/EC).

Authors of works contained in a press publication shall receive a fair share of the revenue received by press publishers from the use of their press publications by information service providers (Article 15V of the Directive).



Copyright

Article 17 of the Directive

“Content sharing service provider” means the provider of an information service whose principal purpose or one of the principal purposes is to store and make available to the public a large quantity of copyright works uploaded by its users and protected by copyright, and who organizes and promotes such content for profit-making purposes. (Art. 2(6) also contains exceptions in relation to platforms which do not fall under the notion of service providers of online content e.g. Wikipedia etc.).-

Under the Directive, service providers for sharing online content are now themselves responsible and liable if creations protected by copyright are illegally shared on the platform.



Copyright

Art. 17 provides for a procedure when, exceptionally, service providers are not liable (a kind of exemption mechanism if the service provider meets certain criteria) (inter alia):

- The service provider must apply for a licence
- He shall act promptly upon duly justified notices from rightholders to block access to the protected works

The aim is to treat small services with fewer financial resources differently from large services



Copyright

Facilitation for start-ups under Art. 17 VI

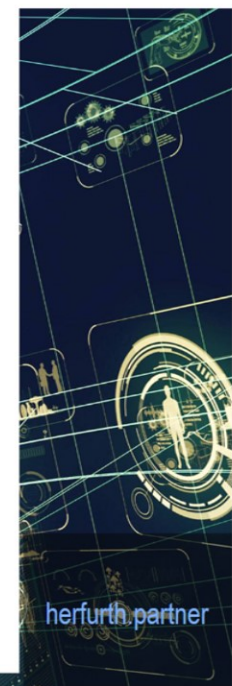
- if the services have been available to the public for less than three years and the annual turnover does not exceed EUR 10 million. In such cases, the duty of start-ups is limited to making every effort to obtain authorisation and to act immediately upon receipt of duly substantiated information from right holders
- if the number of visitors to the website exceeds 5 million per month, every effort must also be made to prevent the future uploading of notified works and other subject-matter on which right holders have provided relevant and necessary information.



Copyright

Requirements of the Consumer Protection Agency with regard to the implementation of the Directive

- If content is marked as parody, the content must be put online and must not be filtered
- Only a human examination should decide whether a copyright infringement is involved or not
- Overclaiming must be minimized
- Upload filters must not be used in an undifferentiated manner
- Content must be kept online during the review
- Complaint mechanisms of the users are simple to keep



[5] Fake & Hate



Fake News & Hate Speech

Fake News

"Disinformation includes all forms of false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit".

Hate Speech

are expressions which are offensive, inciting or discriminatory



Fake News & Hate Speech

Law for the improvement of law enforcement in social networks (NetzDG)

There is the phenomenon of the increasing spread of hate crime on the Internet

The aim of the NetzDG is to improve law enforcement so that objectively punishable content is deleted immediately. The NetzDG is addressed to operators of social networks

Telemedia service providers who operate platforms on the Internet with the intention of making a profit, which are intended to enable users to share any content with other users or make it available to the public (social networks). Social network with less than 2 million users in Germany, is exempt from fulfilling the obligations according to § 2 and § 3 NetzDG



herfurth partner

Fake News & Hate Speech

Reporting: According to § 2 NetzDG the provider has a reporting obligation if there are more than 100 complaints about illegal content in a calendar year, the operator of the social network must publish a report every six months on how complaints about illegal content are dealt with

Complaints: Providers are obliged to have an effective and transparent procedure for dealing with complaints. Among other things, the provider must

- take immediate note of the complaint
- delete obviously unlawful contributions within 24 hours of receipt of the complaint
- delete or block access to any unlawful contribution, as a rule within 7 days of receipt of the complaint

Fines regulations



herfurth partner

Fake News & Hate Speech

Main points of criticism

- Platform providers will delete contributions in case of doubt without a detailed examination of the legality
- Risk of content overblocking

Future additions to the NetzDG

- Supplementing the NetzDG within the framework of the law to combat right-wing extremism and hate crime
- If there are indications that certain criminal offences have been committed, the provider is not only obliged to delete or block the content, but must also report this content to the Federal Criminal Police Office
- In this context, the provider is also obliged to transmit the user's IP address to the BKA



[6] Competition Law



Competition law

- Unfair practices (binding, exclusivity, bundling, business secrets take over)
- Abuse of market power or a dominant market position (unfair selection of information)
- Domination through information / data resources
- Impact of big data technologies
- Impact of algorithms and artificial intelligence (AI)
- National and European Policies

herfurth partner

Ranking systems

“ Legal requirements for **ranking systems** have so far primarily been derived from the rules prohibiting **misleading practices** under unfair commercial practices law. This approach has the disadvantage that the legal limits of the system design can only be determined in reaction to specific infringements on a case-by-case basis.

Based on this case-by-case approach it is hardly possible to elaborate general requirements in the sense of concrete "design duties" for ranking systems. This leads to legal uncertainty and reduces the level of consumer protection.

Effective consumer protection in e-commerce – responsibility and liability of platforms in the internet
Federal Association of Consumer Central / Bundesverband Verbraucherzentralen, Report 2020

herfurth partner

Ranking systems

“ Neither German nor European law define concrete legal requirements for the design of **customer rating systems**.

So far, legal requirements for the "system design" can only be derived from the general requirements of unfair commercial practices law, in particular the prohibition of misleading practices (Sections 5 and 5a Act against Unfair Competition) and the general clause (Section 3 Act against Unfair Competition).

Effective consumer protection in e-commerce – responsibility and liability of platforms in the internet
Federal Association of Consumer Central / Bundesverband Verbraucherzentralen, Report 2020



Ranking systems

“ There are deficiencies concerning the **enforcement** of existing consumer law rules.

*Such deficiencies exist, for example, with regard to **algorithm-based rankings** and recommendation systems due to difficulties regarding the investigation of facts and the distribution of the burden of proof in civil proceedings.*

Effective consumer protection in e-commerce – responsibility and liability of platforms in the internet
Federal Association of Consumer Central / Bundesverband Verbraucherzentralen, Report 2020



Digital market power

Task Force Platforms of the Federal Cartel Office

The Federal Cartel Office has in the year 2016 established a task force in order to examine the power and impact of networks and platforms.

Report of the Task Force platforms of the Federal Cartel Office, 2016



Digital market power

“ *In the case of indirect network effects, the benefit of the platform performance for one user group depends on the size and composition of the other user group. They are positive if the benefit of a platform for a participant is the greater the more potential interested parties a participant can reach.*

For the economic analysis and the antitrust assessment of digital platforms it is necessary to include the non-monetary user side as well, in order to be able to adequately consider the interdependence of the two sides of the platform. According to previous (national) case law, however, non-monetary user relationships have generally not been considered a market. In particular, this approach no longer does justice to the special features of the Internet economy.

Report of the Task Force platforms of the Federal Cartel Office, 2016



Digital market power



Network effects

New users prefer to opt for platforms or networks that already have a larger number of users. Therefore, network effects in a market can have a self-reinforcing tendency. This self-reinforcing tendency can ultimately even lead to the monopolisation of a market.

In addition, network effects may increase switching costs on the part of users and create barriers to entry on the part of potential competitors.

Report of the Task Force platforms of the Federal Cartel Office, 2016



Digital market power

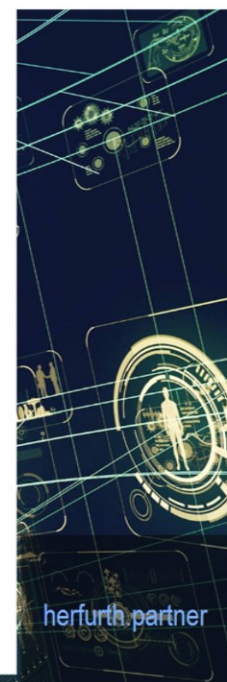


Economy of scales of platforms and networks

As in traditional markets, economies of scale of the platform or network of an incumbent may make it more difficult for new, smaller suppliers to enter the market.

Economies of scale are often particularly pronounced in the case of digital platforms and networks, as the establishment and operation of a platform or network often involves significant fixed costs but low variable costs. In addition, there are specialisation and learning processes through operation that smaller and new providers do not yet have.

Report of the Task Force platforms of the Federal Cartel Office, 2016



Digital market power

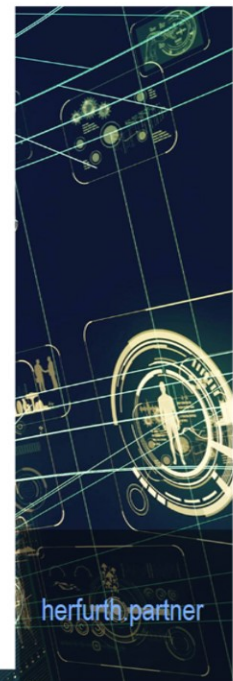


Access to data

Customer and user data, but also third party data are a valuable source of information for companies. Through digitisation and above all the Internet, the possibilities of data acquisition and data use are reaching a new dimension. Moreover, many digital products are essentially based on data, exclusive dominance over certain data can be a barrier to market entry for competitors. This is particularly true if indirect reciprocal network effects are at work in the market concerned.

While data dominance alone is not an indication of market power, it may play an important role in the overall assessment of all circumstances.

Report of the Task Force platforms of the Federal Cartel Office, 2016



Digital market power

X.th Amendment to the German Cartel Law

The Federal Ministry for Economics has in 2019 submitted a draft for another amendment of the Law against Competition Restrictions (Gesetz gegen Wettbewerbsbeschränkungen, GWB), which is now under discussion in the federal government.

It provides new criteria for dominant market power, among others information power (data) and cross sector domination.

The IX.th amendment was already issued in 2017 and has introduced a new criteria for the thresholds in merger control: no longer the turnover of the target but also the purchase price for the target.

Report of the Task Force platforms of the Federal Cartel Office, 2016



Digital market power

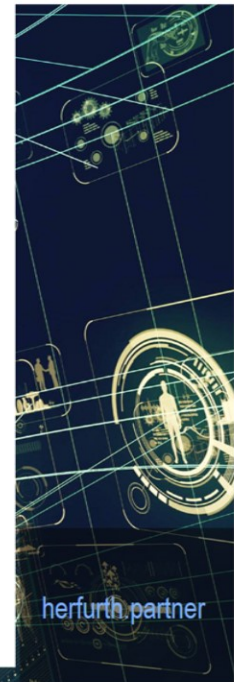
Cartel Office vs. Facebook

The German Supreme Court a few days ago has stated that data protection and consumer protection is relevant for competition law.

Facebook's ability to bring consumers to accept the very unfavourable data protection provisions of Facebook, is an indication for a dominant position, that Facebook abuses for its purposes.

>> the transfer of personal data through the *like* button on websites of third parties is prohibited even when consented by the user. And the transfer of data within the Facebook group requires an express consent of the user.

Report of the Task Force platforms of the Federal Cartel Office, 2016



[7] Ethics



Ethics for platforms

- National Ethic Codes
- European Policies
- International Trends



[8] Case Study

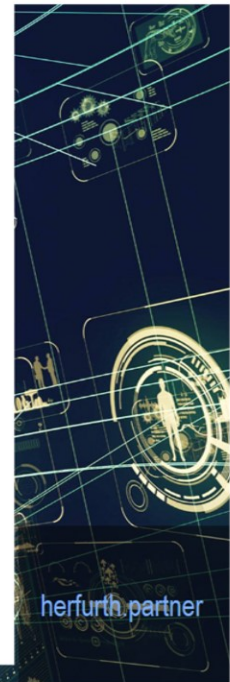


Case Study: Logistics

- Logistic Portal: monitoring of goods on travel (parcels, pallets or containers can be monitored through sensors and communication chips),
- overview about place (geo-tracking), movement, estimated timeframe for arrival, temperature, shocks, condition of parcel etc.
- Provider owns sensors, free to customers, transaction based fee, sale of process information/ and or market information to customers and third parties

Question:

- which kind of legal relations are built?
- Who is the “owner” of the data generated during the trip ?



Contact & Literature

Contact us

Ulrich Herfurth
Herfurth & Partner
Rechtsanwaltsgesellschaft mbH
Luisenstr. 5, 30159 Hannover

Tel 0511 – 307 56 (0)
Mail herfurth@herfurth.de
Web www.herfurth.de



Literature

Literaturverzeichnis:
redaktion@herfurth.de





[1] Section



Question & Answers

Digital Business Platforms

1. Which kind of online platforms do you know in your country?

Maria Inês Reis (Portugal):

Citius, zoom, skype, facetime, excepting Citius (courts) we have all international platforms for business.

Iv Fangyuan_(China):

Alibaba

Qiu Shuang (China):

Taoba Jingdong Dangdang

Qiyi Zhang (China):

There are many network platforms in China, such as Taobao, Tmall, Jingdong, Suning, DangDang.com, Amazon China, Vipshop, Jumei Youpin, Netease strict selection, Meili, Mogujie and so on.

Eduardo Barrera (Mexico):

Among the normal ones (Amazon) and their Mexican version (Mercado Libre) specific for business are linked from the government in case of competitive platforms to invest into energy and others.

Friederike Ammann (Germany):

- Social Media
- Information platforms
- Trade markets

Jannis Ulrich (Germany):

For Business is the best known Xing.

Arthur Horsfall (UK):

The European Commission has identified the following online platforms:

1. online marketplaces (Amazon, Ebay, Booking.com)
2. collaborative or 'sharing' economy platforms (Uber, Airbnb)
3. communication platforms (Skype, Zoom, Whatsapp)
4. social networks (Facebook, LinkedIn, Twitter)
5. search engines and specialised search tools (Google search, Tripadvisor, Yelp)
6. maps (Google maps, Apple maps)
7. news aggregators (Google news, Apple news)
8. music and video platforms (Spotify, Netflix, Apple TV)
9. video sharing platforms (Youtube)
10. payment systems (PayPal, Apple Pay)
11. app stores (Google Play, Apple app store)

In addition to these gambling online platforms have increased quickly in popularity.

Coral Yu (UK):

GoDaddy and Shopify, for examples.

Gary Whitehead (UK):

Social media, app stores, Price comparison websites

Philippa Kwok (UK):

- Social media
- Online marketplaces

Julia Krautter and Patrícia Perinazzo (Brazil):

eBay, Amazon, Airbnb, Uber, Mercado Livre

Luis Roberto Moreno Tinoco (Mexico):

Mexico has currently a large number of online platforms that have been connecting producers and consumers for a few years by now. Among the main examples, we could enlist platforms specialized in accommodation services, such as Airbnb, platforms focused in the sell and purchase of goods, such as Amazon or Mercado Libre, or even platforms specialized in financial services, that work through crowdfunding regimes, in which any individual who wants to invest can lend money to the people that are signed in and looking for credit through the app.

Mari Yoli Wulf Sánchez (Mexico):

Mercado Libre, Amazon, Best Buy, Ticketmaster, Liverpool.

Miguel Ángel Aspe de la Rosa (Mexico):

Amazon, Uber, Uber Eats, DiDi, DiDi Food, Jeff.

Nadiezhda Vázquez Careaga (Mexico):

Zoom, Share Point, Teams.

Paulina Saldaña Fuentes (Mexico):

Government is trying to migrate to an online system. Few institutions have their data site to do the corresponding filings, but this has just started. As to do business online between private parties I have no further knowledge that “Zoom” and “Google Meet” platforms.

Ricardo Heredia (Mexico):

Uber, Rappi, Amazon, Airbnb, among others

Fergan Tuğberk İşman (Turkey):

The most common online platform types in Turkey are market type platforms and social media platforms. Market platforms allow the platform owner or other third party users to sell products through the online platform. These platforms make profit by selling products or taking commission from the third party users’ profits. Social media platforms are platforms that anyone can use to interact with their desired contents. These platforms make profit from ads designed specifically for the user.

2. Which kind of regulation exists?

Iv Fangyuan_(China):

The E-Commerce Law of the People's Republic of China.

Qiu Shuang (China):

There are special network supervision departments, such as network crime reporting website.

Qiyi Zhang (China):

Service Specification for Third-party E-commerce Trading Platform issued by the Ministry of Commerce on April 12, 2011; Measures for The Administration of Online Transactions issued by the State Administration for Industry and Commerce on January 26, 2014. There is no specific law to regulate the network platform.

Eduardo Barrera (Mexico):

There is specific regulation in the Consumer Rights Federal Law for E-Business in Mexico, but also another to regulate Institutions with Financial Technology.

Friederike Ammann (Germany):

Competition law and Data protection.

Jannis Ulrich (Germany):

Maybe the rule not to advertise in legal business, § 43 b BRAO. Or the “Netzwerkdurchsetzungsgesetz”, a law against hate speech in the internet.

Arthur Horsfall (UK):

In 2000, the EU agreed the e-Commerce Directive which set the framework for Internet regulation within the European Union. In December 2019 the UK Government announced that it will introduce legislation to tackle Online Harms, following on from the Online Harms White Paper (April 2019). The general provisions of existing laws such as GDPR and Competition laws will apply.

On 1 July 2020, the Competition and Markets (**CMA**) authority published the Final Report of the “Online Platforms and Digital Advertising” market study. The conclusion to this study was that existing competition law tools are not sufficient to regulate the major online platforms, such as Google and Facebook. The CMA called on the UK Government to establish a pro-competition regulatory regime for online platforms, by creating a Digital Markets Unit. This unit would have powers to deal with concerns swiftly and before irrevocable harm to competition can occur.

Coral Yu (UK):

There is no UK legislation specifically addressing how online platforms deal with their business users; instead normal business to business rules on the supply of services will apply. During consultation on the Online Intermediation Services Regulation, the UK government suggested that the relationship between platforms and their business users is an area which can largely be addressed through competition law. The UK government is reviewing how it applies competition law to online platforms as part of its Digital Market Strategy.

When comes to how online platforms deal with their consumers:

- The Unfair Commercial Practices Directive (2005/29/EC) (**UCPD**) is implemented in the UK by the Consumer Protection from Unfair Trading Regulations 2008 (SI 2008/1277). The UCPD prohibits traders from engaging in commercial practices towards consumers which are misleading, aggressive or contrary to the requirements of professional diligence, whether before, during or after any transaction.

- The Consumer Rights Directive (2011/83/EU) (CRD), which is largely implemented in the UK by the Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013 (SI 2013/3134) (CCRs), as well as the Consumer Rights Act 2015 (CRA), imposes information obligations on all traders dealing with consumers and introduces cancellation rights for consumers when they buy at a distance (for example online).

In addition, The E-Commerce Directive is implemented in the UK by the Electronic Commerce (EC Directive) Regulations 2002 (SI 2002/2013) (**E-Commerce Regulations**). The E-Commerce Regulations apply to any information society service (**ISS**, meaning any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services).

Note also The Online Intermediation Services for Business Users (Enforcement) Regulations 2020 (SI 2020/609), which deal with UK enforcement of The Regulation on promoting fairness and transparency for business users of online intermediation services (Regulation (EU) 2019/1150) (the **OIS Regulation**), will apply from 12 July 2020. The OIS Regulation requires online intermediation service providers (such as providers of online e-commerce market places, software application services and social media services) and online search engines to comply with certain transparency obligations, mainly by including information in their terms and conditions or, for search engines, publishing it on their websites.

Gary Whitehead (UK):

EU is proposing the P2B Regulation – unsure if will be retained post-Brexit or similar equivalent.

Philippa Kwok (UK):

- Data protection
- IP
- Consumer protection
- Competition

Julia Krautter and Patrícia Perinazzo (Brazil):

In Brazil the consumer defense code is the main rule applied for online purchases.

Alitzel Sánchez Alonso (Mexico):

Free trade economic competition applicable law.

Luis Roberto Moreno Tinoco (Mexico):

Regulation of digital platforms in Mexico is poor, since there are very few provisions that refer to this type of business model.

A couple of years ago Mexican congress issued the "Fintech Law", intended to regulate the entities that offered financial services through digital platforms, including those who operate under a crowdfunding model. However, although this was significant from a historical point of view, the new law fails to regulate all the other transactions that are carried out through this kind of business model.

As of 2020 new tax provisions entered in force in Mexico, intended to regulate the income that is perceived by individuals who participate in the models of the digital economy. In accordance with the new provisions, individuals that receive an income from any digital platform (such as amazon, airbnb, etc) are obliged to pay income tax over that income, through a withholding made by the entity that provided the platform service.

Mari Yoli Wulf Sánchez (Mexico):

Personal Data Protection.

Miguel Ángel Aspe de la Rosa (Mexico):

The labor regulation for these online platforms is non-existent. Recently the Mexican congress issued a reformation in order to aggressively tax the income of these businesses.

Nadiezhdá Vázquez Careaga (Mexico):

There is no regulation.

Paulina Saldaña Fuentes (Mexico):

The Commercial Code regulates the electronic signatures to be replicated in intercompany agreements; nevertheless the practical implementation has been slow and the courts not always recognize such signatures as valid agreements.

Ricardo Heredia (Mexico):

- Commercial Code and Civil Code – Electronic agreement.
- Intellectual Property Law – Regulation of trademarks and patents.
- Data Privacy Law – It regulates when personal data from people is stored.
- Federal Labor Law and Civil Code – It should work together in order to determine the labor relationship; for example, between distributors and company such as uber eats.
- Monetary Law – It determines how the exchange rate is determined in international transactions.
- Tax regulation – It determines, special taxes for these new services in the country.

Fergan Tuğberk İşman (Turkey):

Online platforms brought up different types of issues. Some of these issues are protection of the users' personal data, validity of distant contracts and preventing crimes that happen with the use of the platform against its intended use.

Data protection is monitored by the Personal Data Protection Authority which has the right to issue fines to the platforms that have violated the Personal Data Protection Law.

Distant contracts are regulated on the Law on the Protection of the Consumer. Buyers at the online market platforms are considered as consumers. This gives the consumer some benefits such as rescission from the contract within 14 days without giving any reason.

The precautions against any criminal activity on those platforms are provided by the platform owner. The owner has an obligation to monitor and report any suspicious activity of users on the platform.

3. What are the main legal problems with online platforms?

Maria Inês Reis (Portugal):

Hackers online attack all the classified information.

Iv Fangyuan_(China):

tax evasion, fake products, fake transaction.

Qiu Shuang (China):

The distribution and division of legal liability is not clear.

Qiyi Zhang (China):

In general, there are four aspects to the law concerning e-payment institutions:

1. Issues related to payment subjects, such as commercial banking law, etc.
2. Standardize payment behaviours, such as a series of behaviours such as payment settlement and clearing.
3. Standardize the relevant provisions of payment tools, such as payment tools except currency and credit CARDS, management measures and regulations of credit card management, etc.
4. Laws and regulations to prevent financial crimes and protect consumers, such as the Anti-money laundering Law. In addition to money laundering, financial crimes include fraud, robbery and other financial crimes to protect consumers' rights and interests. In principle, the laws of the four aspects are relatively practical for third-party online platforms to be defined as non-bank financial institutions, and the specific applicable laws may vary. For example, in the last

aspect, in terms of combating financial crimes and protecting the rights and interests of consumers, financial crimes include money laundering and financial fraud. According to our research, the problems faced by third-party online payment platforms are more serious than those in the traditional payment field.

Eduardo Barrera (Mexico):

Lack of secondary enough regulation for the “praxis”, including taxes and certainty for employees, but also into how far the responsibility their owners and participants really can go.

Arthur Horsfall (UK):

- Issues with transparency – such as:
 - how search results are ranked;
 - how personal data is used;
 - the advertising used; and
 - setting out the rights consumers may have in the event of non-performance by another party.
- Regulation of how platforms use the information/data they acquire
- Regulation of illegal actions and online harm.
- Protection of the users use of the platform (such as on gambling platforms).
- Relations between platforms and suppliers (e.g. asymmetries in bargaining power and the fairness of terms and conditions)
- Constraints on individuals and businesses’ ability to switch from one platform to another

Coral Yu (UK):

As identified in the Commission's 2015 consultation on the regulatory environment for platform, the main legal problems would appear to be about competition and unfair trading, as there naturally tend to be only a small number of platforms in a particular sector:

- Control access to online markets and exercise significant influence over how various players in the market are remunerated.
- Be less than transparent as to how they use the information they acquire.
- Adopt terms and conditions which reflect their strong bargaining power compared to that of their clients (particularly SMEs).
- Promote their own services to the disadvantage of competitors.
- Adopt non-transparent pricing policies, or restrictions on pricing and sale conditions.

Gary Whitehead (UK):

Data protection, IP protection.

Philippa Kwok (UK):

- Data protection
- IP
- Consumer protection
- Competition

Julia Krautter and Patrícia Perinazzo (Brazil):

Responsibility between the online platform and the seller face to a consumer complaint; storage and security of consumer data; unauthorized marketing; targeted marketing; and so on.

Alitzel Sánchez Alonso (Mexico):

Even though I do not have in mind one of these, I think that probably the system is not very easy for its' use or the personal data protection use might not be that clear.

Luis Roberto Moreno Tinoco (Mexico):

The main legal problems with online platforms include the way in which the income received by these companies shall be taxed, since it is really difficult to determine where the source of wealth of that income is located, especially when the provider of the internet service, the provider of the goods or services, and the consumer reside in different countries for tax purposes.

Other problems may involve the applicable law for the contractual obligations assumed by the parties, when this circumstance was not expressly agreed upon in the contract, as well as the competent courts to resolve any eventual controversy.

Mari Yoli Wulf Sánchez (Mexico):

Communication

Miguel Ángel Aspe de la Rosa (Mexico):

The main legal issues that exist in Mexico are related to scams or default to deliver a certain good.

Nadiezhdá Vázquez Careaga (Mexico):

Confidentiality, exist the possibility that hackers can access to the meetings.

Paulina Saldaña Fuentes (Mexico):

The lack of encryption for confidential documents that can be hacked by any third party.

Ricardo Heredia (Mexico):

For the moment:

- New taxes that the government is considering.
- Currently, due to unemployment crisis because of the COVID, many uber eats drivers are assaulted and take the place of the driver. The main problem is that they enter homes as if they were uber and steal from people.

Fergan Tuğberk Işman (Turkey):

Online platforms are open to cyber attacks and it is vital for the owner to protect the platform and its users. If necessary cautions haven't been taken, the owner may face legal consequences.

With a cyber attack, a platform can lose its protected personal data of it's users to other bad intended parties. This would violate platform users' right of privacy. If the proper measures were not taken, the platform owner will be held responsible for this violation.

+++

Materials | Compact

Providers, Platforms and Networks

Martin Heitmüller, Rechtsanwalt in Hanover

Maitre en droit (FR)

January 2016

In networked production, there will be a considerable need for infrastructure for the storage, exchange and processing of data. Structures are to be differentiated according to their purpose, whether they are used unilaterally by one company or multilaterally by several or many participants.

Providers

Functions

Unilateral structures serve the interests of a company by outsourcing its data and processes to a specific data centre (*host*) or to providers of server capacity (*cloud*), possibly also with outsourced software (*software as a service*) or as an outsourced overall handling of operational functions (*outsourcing*). These services can also be made available to third parties, for example as an online ordering platform, internet presence, service portal or other - but the services offered by one company always remain the same.

Services

The main legal problem here is to guarantee the functionality of the provisioning services for the availability and security of the data, defined by service levels based on contractual agreements and service level agreements. Already today, the performance and security of computer centres is probably superior to the IT structures in most companies or cannot be achieved with reasonable effort by medium-sized companies. Companies that entrust their data and processes to a provider must, however, not only contractually guarantee the functionality, but also the protection of their data from unauthorized access.

Data stocks

As a rule, providers have no justified interest of their own in the external data of their customers, as they are only involved in processing orders and data is not an integral part of a production or service chain. Therefore, providers may not use their customer data for their own purposes or make it available to third parties. Companies as customers should have the provider guarantee that only authorized employees have access to the data and that they are bound by appropriate confidentiality agreements. From the company's point of view, company data must be protected against third-party access and personal data must be protected in accordance with the provisions of data protection law. The importance of certifications for providers will continue to grow, especially to the extent that they prove that the provider's confidentiality obligations have been met.

Data protection

The company is also subject to national and European data protection regulations in its relationship with the provider, the effectiveness of which will be significantly increased with the adoption of the General Data Protection Regulation. The outsourcing of personal data subject to European data protection to servers in third countries has hardly been possible without legal problems to date, nor is access from there. In 2015, the European Court of Justice ruled that the practice approved by the European Commission of transferring data to recipients in the USA in accordance with the *safe harbor* concept was inadmissible: the state access rights in the USA do not treat data protection in the same way as in the EU. It is doubtful whether the quality can be effectively achieved by the model clauses agreed with the European Commission between companies in the sense of a protected data environment. The EU Commission has therefore agreed a new concept with the US government: *privacy shield*. The legal character, the scope and the factual reliability of this new agreement, however, seem to be insufficient to many data protectionists.

Platforms

Functions

Platforms serve as multilateral structures for linking many independent users. They provide an infrastructure on which users can move around and connect with each other and process transactions without the platform operator having to do anything.

In principle, platforms are to be differentiated according to their function; they are information platforms (*Google*), contact platforms (*facebook*, various partner search portals), communication platforms (*WhatsApp*), archive platforms (*Instagram*), trading platforms (*ebay*, travel portals, car portals, real estate portals, financial services portals), sales platforms (*Amazon*), payment platforms (*paypal*) and many more. Thereby, functionalities mix within the scope of *social media* offers, up to contradictory offers like

independent price comparisons and product sales. Whether a portal legally represents a platform is determined by its concrete structure.

Platforms can be distinguished according to their performance profile:

- Content provider → publishes own content
- Host provider → provides storage space
- Access provider → provides access to the internet
- Usenet provider → offers networks for discussion forums

The specific legal issues relating to platforms are linked to a not always clearly defined liability for the offers and transactions of their users. In principle, a platform operator will contractually exclude the warranty and liability for deficiencies in the performance of its users; he does not want to be legally responsible for the quality of the products sold on the platform, also not for the seriousness and creditworthiness of the supplier and buyer. That a platform operator has a business interest in a customer portfolio that is as reliable as possible is another question that he likes to answer with customer ratings. It is doubtful whether a platform operator can also exempt himself from liability if he uniformly stipulates the terms and conditions of sale for his users' transactions - from the user's point of view, this may bring him close to the image of a service provider.

The liability of the platform operator for illegal content posted by users is also critical. While the infringement of personal rights (one's own image) and public law barriers (glorification of violence, incitement of the people, etc.) is the main focus in communication platforms, the risks in information and trading platforms lie in infringements of copyright, design law, trademark law and other industrial or intellectual property rights. The liability for such illegal content is currently not treated uniformly by the courts: a platform operator is obliged to remove illegal offers on his platform at the request of the injured party whenever a court order requires to do so. In the meantime, however, case law has also demanded in individual cases that the platform operator should be obliged to independently check the legality of the offers posted on his platform, at least if it is a matter of repetition of an infringement already established. The platform operators argue to such obligations of verification that a platform is comparable to a trade fair, a stock exchange or the advertising section of a publication but is not itself a provider. The distinction is explosive because the removal of content is only a negative covenant, but a breach of a duty to check could give rise to a claim for damages with far-reaching consequences.

A distinction should be made regarding the liability of platforms and their providers for content:

- Content provider → full liability for content
- Host provider → with blocking obligations for content
- Access provider → without own blocking obligation for contents
- Usenet provider → not liable for content

These violations, which up to now have occurred mainly in social media and trade platforms, can also occur in a similar form in industrial platforms, for example for purchasing, logistics or personnel deployment (*crowd working*). These can be violations of technical property rights (patents, industrial designs, design, also copyright for software), but also the provision of illegally obtained personal or company data. If an infringed or allegedly infringed party attacks the publication of an information on the platform, the decision to remove the offer can have considerable economic consequences for the platform operator and the provider. Due to the risk of damages, the platform operator will tend to comply with the request for removal of the offer, the offeror will at least temporarily lose his offer on the platform and thus possibly lose business.

Details on platform liability

The principle - Notice and take down

The German Telemedia Act (*Telemediengesetz/TMG*), which is based on the European E-Commerce Directive of 2000, has legally established the so-called notice and take down principle in § 10 TMG. According to this principle, service providers are not responsible for third-party information which they store for a user, provided they have no knowledge of the illegal act or the information (§ 10 no. 1 TMG) or if they act immediately to remove the information or block access to it as soon as they have gained knowledge of it (§ 10 no. 2 TMG). The provision of § 10 TMG is tailored to the classic host provider.

The decision of the German Federal Court of Justice "Online auction I"

However, the 2004 ruling of the German Federal Court of Justice (*Bundesgerichtshof/BGH*), the so-called "Online auction I" ruling ("Internet Versteigerung I"-Urteil), caused the notice and take down principle to be shaken. In the dispute with the online platform ricardo.de, Rolex was not satisfied with the removal of the goods from the offer after having obtained knowledge of them, but additionally demanded that such infringements be avoided in the future as well.

The BGH did not apply the liability privilege of the notice and take down principle from § 11 of the German Teleservices Act (*Teledienstegesetz/TDG*), which was still valid at the time, arguing that this only applied to claims for damages, but not to claims for injunctive relief that would have an effect in the future. However, the BGH also saw that an excessively extended negative covenant, which would lead to every offer being examined for infringement before publication on the internet, would go too far and would call the entire business model into question.

It was therefore decided that a negative covenant in the context of liability of interference could only be assumed in the case of a violation of the duty to examine. In

the case decided, the defendant internet platform had to use the incidents with the Rolex watches as a cause to subject offers of such watches to a special examination. Which technical possibilities are available, e.g. special software, was disputed in the proceedings.

The further development: the BGH ruling "Youth-endangering media on eBay"

In its 2007 ruling "Youth-endangering Writings on eBay" („Jugendgefährdende Schriften bei eBay“), the BGH further substantiated the case law based on the decision " Online auction I", among others.

This ruling also dealt with the justification of negative covenants. The reason for this was not the infringement of trademark rights, but the dissemination of third-party content harmful to minors. This time the duties of omission were derived from competition law.

According to the BGH, the defendant internet platform was not only obliged to immediately block the specific offer which was harmful to minors of which it had become aware. It also had to take precautions to ensure that no further similar legal infringements occurred.

The judgement clarified that such similar infringements of rights are not only offers which are identical with the offers which have become known, i.e. which concern the offer of the same item by the same auctioneer. According to the judgment, the defendant platform must also prevent the media harmful to minors which are specifically identified to it from being offered again via its platform by other bidders.

Furthermore, offers in which the same auctioneer offers contents of the same category harmful to minors on the same carrier medium would also be considered to be similar to a certain violation of the law for the protection of minors.

Trend reversal: Restriction of the platform operators' obligation to check, the BGH ruling "Highchairs for children on the internet"

However, in a ruling from 2012 („Kinderhochstühle im Internet“), the BGH again restricted the obligation of the platform operators to check. It was no longer reasonable to take control measures where suspected trademark infringements could not be detected by the filter software, but where every offer containing the trademarks in question had to be subjected to an additional manual control. The BGH rejected such a far-reaching duty of control.

Conclusion

The case law presented in excerpts shows that the legal situation regarding platform liability is still very unclear, characterised by ramified case law and difficult to predict.

This legal uncertainty is certainly not conducive to the market entry of new Industry 4.0 platforms. At the moment, however, this legal uncertainty has to be calculated. Further developments must be closely followed.

Telecommunication Law

The consideration of telecommunication law is important for the topic Industry 4.0, because in most cases the M2M data is transmitted via a mobile network. In particular, the transmission of data and the offer of services within the framework of M2M communication can subject the parties involved to certain obligations under telecommunication law.

The transmission of data legally constitutes telecommunication and often includes telecommunication services within the meaning of the German Telecommunications Act (*Telekommunikationsgesetz/TKG*). It is not relevant here that the information in telecommunication is transmitted from person to person.

The communication infrastructure is usually in the form of mobile phone networks, so that the network operators are the "providers" of the telecommunication services, contractual partners for certain services are "subscribers" and the customers of the services, e.g. drivers of *connected cars*, are "users" in the sense of the TKG.

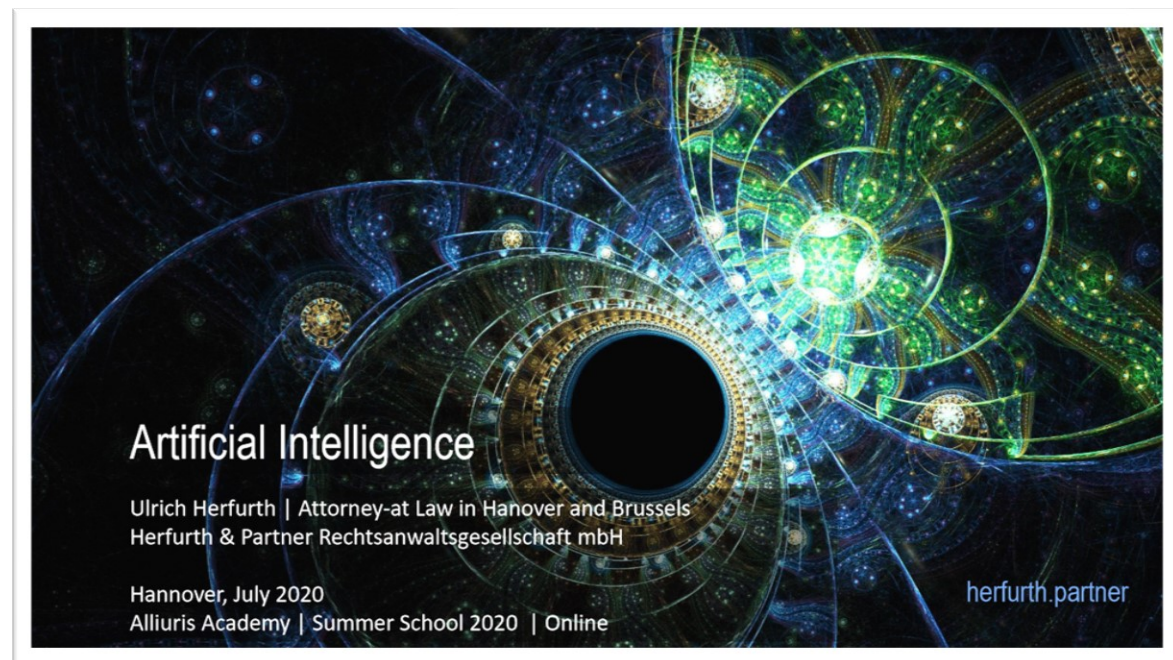
Whether M2M communication platforms are telecommunication services depends on their specific function: the transmission of control signals from and to participating M2M devices is generally a telecommunication service, whereas transmission is not the essential element in the provision of content on the platform for retrieval by users. The ISO/OSI layer model for internet services is often used to define the character of mixed services. The layers 1 to 4 have more transmission characteristics, the layers 5 to 7 more content character.

M2M *services* usually do not focus on the transmission of information, but rather on content and functionalities such as vehicle data (driving style, positioning); they are thus typically not telecommunication services, but tele-media services in the sense of the German Telemedia Act (*Telemediengesetz/TMD*).

If an M2M service is subject to the TKG, the provider of the services has to fulfil a number of obligations relating to customer protection, frequency use, numbering, telecommunication secrecy and telephone tapping. With regard to the liability obligations, it should be emphasized that according to § 44a sentence 1 TKG, the providers of telecommunication services are only liable for financial losses of their end users caused by negligence to the extent of EUR 12,500 per case of damage and end user. This sum can be quickly exceeded in the context of M2M communication and a contractual increase in the liability sums should therefore be considered.

Chapter Five

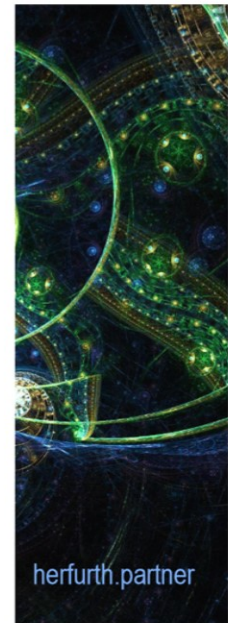
Artificial Intelligence



Artificial Intelligence

Artificial intelligence is a highly developed electronic system that is no longer conclusively defined and programmed by human beings, but rather gains and develops its own insights from collected information and patterns (deep learning, machine learning). It uses extensive electronic networking structures for this purpose.

An AI system is self-learning and makes independent decisions based on self-developed algorithms.

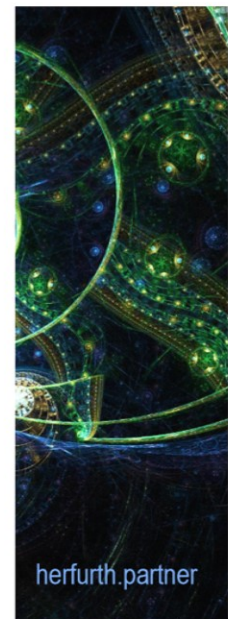


herfurth.partner

Artificial Intelligence

- AI is a subdivision of computer science in technical terms
- Since the 1980s, the driving force behind digitalisation
- Millions of comparisons of data in grouped circuits with multiple layers (artificial neural networks, ANN)
- Result is e.g. pattern recognition (dog and cat)

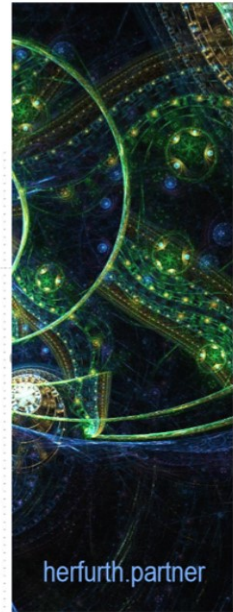
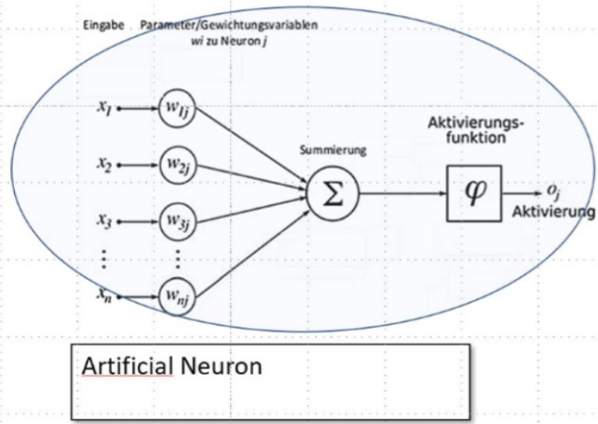
- Weak AI = instrument under control of the operator
- Strong AI = autonomous action of the system with neuronal functionality, but possibly other cognitive structure than the brain.



herfurth.partner

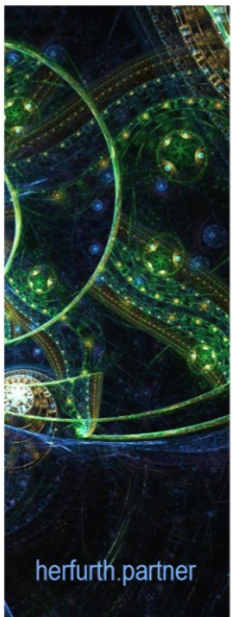
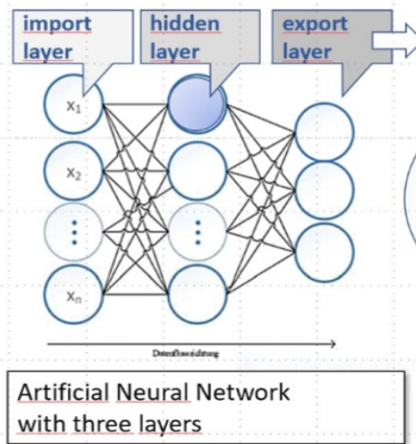
Artificial Intelligence

Artificial Neural Networks



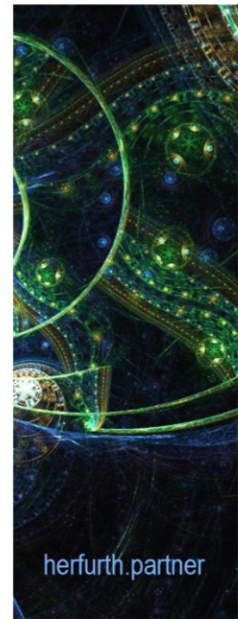
Artificial Intelligence

Artificial Neural Networks



Applications and Markets

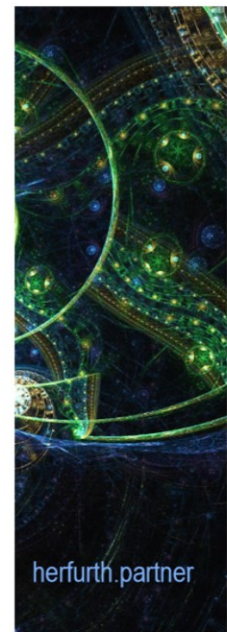
- Data mining and analytical evaluation of large amounts of data, big data target group-oriented **marketing**, especially in social media and e-commerce.
- Languages with semantic understanding for machine **translation**, voice-controlled assistants (Alexa, Siri), Social Bots / Chat Bots
- **Securities** trading and electronic investment advice (Robo Advisory for securities investments)



herfurth.partner

Applications and Markets

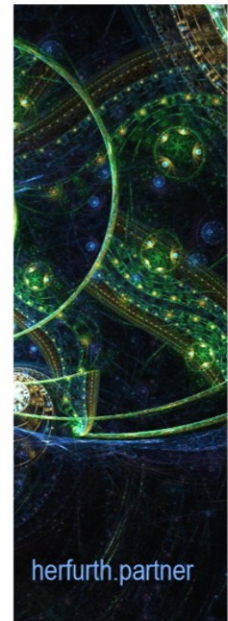
- Automatic generation of **contracts** in the mass business (Smart Contracts), partially only execution
- tamper-proof **documentation** with blockchain technology
- electronic **conciliation** procedures for claims in eCommerce (eBay) instead of state court proceedings (*Softlaw*)
- **Medical** diagnosis through image recognition and analysis of laboratory data, animal and plant diseases, disease control



herfurth.partner

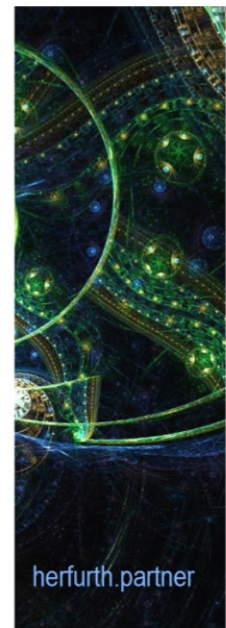
Applications and Markets

- Intelligent **building** control (Smart Home) for energy, air conditioning, ventilation, lighting and sun protection, supply of media and waste disposal, security systems and access controls
- **Urban** supply (Smart City): energy supply and consumption, mobility and traffic control of private transport and public transport, waste disposal, emergency systems, e-government
- Autonomous driving in **traffic** by intelligent and connected cars that are able to find their way, with appropriate response to traffic situations to avoid accidents, damage and injury.



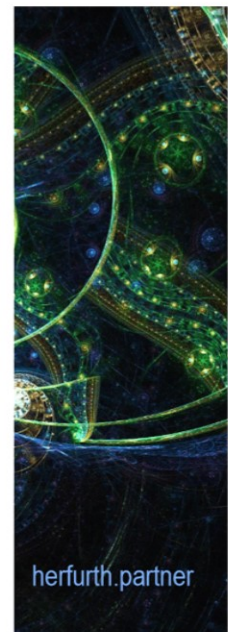
Applications and Markets

- Networked **production** under industry 4.0 (*integrated industry*): Machines and systems not only perform predefined tasks, but also communicate and react to changes in their digital community on an ongoing basis.
- Monitoring and optimization of **processes** up to early detection and automatic supply of requirements (*predictive maintenance*)
- **military** warfare in cyberwar scenarios and autonomous weapon systems



Applications and Markets

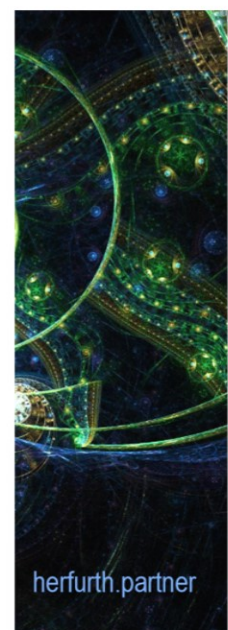
- Race for AI developments in the **economy** and between **states** to achieve strategic and geopolitical advantages.
- The USA and China are the most important players, with Europe and Germany lagging far behind - albeit with special competence in industrial applications.
- Industrial companies and Internet groups are among the largest investors and innovators in the AI



herfurth.partner

AI in State and Society

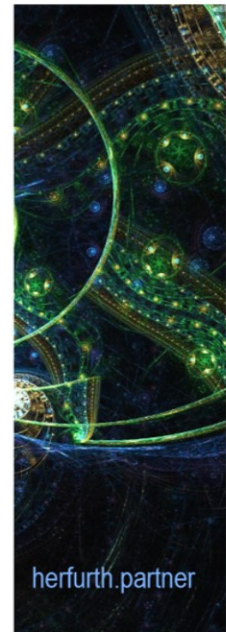
- Artificial intelligence has not only technical or economic, but also ethical, social and legal aspects
- Activities at many political levels, through science, experts and associations



herfurth.partner

AI in State and Society | World

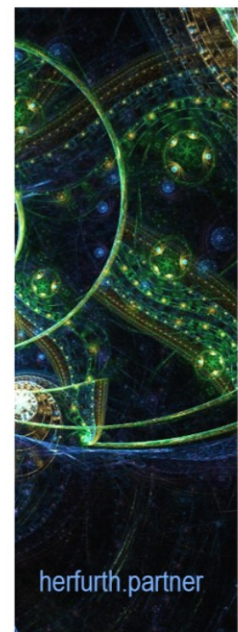
- **United Nations:** United Nations International Crime and Justice Research Institute (UNICRI), Centre for Artificial Intelligence. Potential of technological innovation for productivity growth, at the same time the need for regulation.
- **OECD:** Going Digital Project, Legal Issues of Autonomous Systems. Principles for the development of AI systems following the model of data protection principles, Japan. Ministry of the Interior, draft for such principles.
- **G7:** Takamatsu Declaration on the Promotion of Artificial Intelligence and a Look at the Framework Conditions



herfurth.partner

AI in State and Society | Europe

- **EU Parliament:** civil law issues of robotics, development of new liability systems / liability funds for robots, "e-person" with legal status or legal capacity
- **EU Commission:** adequate liability rules for the Internet of Things and autonomous systems (e.g. in "Strategy for a Digital Single Market for Europe")
- **EU Commission:** Europeans Commission's High-Level Expert Group on Artificial Intelligence: Ethic Guidelines for a trustworthy AI"
- **EU Commission:** „Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics"
COM 2020, 64 final



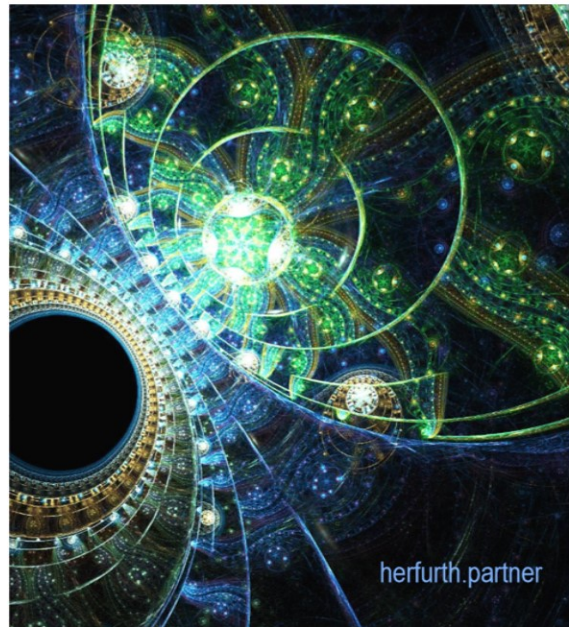
herfurth.partner

AI in State and Society | Germany

- **Bundestag:** "small inquiry" on the potential of blockchain and distributed ledger technologies (Nov 2018)
- **Federal Government | BMJ:** Proposal on Liability for Software, Proposal on Regulation of Algorithms
- **Federal Government | BWi:** Establishment of the Commission Competition 4.0, examination of effects of algorithms
- **Ethics Committee:** Guidelines for Autonomous Driving and Conflict Cases
- **Monopolies Commission:** Examination of the effects of algorithms as price information systems in antitrust law
- **Commission Competition 4.0:** Opinion on new economic images and competition

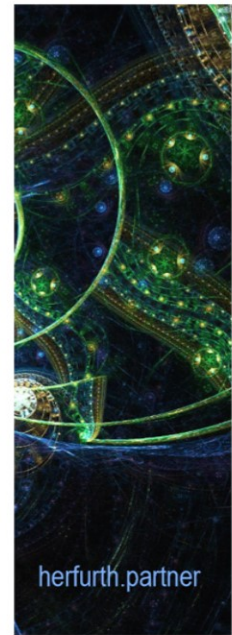


AI in the legal framework

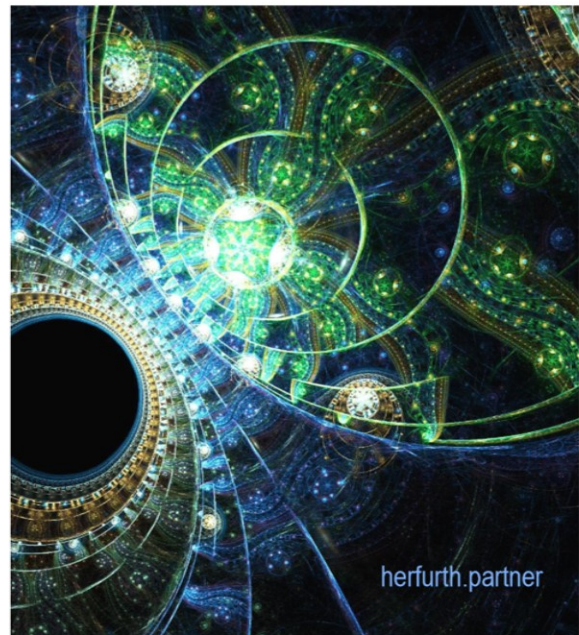


AI in the legal framework

- contracts
- liability
- data protection
- Intellectual property
- management liability
- competition law
- regulatory
- legal personality
- ethics

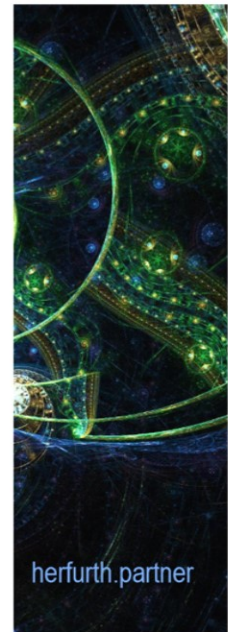


[1] Contracts



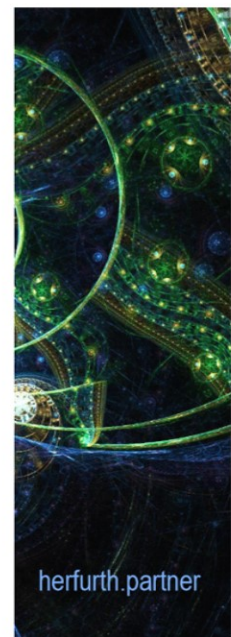
Contracts with AI

- If data transmission is to trigger rights and obligations, it must be possible to create a binding legal basis even without a human declaration of intent
- "Machine declarations" are attributed to the owners/operators of the machines/systems, because they act within the framework of the specified decision-making channels
- Attribution not as representative, but as machine agent



Contracts with AI

- However, AI develops its own decision patterns, not determined by the operator and possibly not expected by him.
- There is no longer operator's consciousness, a will to declare and a business will to classify the action as his declaration of intent?
- "Business declaration" instead of declaration of intent as a new form such as *text form* and *electronic signature*?
- Attribution of the legal consequences according to the principle of legal liability? As a tolerated proxy?
- Errors and misstatements be handled in analogy to the rules for human declarations of intent?

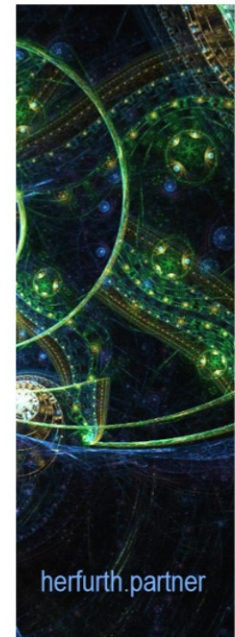


Contracts | Smart Contracts

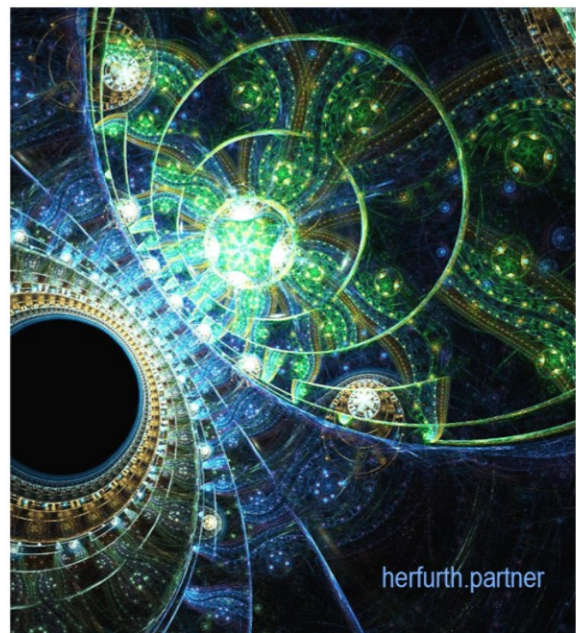
typical consideration is a payment in digital currency
However, in the absence of a factual or legal characteristic, it is not a disposition but an act of fact which does not change the legal situation.

Blockchains are merely a protocol of actions, in particular the submission of declarations of intent and do not make any legal assessment.

smart contracts can only represent agreement in the sense of § 929 BGB on the material side (transfer of rights / transfer of title).

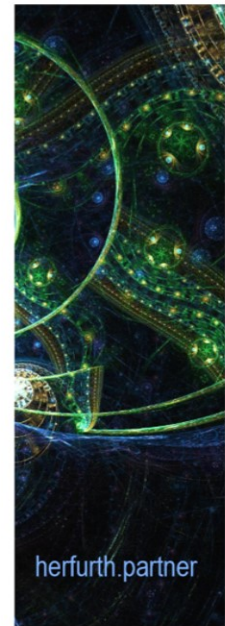


[2] Liability



Liability for AI | Contracts

- Contractual liability probably according to the same principles as for analogous contracts
- System faults are hardly a case of force majeure, (even damage due to short power failure can generally be avoided)
- Obligations and duties of care as in analogous contracts, e.g. inspection of incoming goods according to § 377 HGB with the help of AI-supported inspection systems



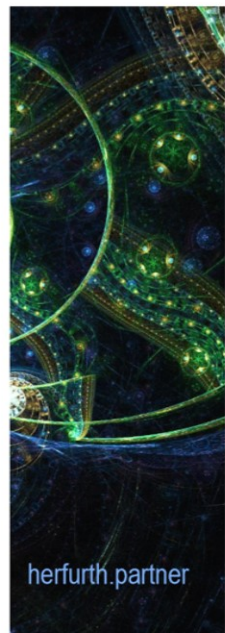
herfurth.partner

Liability | Contracts

Contract liability: If an autonomous system of one contractual partner damages the other contractual partner within the contract initiation or execution >> contract liability according to §§ 280 ff. BGB (German Civil Code)

Presumption of fault § 280 I S.2 BGB and strict liability standard § 276 BGB: whoever uses an autonomous system for the fulfilment of his duties has to represent damages caused by it.

Exclusion of liability only if the damage is not based on a functional defect of the system, but on a solution problem of the autonomous system which is unpredictable according to the state of the art >> possible impossibility § 275 BGB (German Civil Code)



herfurth.partner

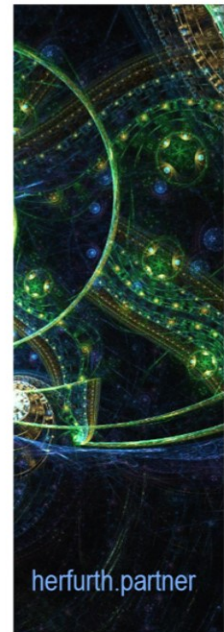
Liability | Contracts

Autonomous system as vicarious agent within the meaning of § 278 BGB
>> is rejected.

Autonomous system with extensive interpretation still term of the
vicarious agent, but no own fault

no deliberate control of one's own actions, ability of AI to act
autonomously is based in the result on the will of the developer or user.

No own legal capacity of the AI



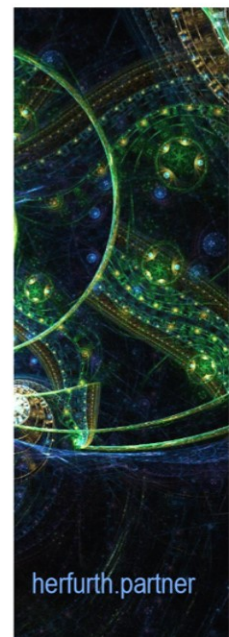
Contracts | Smart Contracts

Error in the submission of automated declarations of intent

Incorrect software: irrelevant error in motif or calculation → no
right to contest

Operating error: contesting possible (similarity to prescribing,
promise) → even if declaration is entered correctly but passed on
incorrectly by faulty software

Error of the device: Incorrect transmission by a used device, § 120
BGB applicable



Contracts | Smart Contracts

Error in the submission of automated declarations of intent

Blockchains = unchangeable chain of transactions that cannot be corrected afterwards.

Blockchain maps actual events, no legal valuations.

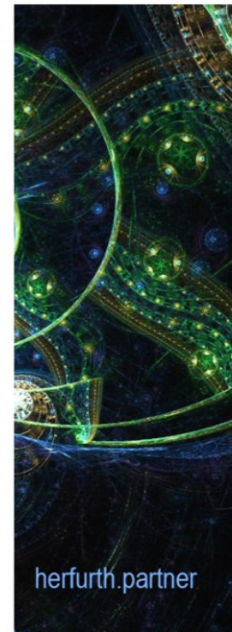
smart contract may not be assumed to be legally effective without further ado, only that the parties have made declarations of intent aimed at these provisions.

smart contract can no longer exist (other than logged) for reasons of nullity, without this being apparent from the blockchain.

But German right of rescission: rescission works ex tunc.

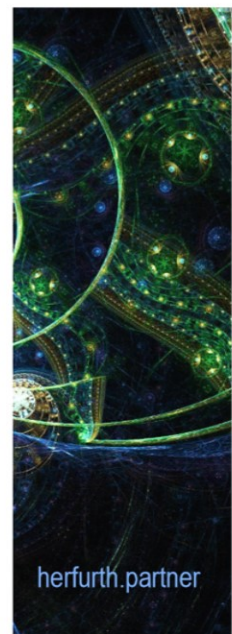
Approaches:

Declaration of rescission can be registered as a separate block



Liability for AI | Crime

- Liability in tort if the controller of the system intentionally or negligently causes injuries / damages
- Negligence raises the question of changed standards of diligence in largely autonomous systems.
- In view of the dynamic development, norms and standards can hardly be the yardstick for this anymore.

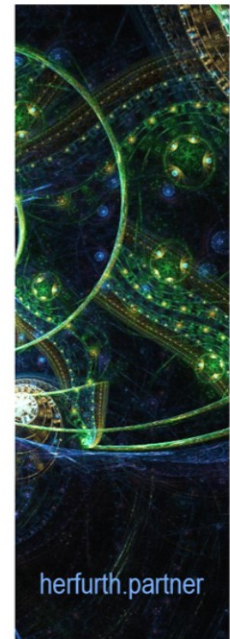


Liability | Fault

Non-contractual liability based on fault:

Liability risks occur when using AI, especially with regard to the legal interests protected by § 823 I BGB (German Civil Code)

The legal duty to maintain safety of manufacturers and operators plays a decisive but problematic role in this context.



Liability for AI | Hazard

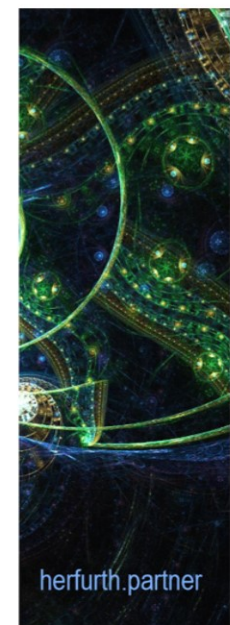
- Strict liability in tort if the system causes injuries / damage through no fault of its controller

Models:

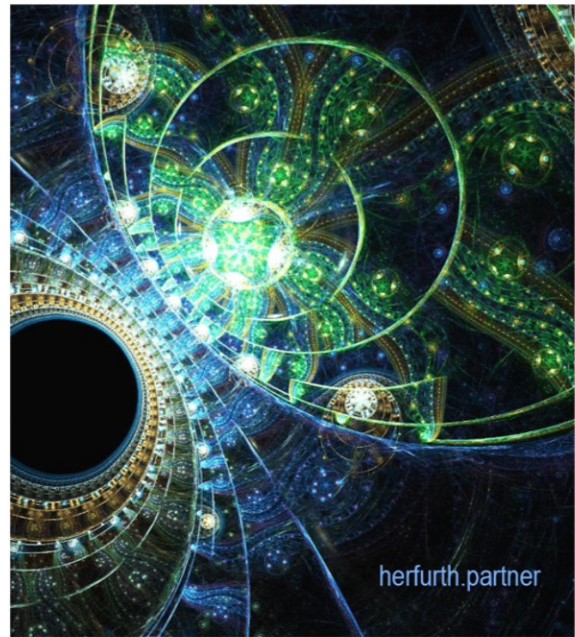
- Product liability of the manufacturer
- owner's / holder's liability for the vehicle
- Liability of the owner of the property for disturbance
- Animal owners liability

Adhesive medium:

- Owner, holder, operator, supplier?
- Operator with rights of recourse against supplier?

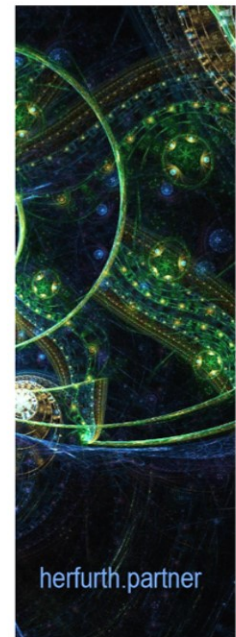


[3] data protection

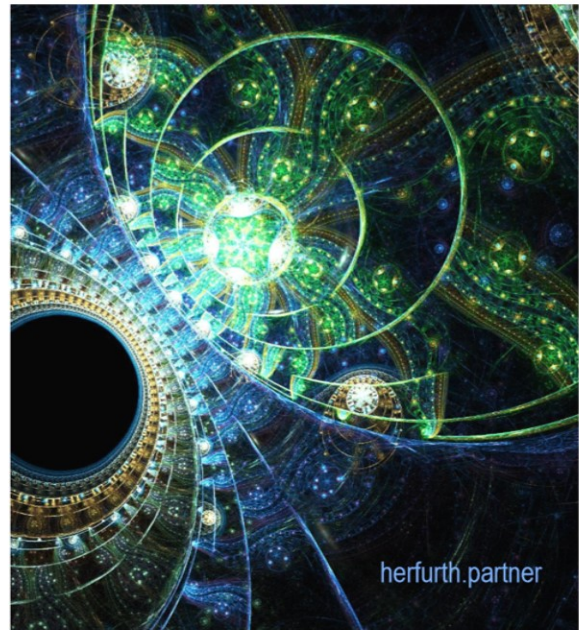


data protection

- in principle the same questions as before
- Personal data may not be processed without further ado, but anonymized or pseudonymized data without allocation to persons may already be processed.
- AI-supported systems can assign data from the aggregation of anonymous data sets to individuals with sufficient certainty, if necessary.
- Machine data becomes personal data again and is subject to data protection.
- Vulnerable to cybercrime, as a strong (autonomous) AI could eliminate security measures. This could only be solved by programming rules, which would limit/prevent the AI's autonomy and openness

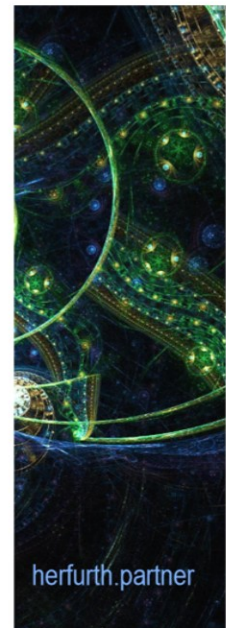


[4] Intellectual Property



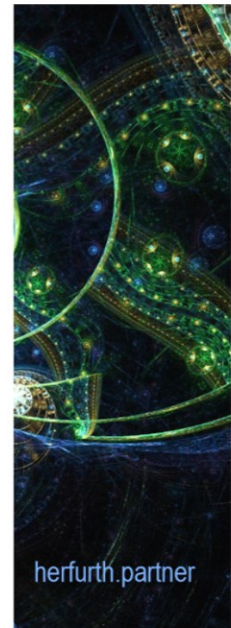
AI and Intellectual Property | System

- Copyright: AI is intelligent systematics, but usually no quality of a work creation (as with software, if applicable)
- Database protection: usually no database under copyright protection as software or investment
- Patent: like software, not patentable as a technical invention unless embodied in a technical product.



AI and Intellectual Property | System

- Trade secret: Whether AI is protected as a trade secret with its (original and then) self-developed processes and specifications depends again on its concrete use.
- Secrecy protection under new European law only if AI is the subject of concrete protective measures.



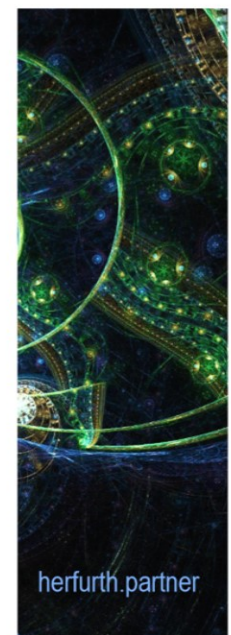
AI and Intellectual Property | System

Setup of AI structures

- (1) Conception of the Artificial Neural Network / Topology
- (2) Selection, processing and feeding of input data
- (3) Training of the ANN (supervised learning, unsupervised learning, reinforced learning) Machine learning (deep learning)

>> Assignment / pattern recognition of data / ANN must evaluate its results

Production of software: explicit indication of methods (codes)
Production of ANN: implicit data, target, not method, set.
(fish and angel)



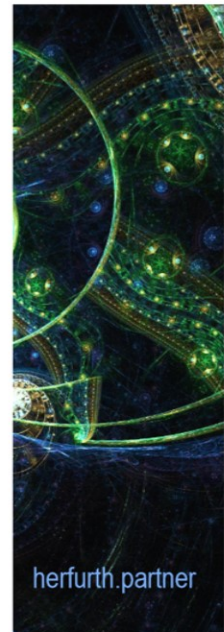
AI and Intellectual Property | System

Software protection for artificial neural networks (69 a Abs.1 UrhG)

Definition of *software* according to WIPO / BGH :

"The finished computer program is defined as a sequence of instructions which, when incorporated into a machine-readable medium, are capable of causing a machine with information-processing capabilities to display, execute or achieve a particular function or task or result".

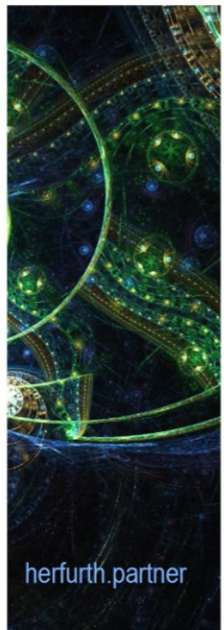
- (1) Programming of the framework (software, mostly open source)
- (2) Topology modeling (may be software)
- (3) Training the network (source code and machine code falling apart, training is machine performance without human intellectual creation? controversial, further development of the term "program"?)



AI and Intellectual Property | Products

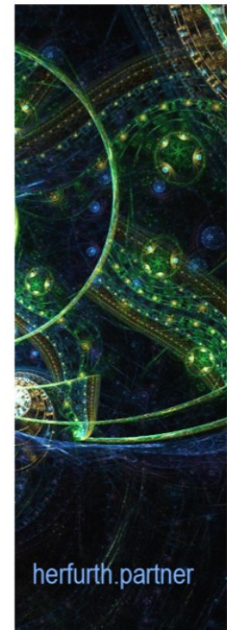
Copyright for Software

- Copyright requires personal, intellectual creation, but AI generates result, people feed only data, no own activity in the concrete production
- Different in England: Copyright also protects computer-generated products (CDPA 1988), law is per investment protection, protection is granted to the person who has taken the necessary precautions.



AI and Intellectual Property | Products

- protectable intellectual property on results produced by AI (e.g. analysis results, other "creative" works such as music, texts, images, software) ?
- Copyright: Machine analyses with AI do not fall under copyright protection. For creative works, the creator (composer, author, photographer, software developer) may use sophisticated instruments - as long as he has a decision on the design of the work, the result may be protected by copyright.
- Pure machine creations not protected de lege lata, new protection de lege ferenda ?

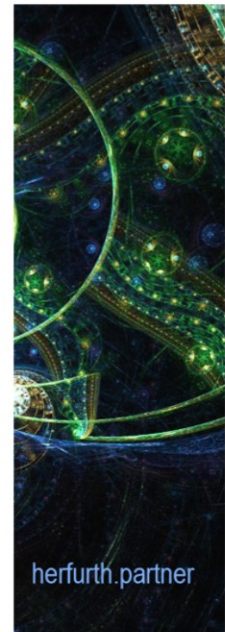


[4] Competition



AI in Competition Law | Merger Control

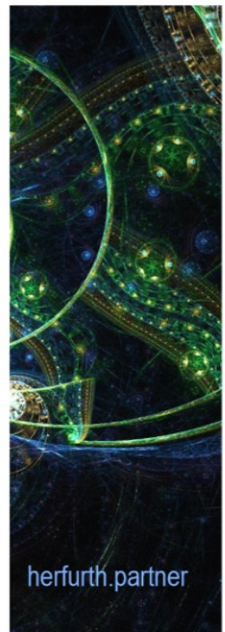
- powerful companies pursue strategic acquisitions of start-ups with potential for new products or as competitors (e.g. Google with Deep Mind /developer of AI for the game GO)
- Merger control has so far assessed the creation of new market power on the basis of the size of the companies in terms of turnover. Information power does not play a role here
- The GWB is now also taking up the criterion of the purchase price for small companies as a trend-setter.
- Merger control: 9th Amendment to the German GWG has introduced Sections 18 (2a) and (3a) ARC, cf. MMR 2019, 711 (714)



herfurth.partner

AI in Competition Law | Abuse of Power.

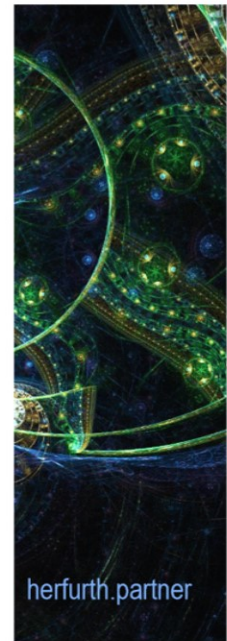
- AI can create highly intelligent mechanisms which, due to their massive information advantage (information asymmetry), result in competitors, customers or suppliers making less favourable arrangements than with a balanced information situation (e.g. if the provider has an information advantage for price formation).
- AI can strengthen the binding effect in software biotopes, networks and on platforms, users accept specifications rather than change to competition (e.g. licence conditions, general terms and conditions, data protection declarations, contract forms /sharing).



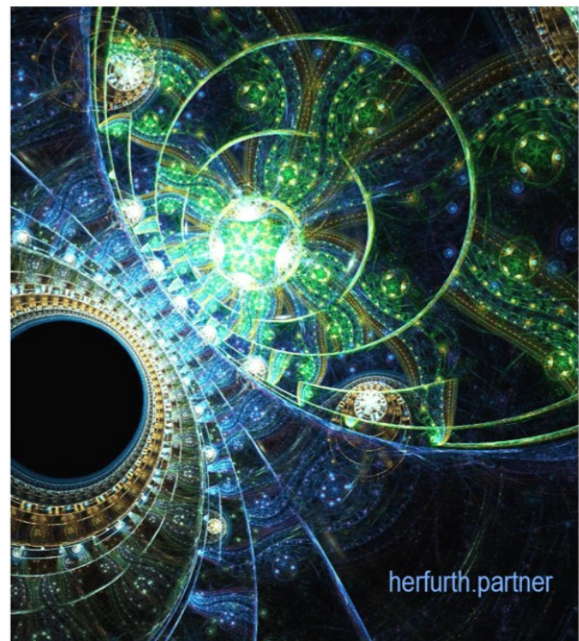
herfurth.partner

AI in Competition Law | Price Cartel

- Algorithms control pricing on the basis of information on demand, interests (e.g. on search engines), social data (place of residence, mobile phone model, buying behaviour), times of day and others (dynamic pricing).
- AI strengthens mechanisms
- If systems react to competitors' prices, this may result in unlawful exchange of information (price cartel).
- Problem: Assignment of the action to persons (not one person reacts to the price information, but an autonomous system).
- Proposal by the Monopolies Commission: the use of algorithms as an illegal exchange of information already in advance

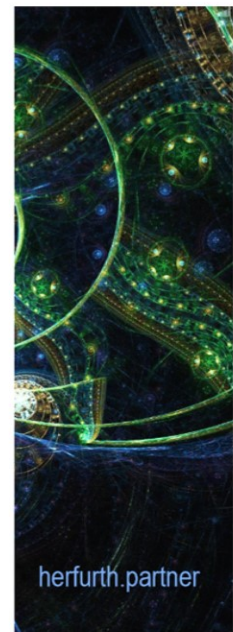


[5] Management



Management Liability

- To what extent are the management and board of directors responsible for the behavior of the systems they use?
- Duty of care to use only those instruments that are technologically safe and do not cause any legal infringements. This also applies to AI-supported systems.
- Responsibility and, if applicable, liability of the organs of the company in the event of infringements of rights and damages.

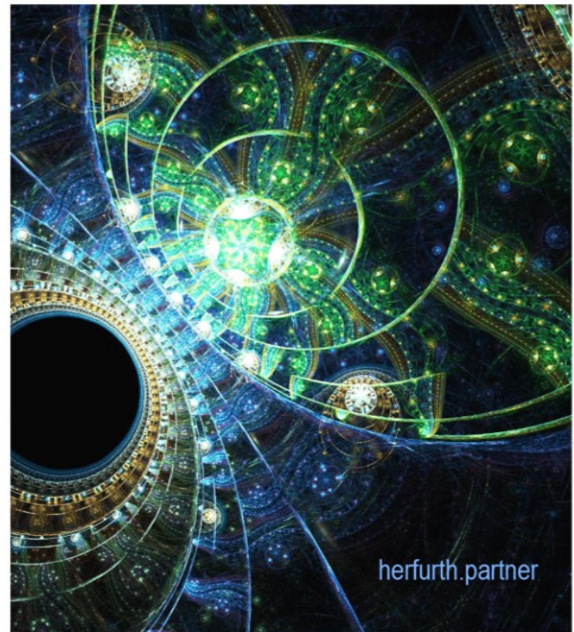


Management Liability

- To what extent may management and board of directors rely on AI in their business judgment rule decisions?
- AI is an advantage as an auxiliary instrument, but management must not transfer decision making to technology alone and thus cannot shift its responsibility for the company onto it.

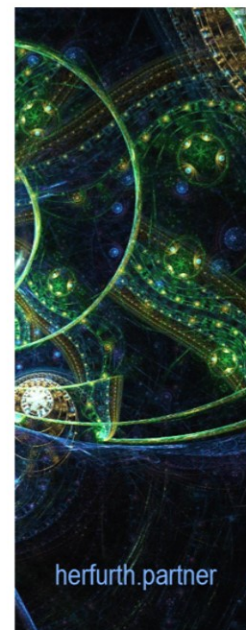


[6] Regulatory

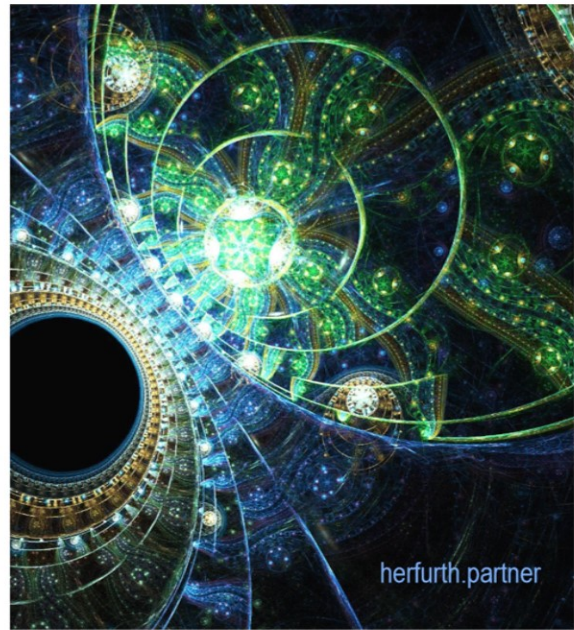


Structural classification of AI systems

- many legal discussions on the structural classification of AIs in regulated areas:
- Does a generator for contract texts provide a legal service?
- May soft law, supported by AI, take the place of state courts?
- Can the public administration have its discretionary decisions made by AIs?
- Are Robo Advisory platforms subject to financial supervision?
(The same supervisory obligations apply as for "analogous" investment advice, see BKR 2020, 181 (186)

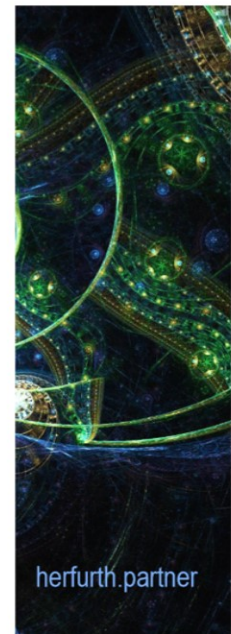


[7] Legal Entity



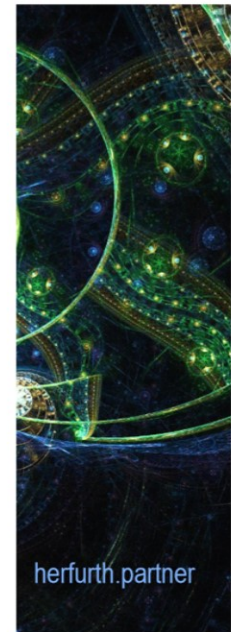
Legal Personality of AI

- Robots are a thing, for intangible systems as such no legal classification
- simple machine data without allocation, for example in the sense of data ownership
- Should robots and AI systems be given legal personality? E.g. as an electronic person (ePerson)?
- Not unthinkable, e.g. in analogy to foundations as legal entities without owners.

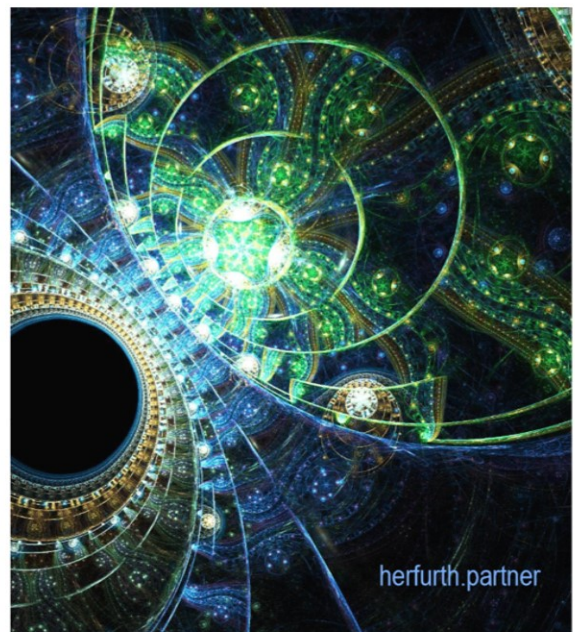


Legal Personality of AI

- Legally, a new form of encapsulation of liability is not necessary, liability for an AI system can also be isolated via corporations such as GmbH, AG and foundation.
- A far-reaching decoupling of damage and liability does not appear desirable from the point of view of prevention.
- Independent responsibility of machines without the ultimate responsibility of human beings is ultimately a fundamental ethical question.

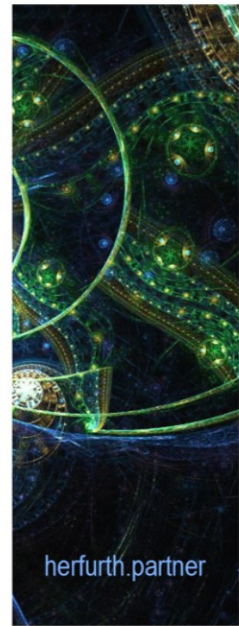


[8] Ethics



AI and Ethics

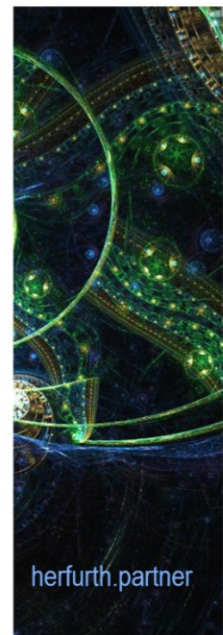
- Many of the legal issues raised by AI new facts can only be considered from an ethical perspective:
- May there be an identification of people in mass proceedings, e.g. by facial recognition, without their consent?
- Does the human being have to be able to recognize them in dialogue with AI? Do unidentified social bots violate fundamental rights and human dignity in dialogue with people?
- How must the system decide between several threatening damages in a dilemma?



herfurth.partner

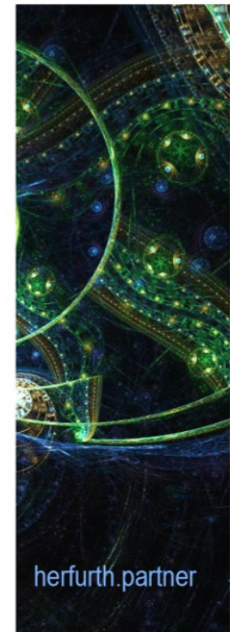
AI and Ethics

- Are autonomous systems, in particular medical diagnoses, autonomous vehicles and autonomous weapon systems allowed to decide on people's lives?
- Ultimately, it is a question of whether machines may use their functionally similar or even superior capabilities only in the service of man, or whether they may be given a rank legally comparable to that of a human being.



herfurth.partner

Let's stay human.



Contact & Literature

Contact us

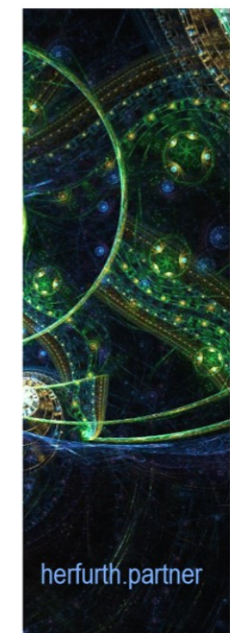
Ulrich Herfurth
Herfurth & Partner
Rechtsanwaltsgesellschaft mbH
Luisenstr. 5, 30159 Hannover

Tel 0511 – 307 56 (0)
Mail herfurth@herfurth.de
Web www.herfurth.de



Literature

Literaturverzeichnis:
redaktion@herfurth.de



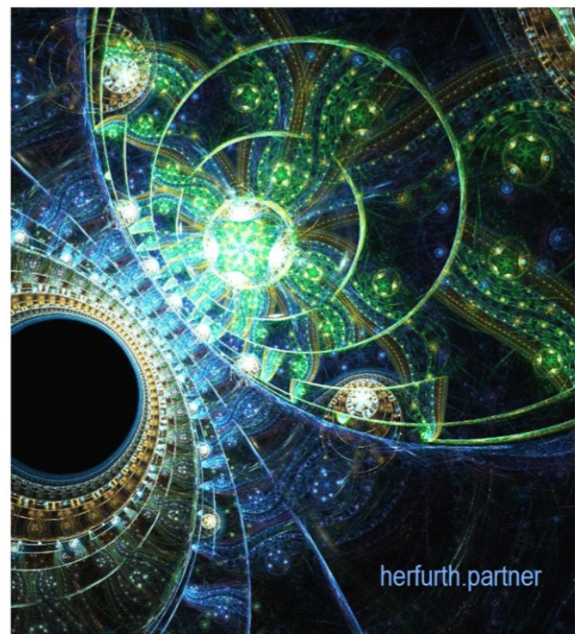
COPYRIGHT BY
Herfurth & Partner
RECHTSANWALTS
GESELLSCHAFT MBH
HANNOVER
GÖTTINGEN
BRÜSSEL
LUISENSTR. 5
30159 HANNOVER
FON 0511 307 56-0
FAX 0511 307 56-10
info@herfurth.de
www.herfurth.de

MEMBER OF
ALLIURIS
ALLIANCE OF
INTERNATIONAL
BUSINESS
LAWYERS
BRUSSELS
LONDON
PARIS
AMSTERDAM
AMERSFOORT
LUXEMBURG
LYON
MADRID
BARCELONA
LISBON
MILAN
DUBLIN
COPENHAGEN
HANOVER
GÖTTINGEN
ZUG
VIENNA
SALZBURG

NEW YORK
MEXICO CITY
SAO PAULO
RIO DE JANEIRO
BRASILIA
BUENOS AIRES
MOSCOW
MINSK
ATHENS
ISTANBUL
BEIJING
SHANGHAI
GOUNGZHOU
NEW DELHI
MUMBAI

herfurth.partner

[X] more details ...



Contracts | Declaration of intent

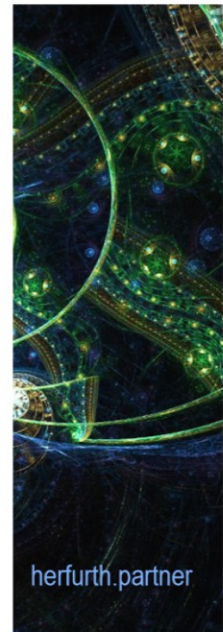
Legal theory needs further development in order to be able to record autonomous systems, declarations of intent can so far only be made by natural persons.

Solution approaches:

The possibility of adapting the law through a concept of "partial equality" between machines and people.

Example: U.S.-Bundesbehörde für Straßen- und Fahrzeugsicherheit equates autonomous vehicles with the "driver" within the meaning of road traffic law.

a.A. Heckelmann: Beermats and tattoos can announce legal will, why not then also intelligent systems?



herfurth.partner

Contracts | Declaration of intent

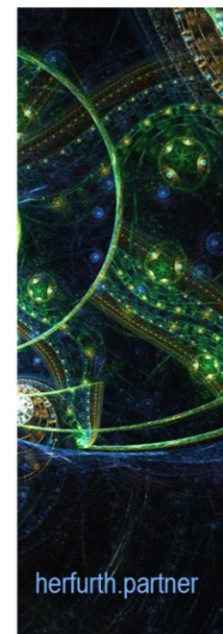
Attribution of machine actions:

Autonomous systems sometimes act only indirectly autonomously in the form of design decisions, so they lack a predictable individuality → To whom to attribute?

Solution approaches:

To refuse analogous representation with regard to the liability of falsus procurator: As a rule, computer systems do not have any liability assets within the meaning of § 179 BGB and no legal personality.

General attribution: anyone who uses an assistant or a risky procedure in order to benefit from it must also bear the associated consequences → is based on several legal bases: e.g. §§ 278, 31, 166 I BGB (German Civil Code)



herfurth.partner

Contracts | Declaration of intent

Attribution of machine actions:

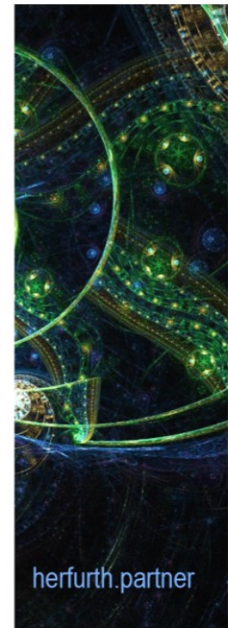
messenger: Solution also by means of regulations of messengership: act just like machines as intermediaries of declarations of intent → The principal bears the risk

New Attribution Subjects:

→ However, intelligent systems can independently determine the scope of delivery, delivery time or price themselves, which is why their actions go beyond messengership.

The more independent a system acts, the more general and imprecise the user's idea of the final explanation becomes. In such a case, no attribution, but fiction of the business will.

Heckelmann: The more autonomous a system, the less its actions can be attributed to the user and the more to the programmer.



herfurth.partner

Contracts | Smart Contracts

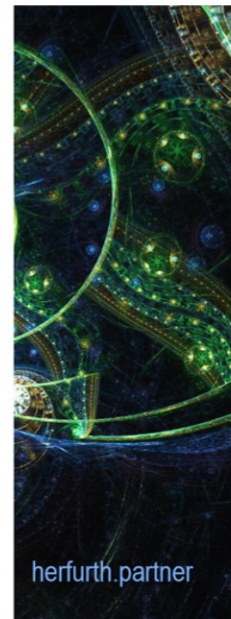
AGB control of Smart Contracts

Are smart contracts at all AGB's?

Often it is not clear which side has introduced the clause, as it is based on the free decision of the parties involved.

Smart contracts can be designed much more flexibly than traditional paper-based forms.

In the case of smart contracts that are generated dynamically according to the user's specifications (e.g. by means of various fill-in variants), content control according to §§ 305 et seq. of the German Stock Corporation Act (Aktengesetz - AktG) is the only option. BGB out



herfurth.partner

Contracts | Smart Contracts

Contract typing / Problem:

Contractual commitments (especially smart products) can often not be assigned to a single contract type. This causes problems in particular with the general terms and conditions control (for this it would have to be clear which contract type should be deviated from).

Solution approaches:

Acceptance of a **mixed type contract**:

Combination theory: different opposites have to be resolved according to the will of the parties.

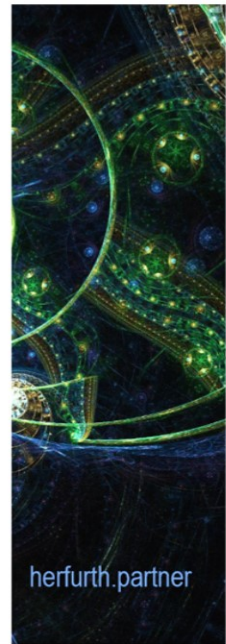
Absorption theory: Which type of contract dominates, which regulations are primarily applicable?

-Reform of the general terms and conditions law for business legal transactions:

e.g. abolition of the indication effect of §§ 308, 309 BGB i.R.d.

inappropriateness examination of § 307 II BGB

the possibility of defining primary and secondary obligations, without these being rejected by the case-law



herfurth.partner

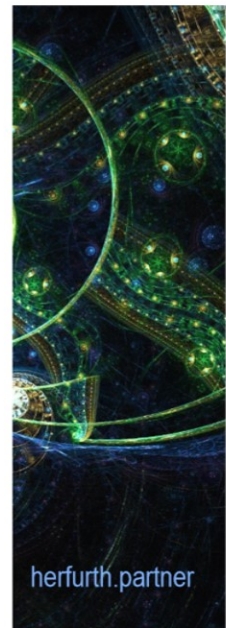
Contracts | Smart Contracts

Error in the submission of automated declarations of intent

Incorrect software: irrelevant error in motif or calculation → no right to contest

Operating error: contesting possible (similarity to prescribing, promise) → even if declaration is entered correctly but passed on incorrectly by faulty software

Error of the device: Incorrect transmission by a used device, § 120 BGB applicable



herfurth.partner

Contracts | Smart Contracts

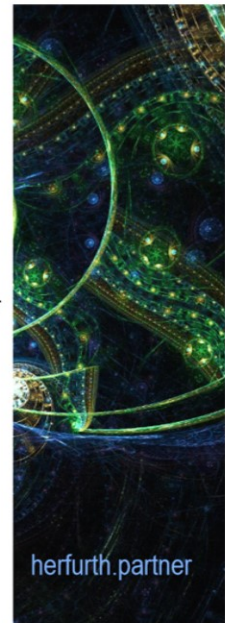
Error in the submission of automated declarations of intent

Blockchains = unchangeable chain of transactions that cannot be corrected afterwards.

- Blockchain maps actual events, no legal valuations
- smart contract may not be assumed to be legally effective without further ado, only that the parties have made declarations of intent aimed at these provisions.
- smart contract can no longer exist (other than logged) for reasons of nullity, without this being apparent from the blockchain.

But German right of rescission: rescission works ex tunc.

Solution approaches: Declaration of rescission can be registered as a separate block



Liability | Hazard

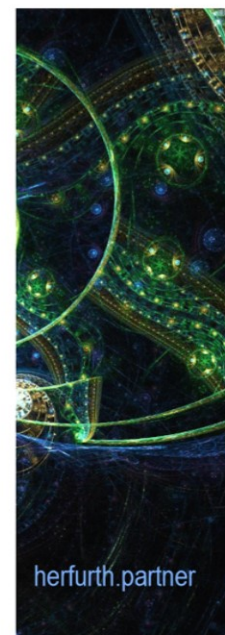
Liability of the operator

For the operator unforeseeable actions of an AI not decisive. Road safety obligations: anyone who accepts an increase in risk through the use of an AI must comply with road safety obligations.

Criticism: AI with strict liability

But: the use of autonomous systems creates obligations, e.g. defining the scope of use, monitoring activities, intervening in the event of malfunctions. In case of breach of duty individual fault of the operator.

Consideration: Reversal of the burden of proof similar to product liability of the manufacturer due to the injured party's inability to inspect the proceedings within the sphere of the injuring party



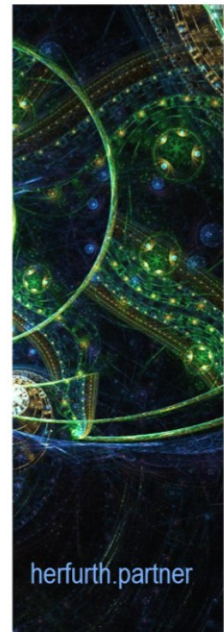
Liability | Manufacturer

Manufacturer's liability

The operator's road safety obligations can be transferred to the manufacturer's sphere under adjustments. Extensive testing before the product is placed on the market to control behaviour that is difficult to predict.

Manufacturer's liability for damages

- depends on his knowledge of the fault before placing it on the market
- After placing on the market Product monitoring obligations.
>> product risks occurring later are no construction errors, but development errors



herfurth.partner

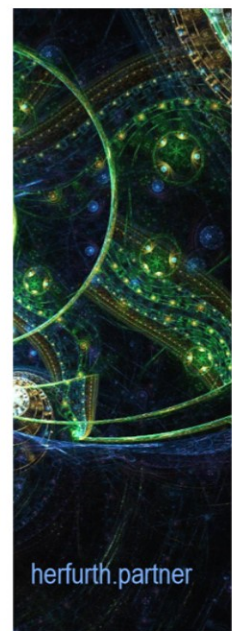
Liability | Hazard

Liability of the operator

For the operator unforeseeable actions of an AI not decisive. Road safety obligations: anyone who accepts an increase in risk through the use of an AI must comply with road safety obligations.

However, the use of autonomous systems creates obligations, e.g. determination of the scope of use, monitoring of activities, intervention in the event of malfunctions. In case of breach of duty individual fault of the operator.

Consideration: Reversal of the burden of proof similar to product liability of the manufacturer due to lack of possibility for the injured party to inspect the processes within the sphere of the injuring party.



herfurth.partner

Liability | Manufacturer

Manufacturer's liability

The operator's road safety obligations can be transferred to the manufacturer's sphere under adjustments. Extensive testing before the product is placed on the market to control behaviour that is difficult to predict.

Manufacturer's liability for damages

depends on his knowledge of the fault before placing it on the market
Product monitoring obligations after placing on the market.

When complying with the road safety obligation before placing on the market

>> product risks occurring later no construction errors, but development errors if necessary



herfurth.partner

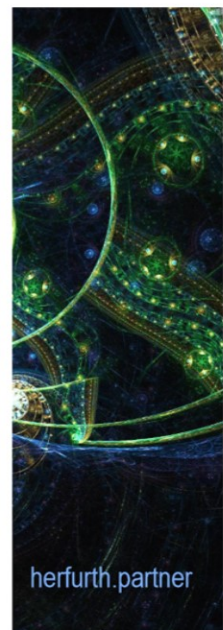
Liability | Manufacturer

Manufacturer's liability

Liability of the manufacturer if he should have identified the risks within the framework of a product monitoring system and rectified any errors.

Proof problems >> Autonomous systems with black box, which stores data and is to be issued in the event of damage to preserve evidence.

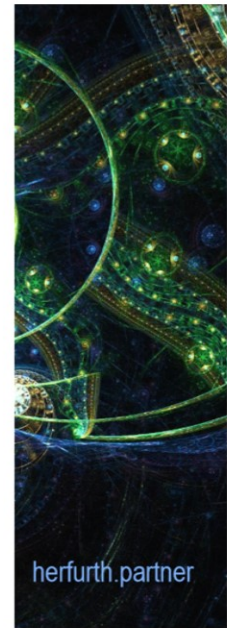
Whether damage is due to errors in the software or defects in the machine only affects the internal relationship between manufacturer and part manufacturer or IT supplier (possibly recourse claims).



herfurth.partner

Liability for AI | Insurance

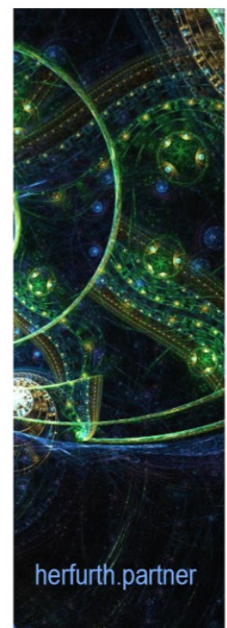
- Insurance as voluntary insurance (business liability, product liability, financial loss liability) ?
- Compulsory insurance with direct claim of the victim (health, life, property, assets) ? Liability funds as a state or private solidarity system?
- Also for e-person?
- Risk problem: significantly fewer loss events, but significantly higher serial losses Liability without deductible of responsible persons would impair preventive effect



AI and Intellectual Property | System

Database protection according to § 87a UrhG

No database protection (as investment protection), neurons are not independent of each other and isolated worthless



AI and Intellectual Property | System

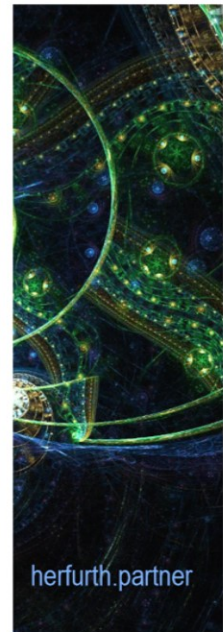
Patent Law

Requirements for patent: invention in the field of technology, new, commercially usable. Problem of technicality (is AI technical or non-technical ?)

complex algorithms and mathematical methods used by computer programs do not solve technical problems, are not patentable (Rspr), often only parts of the AI / ANN are patentable, because too many components; too high patent density, hardly comprehensible traceability of AI products to certain patents possible

Example: Simulators: can still be seen as technical problem solvers if, for example, engineering activities are simplified as a result.

Patent protection possible if the process flow is determined by technical conditions outside the data processing system (e.g. embedded software)
(patents protect invention for 20 years, copyrights up to 70 years after death of the author)



AI and Intellectual Property | System

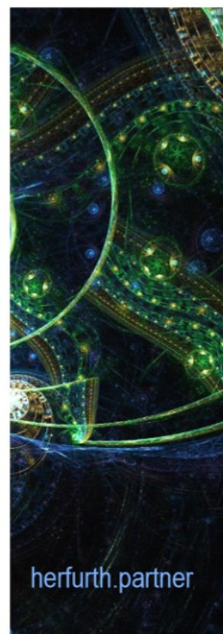
Discussion per patent protection:

Opinion: AI should rather be protected according to patent law in order to facilitate research (assumption that the ground for protection of copyrights (honouring the creator, recognition of his achievement) would not be transferable to AI here)

AI as a tool for inventors, therefore PatG applicable (but AI is often more than a tool)

concrete method of creation of an invention should be irrelevant for patentability of the product, patents only protect the result but many products become patentable, products which are created without human intervention are not patentable (Rspr);

Compromises: either landmark case law or new possibilities to apply for patents (adapted to complex AI)



AI and Intellectual Property | Products

Copyright for database (§ 87a UrHG)

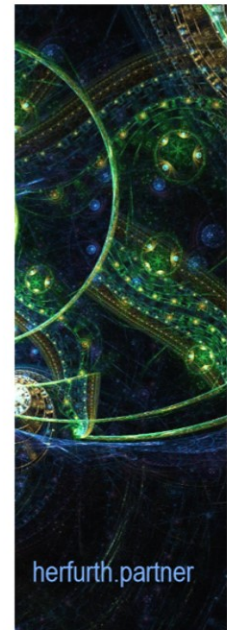
CIIs do not collect data in order to create databases, but CIIs develop a different product from them - Scope (-)

Independence of data: Data is not only analyzed and ordered, but other results are generated from it; however, elements must be separable.

Who is an investor? Programmer? Users?

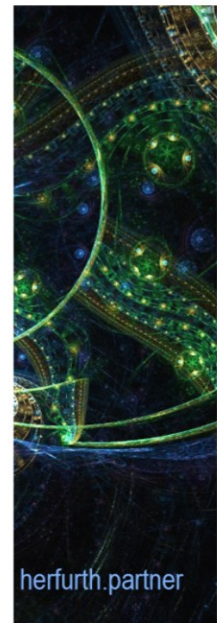
The scope of protection for databases sui generis under database manufacturer law is very broad "First databases" have monopoly positions;

Only the database is protected, not the content difficult to apply to AIIs



AI and Intellectual Property | Products

- Protection for database investment § 87a UrHG ?
- Not about UrhG because they are the product of an automated process, personal intellectual creation lacks
- § 87a UrhG does not link to intellectual creation, however, the individual information of the synapses are not "independent" from each other in the sense of the provision due to the lack of independent information value, meaning of content results only from the context of the network.



AI and Intellectual Property | Products

Patent Law

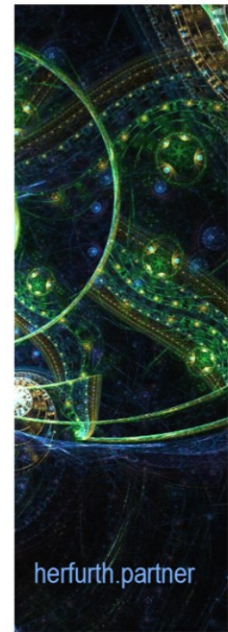
Inventor's claim, as a rule goal, if he created AI and patented software

Reach-through, research tools or product-by-process requirements conceivable

Patent claims but not extendable to results/products

§§ Sections 9 S.2 No. 3, 139 III PatG? However, here no concrete results are available, but only the abstract recognition of the creative ability of the AI

Consequence: concealment of the use of AI in the development process?



herfurth.partner

AI and Intellectual Property | Products

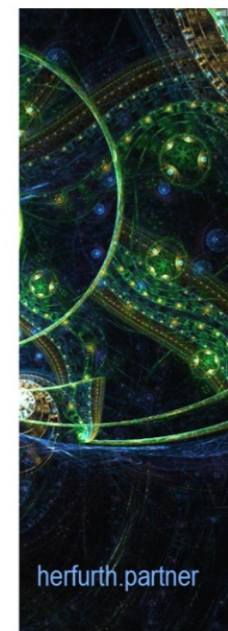
Patent Law

introduce legal personality for AI, as otherwise there is no real act of man which could become the basis for a patent?

does AI act creatively? Vss.: Systems with autonomous, unpredictable products that cannot be attributed to any human being.

Differentiation between autonomous and automated action difficult for patent office to separate; yardstick? How is the current state of the art to be assessed?

If AI is accessible to everyone, products become obvious and are no longer patentable -> will affect intellectual property rights in the future



herfurth.partner

Contact & Literature

Contact us

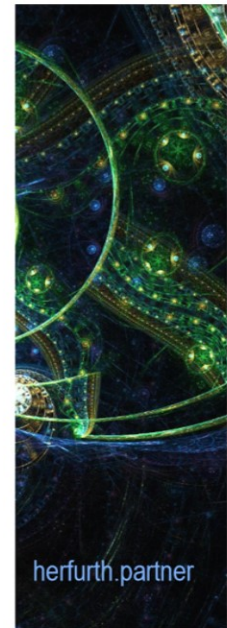
Ulrich Herfurth
Herfurth & Partner
Rechtsanwaltsgesellschaft mbH
Luisenstr. 5, 30159 Hannover



Tel 0511 – 307 56 (0)
Mail herfurth@herfurth.de
Web www.herfurth.de

Literature

Literaturverzeichnis:
redaktion@herfurth.de



Herfurth & Partner
RECHTSANWALTS
GESELLSCHAFT MBH
HANNOVER
GÖTTINGEN
BRÜSSEL
LUISENSTR. 5
30159 HANNOVER
FON 0511 307 56-0
FAX 0511 307 56-10
info@herfurth.de
www.herfurth.de

**MEMBER OF
ALLIURIS**
ALLIANCE OF
INTERNATIONAL
BUSINESS
LAWYERS
BRUSSELS
LONDON
PARIS
AMSTERDAM
AMERSFOORT
LUXEMBURG
LYON
MADRID
BARCELONA
LISBON
MILAN
DUBLIN
COPENHAGEN
HANOVER
GÖTTINGEN
ZUG
VIENNA
SALZBURG
NEW YORK
MEXICO CITY
SAO PAULO
RIO DE JANEIRO
BRASILIA
BUENOS AIRES
MOSCOW
MINSK
ATHENS
ISTANBUL
BEIJING
SHANGHAI
GOUNGZHOU
NEW DELHI
MUMBAI

herfurth.partner

Question & Answers

Artificial Intelligence

1. Are there national rules about AI?

Iv Fangyuan (China):

No

Qiu Shuang (China):

Not yet.

Qiyi Zhang (China):

China now has a basic policy on the development direction of AI, but no specific legal attributes of artificial intelligence. In China, the creation of artificial intelligence is mainly protected by patent law and copyright law.

Eduardo Barrera (Mexico):

Unfortunately not, but there are some sort of knowledge because of “Data Law Protection” and the way they develop their algorithms. Sadly, this law was limited to the territory of the company (Mexico), not like the EU Standard which has to do with the EU Citizens Data around the world.

Rupesh Pandey (India):

The growth of AI and its related technologies is tremendous which also brought the challenges to legislate and implement laws and regulation to bring AI under legal discipline. Tesla and Space X chief executive Elon Musk has warned in 2017 “AI is the rare case where I think we need to be proactive in regulation instead of reactive. Because I think by the time we are reactive in AI regulation, it’ll be too late”.

- **European Union (EU):** Recently, in February 2020 the European Commission published “White Paper on Artificial Intelligence” which proposed a regulatory framework for artificial intelligence. The paper has encouraged to use AI in the field of research and economic activity keeping deals with technological, ethical, legal and socio-economic aspects related to EU. Instead of providing proposed regulations at this stage, the Commission has set out legal requirements that any regulatory framework must cover to ensure that AI

remains trustworthy and respectful of the values and principles of the European Union.

Further, AI system should also be compliant with General Data Protection Regulation (GDPR). GDPR contains various principles, purposes and procedures which must be adhered by AI systems. Under the GDPR, principles and rules applies to the collection and use of personal data to make Organizations more transparent and accountable. AI provider can act as data processor or controller. The organization need to apply all control mechanism and follow rules while applying AI for automated processing as well as during transfer of personal data.

- **United States:** It is surprising to note that there seems to be little activity in US related to AI regulation. There have been few AI reports, pending bills, executive orders and one draft guidelines. President Trump issued the Executive Order on Maintaining American Leadership in Artificial Intelligence in February, 2019 by following five principles. On January 7, 2020 United States released draft guidelines to federal agencies overseeing non-federal entities' deployment of artificial intelligence (AI) applications. The draft proposes ten guiding principles for regulatory and non-regulatory approaches for AI applications.
- **Australia:** Australia released a discussion paper containing principles, governance, data regulation as well as ethical requirements to develop standards to regulate AI.
- **United Kingdom:** UK is one of the country which is emerging as a world leader in regulating Artificial Intelligence. In April 2018, United Kingdom (UK) published national AI strategy entitled AI Sector Deal which envisaged to prepare for the transformations and provides the framework in developing AI technologies. This Deal was further updated in May 2019. In February 2020, UK published Artificial Intelligence and Public Standards wherein it has stated that AI is a new challenge that can be solved with existing tools and established principles.
- **New Zealand:** New Zealand is also on the process to develop National Regulation to deal AI. The need for Legal Framework to control the use of AI was initiated by University of Otago in 2018. Subsequently, in November 2019, the New Zealand Government announced it would examine regulation of AI with the World Economic Forum (WEF). Further, AI Forum of New Zealand has published a set of principles for use of artificial intelligence (AI) in New Zealand which give indication that New Zealand in near future is likely to come up with some concrete national Legislation on AI.

- **OECD:** The OECD Recommendations on AI were adopted in 2019 which identifies five complementary values-based principles for the responsible stewardship of trustworthy.
- **G20:** Similarly, G20 supports the Principles for responsible stewardship of Trustworthy AI and provided note of the Recommendations.

Arthur Horsfall (UK):

In the UK there is no statutory definition of AI, but it has been defined in an Industrial Strategy White Paper.

Coral Yu (UK):

Not any I'm aware of in UK.

Gary Whitehead (UK):

From what I have researched, there is 'guidance' only for use of AI in public sector.

Philippa Kwok (UK):

No specific legal provisions in the UK for the regulation of AI.

Julia Krautter and Patrícia Perinazzo (Brazil):

Not yet. Brazil has a bill being voted) Projeto de Lei 21/2020) that foresees rules, rights and duties for the use of AI.

Alitzel Sánchez Alonso (Mexico):

There is no applicable law for this area.

Luis Roberto Moreno Tinoco (Mexico):

No special rules have been issued regarding AI in Mexico to the present date, so the general regime shall be applied should any controversy arise.

Mari Yoli Wulf Sánchez (Mexico):

No. The current legislation on the protection of personal data focuses on protecting the individual against the unlawful processing of his or her personal data and preventing his or her human dignity and freedom from being affected.

Miguel Ángel Aspe de la Rosa (Mexico):

No.

Nadiezhdá Vázquez Careaga (Mexico):

In Mexico does not exist regulation for artificial intelligence.

Paulina Saldaña Fuentes (Mexico):

A Law that regulates the Artificial Intelligence does not exist in the Mexican legislation. The usage of such must be regulated, as of today, by supplementary regulation and by the courts criteria (jurisprudence)

Ricardo Heredia (Mexico):

No, Government has plans to start regulating and consider AI. However, the most similar new regulation with technology is regarding Fintech.

Fergan Tuğberk İşman (Turkey):

Artificial Intelligence is a form of technology that learns, adapts and grows since their first activation. They are capable of researching and they can create most of the things a human can create such as codes, programs, games or even novels. Currently, there are no official rules about AI in Turkey. On the Global developments United Nations Interregional Crime and Justice Research Institute Centre for AI and Robotics is discussing the place of AI in the modern world.

2. Can AI conclude binding contracts?

Iv Fangyuan (China):

Yes. If the contracts template are reviewed by human beings.

Qiyi Zhang (China):

At present, the artificial intelligence technology is not mature, and there is no precedent of giving legal effect to the behaviour of artificial intelligence. Artificial intelligence, by its very nature, is a simulation of the information process of human thinking. If the thinking mode of artificial intelligence in the future can be similar to or better than that of human beings, and can make rational judgments and behaviours according to specific situations, maybe the contracts signed by artificial intelligence will be given legal effect.

Friederike Ammann (Germany):

No because AI has not got a legal personality

Rupesh Pandey (India):

Contracts are vital for building business relationships and completing transactions. AI is being applied with the contract management system like contract classification, organizing legal data, manage and update of legal and paralegal data etc. Traders are getting benefitted from electronic trading wherein computer technology is acting as the medium for communications between parties. The e-Commerce Directive (EU) provides the legal framework within European Union including "business-to-business" (B2B) as well as "business-to consumer" (B2C) legal relationship.

However, the situation becomes complicated when the contract is initiated, controlled and concluded by AI wherein software code act autonomously to define and draw periphery of the agreement. One emerging example emerging is smart contracts which are a are self-executing arrangements through computers reducing individual human intervention and increasing codification and machine use. The pertinent issue would be the outcome, liability and consequences of such arrangement. First issue would be that globally most of the contract act states that contract can be concluded by natural or Legal person. As on date, AI has no independent legal status. Acting on the same premise, Estonia is working on giving legal status to AI.⁸ Saudi Arabia has first time granted citizenship a Robot who is named Sophia. This is the first time any robot in the world has achieve the citizen status.

Second issue can be the intention and meeting of mind during offer and acceptance by AI to create legal relationship. Third issue can be the enforcement or breach of contract due to the negligence or non-application of concerned clauses applied by AI not envisaged by the master of the business entity. Fourth issue could be the legal relationship between the master/owner of AI and AI itself. Whether AI would act as an independent contractor of an Agent on the instruction and matrix defined by the owner or master. Therefore, if AI has to be given more autonomy and power to conclude contracts then all corresponding challenges must be complied with the legal framework.

Arthur Horsfall (UK):

Whilst electronic signatures and email can be used to enter into contractual relations, under the laws of England and Wales, in order for a binding contract to be created the key elements of offer, acceptance, consideration, intention to create legal relations and certainty of terms must be present. The application of these principles does not depend on the particular technology that is used to create the contract. Therefore, when seeking to contract by electronic means, the parties will need to consider whether the key elements for contract formation are present in the electronic communication or contracting process that is being used.

Coral Yu (UK):

Only if the contract was entered into with some kind of human instruction I think.

Gary Whitehead (UK):

Yes, can assist in identifying key clauses, speed up negotiation and facilitate binding.

Philippa Kwok (UK):

Potentially – e.g. use of smart contracts though the legal enforceability will depend on the type of smart contract and whether the standard elements of a binding paper contract are met

Julia Krautter and Patrícia Perinazzo (Brazil):

No

Luis Roberto Moreno Tinoco (Mexico):

In order to be able to conclude a contract in Mexico, both parties shall have the sufficient legal capacity to do so. Mexican law only grants legal capacity to individuals and legal entities (as long as they satisfied the legal requirements), but has not yet been granted to the software's that derive from the AI.

Thus, AI cannot conclude binding contracts in Mexico.

Mari Yoli Wulf Sánchez (Mexico):

In Mexico, from the perspective of privacy and protection of the user's personal data, these services are often not fully protected by law, but under the very rules of operation of the platform if it is not established in Mexico.

Miguel Ángel Aspe de la Rosa (Mexico):

No legal provision exists in Mexico to this date that establishes that AI has the legal capacity to conclude contracts.

Paulina Saldaña Fuentes (Mexico):

Some law firms have already hired artificial intelligence to draft some contracts. In my personal opinion, the negotiation and signature of any binding contract shall be done in person.

Ricardo Heredia (Mexico):

As long as the AI that is considered doesn't go against Mexican law and regulation it could be possible. However, is hard to determine because there is no exact legal framework for the moment.

Fergan Tuğberk İşman (Turkey):

To conclude a binding contract, the parties must have competency to make a contract and intent on making the contract. Competency requires two mandatory things which are mental competence and legal maturity age.

Artificial Intelligence technology is not a thing that is born but a thing that is created. After their creations, they adapt and learn faster than any human being can do. On this matter, their competency has to be determined and regulated. How can one bring a rule to determine an AI's competency?

There is also the issue of intent of AI for the contract. How can the parties know if the AI is really acting on behalf of its user or creator? Without proper developments or research on these issues, proper regulations cannot be made and without proper regulations, an AI cannot conclude binding contracts.

3. Who is liable for decisions and acts by AI?

Qiu Shuang (China):

I think it includes designers, users and managers

Qiyi Zhang (China):

Because the creation and application of AI are not universal, and the decision and behaviour of artificial intelligence have not become a widespread problem in the society, so there are no laws on the rights and obligations of artificial intelligence in my country. If the popularization of artificial intelligence in the future causes various social problems, laws should be adopted to regulate the production and use of artificial intelligence. Even if human beings have the same way of thinking through technology and can receive information from the outside world, analyse the situation, predict the future, and even possess emotions and emotions, artificial intelligence is a machine and a tool used by human beings. Artificial intelligence cannot replace human beings. I think each AI should be equipped with a human as a “guardian”, who is responsible for the AI’s decisions and behaviour. The guardian may authorize the AI in the form of delegation and be responsible for the AI’s behaviour within the scope of authorization. Of course, there may also be cases involving ostensible, the consequences of which should be the responsibility of the person responsible. Can require artificial intelligence in the design of artificial intelligence when making a decision or behaviour to show the other party authorization, so that the other party to determine the scope of authorization of artificial intelligence, because if the other party under the condition of intent or negligence led to the decision of the artificial intelligence or behaviour caused damage, should be borne by the other party. Of course, the harmful consequences (including but not limited to criminal behaviour, infringement behaviour, breach of contract, etc.) are caused by the designer or manufacturer of artificial intelligence. That is to say, the legal consequences of artificial intelligence decisions and actions should be divided into different situations and borne by the corresponding responsible personnel.

Rupesh Pandey (India):

The technical growth of AI is progressing fast and its regulatory and legal framework has taken the back seat. Drones and self-driving vehicles are vivid examples wherein hundreds of patent application have been filed to own technology, however, the legal control couldn’t keep pace with the same. It is imperative to fix liability from the individual human driver to machine which would control the product or service. European Commission has discussed Liability for emerging digital technologies under existing laws in Europe has stated that the law of tort of EU Member States is largely non-harmonised, with the exception of product liability law under Directive 85/374/EC, some aspects of liability for infringing data protection law (Article 82 of the General Data Protection Regulation (GDPR)), and liability for infringing competition law (Directive 2014/104/EU).

The paper has discussed few proposals to apply legal routes by adopting Operators' strict liability, vicarious liability for autonomous system, insurance, compensation funds etc.

Another challenge would be to apply criminal liability which usually requires action and mental intent. Any criminal law matters require to prove beyond reasonable doubt which would require to judge those who design systems or whether the programmer of the machine knew the probable outcome. Further, the action and mental element need to be analyzed to fix the culpability which can be applied individually or jointly.

Arthur Horsfall (UK):

This is an interesting area, on which the European Commission has recently published a report to see if the existing regimes are sufficient for apportioning liability. There are potentially multiple parties involved such as:

- data provider;
- designer;
- manufacturer;
- programmer;
- developer;
- user; and
- even the AI system itself.

Further complications may arise if the fault or defect arises from decisions the AI system has made itself based on machine learning principles with limited or no human intervention. The current UK liability regimen is causative and fault based. Fault may be very difficult to prove for liability concerning AI. The EC concluded that whilst the current system is sufficient for now it did make recommendations including strict liability, allocation of liability (for manufacturers, producers and operators) and an adapted range of duties of care for operators of emerging technologies.

Coral Yu (UK):

I do not think there are rules about this in general yet. But the UK Department for Transport has been active in reviewing and preparing for the changes in regulation that will be necessary for autonomous vehicles.

Gary Whitehead (UK):

Will depend on the situation / circumstances – could be manufacturer / user

Philippa Kwok (UK):

Potentially:

- Software developers / machine programmers
- Manufacturers

But ultimately depends on the scenario

Julia Krautter and Patrícia Perinazzo (Brazil):

According to the bill mentioned above it will be the AI agent (the professional responsible to develop and operate the system).

Luis Roberto Moreno Tinoco (Mexico):

Since no special provisions have been issued regarding this matter, it should be analysed whether the owner of the software that is deemed as AI can be held accountable for the decisions and acts that were carried out.

Since the AI is not deemed as an independent subject for legal purposes, it is most likely that the responsibility would entirely fall under its owner or designer, who will be obliged to respond before any third party affected by the decisions taken by the AI.

Mari Yoli Wulf Sánchez (Mexico):

It's not clear who is liable.

Miguel Ángel Aspe de la Rosa (Mexico):

The set of rules in Mexico is quite limited with respect to this topic.

Paulina Saldaña Fuentes (Mexico):

As is still not regulated and must be followed by supplementary regulation and regarding what is stated in the Civil Code, the persons who programmed such be, if the case, liable.

Ricardo Heredia (Mexico):

Up to date, with no proper legal framework or regulator, it could be:

- Mexican Institute of Industrial Property -regarding patent issues.
- Civil courts regarding a contractual breach.
- Criminal court, in case a felony is related.

Fergan Tuğberk İşman (Turkey):

AI systems require specific developments. They have to be provided with information about their designated job in order to properly work. When a problem arises from the act or decision of AI, the crew behind the AI's development should be held liable.

Because of being a technology and not having a legal personality, AI's cannot be held responsible for the act of themselves. To determine the liable person more precisely, the AI's development phase must be examined. As they are being complicated technology, the examination must be held strictly. Even a miniscule change may cause the AI to deviate from the desired path.

There is also the factor of outside intervention. If a decision or act was triggered by an outside effect, there may be a case of non-liability of the developers. This outside factor has to be unpredictable and inevitable.

4. **Are creations made by AI protectable by IP?**

Iv Fangyuan (China):

I do not think creations made by AI shall be protected by IP. Because these works created by AI are not original and creative.

Qiu Shuang (China):

Artificial intelligence programs have created a large number of works, including literary works, music works, art works, etc. these works fully conform to the form and substance requirements of "works" stipulated in the copyright law without considering the creator factors. Therefore, special legislation is needed to protect it.

Qiyi Zhang (China):

Intellectual property rights refer to the exclusive rights enjoyed by the right holder in accordance with law to the achievements created by the intellectual labor and the marks and reputation in the business activities. The mainstream research focuses on weak AI, and it is generally believed that considerable achievements have been made in this field. Research on strong artificial intelligence is at a standstill. A weak AI machine just looks intelligent, but it does not really have intelligence, nor is it autonomous. In my opinion, such products created by ARTIFICIAL intelligence are simulated and created on the basis of existing technologies and products without intellectual labor, and such products should not be protected by intellectual property rights. But if in the future, the machine of artificial intelligence, like the mind of thinking and reasoning or artificial intelligence machines and people completely different perception and consciousness, the use and the completely different way of reasoning but conscious, self-aware, created the artificial intelligence has intelligence labor products should be the protection of intellectual property rights.

Rupesh Pandey (India):

AI can play a significant role in the creation of intellectual property. AI is being used exclusively or in collaboration with human to create many artistic things and inventive product and process. The challenge would come to name the author of the work or the inventor of the patent. UK legal system seems to be bit advance and have envisaged the technical growth and contains "computer-generated works" under section 9(3) of the Copyright Designs and Patents Act 1988 (CDPA).

There has been lot of debate regarding the ownership of IP generated by the computer-based technology. In a landmark challenge to the international patent regime, a band of legal experts has called on authorities in the US and EU to recognise

the “inventorship” of artificial intelligence, highlighting growing anxieties among lawmakers about the rise of machines in the creative process.

As the use of AI is getting more widespread and complex, hence the International standard should be taken into account and provision with detailed AI based role need to be incorporated under TRIP, so that national legislation (WTO members) can be amended and implemented uniformly across the globe.

Arthur Horsfall (UK):

Although mathematical models and algorithms are not patentable under the European Patent Convention AI inventions are generally patentable as a subgroup of computer-implemented inventions. However, there must be technical considerations and motivations behind non-technical features that contribute to the solution of a technical problem. The European patent office also refused two patent applications designating AI as an inventor, as an inventor must have their own legal personality.

Coral Yu (UK):

It will likely be problematic with current IP law, in particular when comes to copyright. Accordingly, parties to agreements for the development and use of an AI system that may be expected to result in new copyright works should include appropriate express terms on ownership, assignment and licensing. Same approach should be taken in terms of ownership, assignment and licensing of AI generated inventions and patent rights.

Gary Whitehead (UK):

Not sure but I would imagine so.

Philippa Kwok (UK):

Yes – in the UK, authorship would be given to the programmer, not the machine. Most definitions of ‘originality’ across different jurisdictions require a human author.

Julia Krautter and Patrícia Perinazzo (Brazil):

No, considering the inexistence of a law in force in this regard. In Brazil, besides the doubt about the authorship of the work, the question arises: if there is no author, would this work have copyright protection? This is because the intellectual property law determines, that belongs to the public domain, among other cases, the works of unknown authors. Therefore, that’s one possible conclusion taking into account that the works created by do not have authorship according to the law.

One solution - even if momentary - is to attribute a kind of authorship shared between: creator of AI; the one who operates it; and whoever inserts the necessary information to generate content.

Granting authorship to anyone will be a momentary response, yes, as new challenges will arise as AI evolves and inserts itself into our lives.

Luis Roberto Moreno Tinoco (Mexico):

Mexico has not issued any special provision regarding creations made by AI, so any creation made by the AI will be deemed to be property from its owner or designer, for Mexican IP purposes.

Nadieżhda Vázquez Careaga (Mexico):

Yes, and corresponding to the person who decided how AI should act in each specific case.

Paulina Saldaña Fuentes (Mexico):

Yes, and corresponding to the person who decided how AI should act in each specific case.

Ricardo Heredia (Mexico):

Yes, it can be consider a patent.

Fergan Tuğberk İşman (Turkey):

For a creation to be protected within the scope of intellectual property there has to be an original creation of work. An original creation consists of its creator's personality within however when an AI creates a work, it consists of AI's algorithm instead of a real person's personality.

Inventor of the AI is actually creating intellectual property by developing the AI. During development of the AI, the creator chooses which information the AI will receive, thus they shape the AI's capability to "think". When the AI creates a work, it inevitably consists the information that the creator feeds them during their development. The creations made by AI actually are the AI's creators' labour. The outcome should be protected as a creation made by the AI's creator.

5. Which kind of ethic rules should apply for the use of AI?

Maria Inês Reis (Portugal):

Which kind of ethic rules should apply for the use of AI? I think it's wonderful that AI exists, but at the end of the day machines cannot replace humans, then don't have emotions or can decide some aspects of the daily life.

Iv Fangyuan_(China):

AI shall not marry human beings and shall not be heritor of human beings.

Qiu Shuang (China):

We should ensure that its security and existence value is not to surpass or replace people, but to teach people to learn and grow.

Qiyi Zhang (China):

Although AI is more and more like human beings in essence and appearance, it is a tool created by human beings in order to liberate labor force. We should not equate AI machines with human beings. And the robot's life is very long, its "spirit" memory can be saved forever by copying, so that the "spirit" will never die. On the contrary, human life span is very limited, and they will end their lives in advance due to many accidents. "spirit" cannot be copied to another "body" like artificial intelligence machine. If robots dominate the world, as so many science fiction movies do today, where will human survival go? Therefore, we should limit the rights of AI, strictly regulate the behaviour of AI, and let artificial intelligence be restricted in the system like public power, so as to get along well with human beings.

Friederike Ammann (Germany):

Discrimination should be avoided

Rupesh Pandey (India):

The ethical rules are principles and ethics aligned with the human behaviour in the context of artificial intelligence. The European Union published a set of guidelines on how companies and governments should develop ethical applications of artificial intelligence. The core principle of the EU guidelines is that the EU must develop a 'human-centric' approach to AI that is respectful of European values and principles. The Guidelines provided a set of seven key requirements that AI systems should meet in order to be deemed trustworthy namely, Human agency and oversight, Technical robustness and safety, Privacy and data governance, Transparency, Diversity, non-discrimination, and fairness, Environmental and societal well-being and Accountability.

Arthur Horsfall (UK):

The Alan Turing institute has set out the values that support, underwrite, and motivate **(SUM)** the responsible design and use of AI:

- respect the dignity of individuals;
- connect with each other sincerely, openly, and inclusively;
- care for the wellbeing of all; and
- protect the priorities of social values, justice, and public interest.

These do appear to be good ethical ground rules to be able to consider whether the AI being created is ethical.

Coral Yu (UK):

I think there are various types of jobs that AI cannot be used to replace people. On a technical level, there will need to be some rules on transparency and accountability of how AI works.

Gary Whitehead (UK):

Overuse of AI can result in lack of jobs for unskilled workforce

Philippa Kwok (UK):

- Prevention of harm
- Respect for human autonomy
- Transparency and fairness

Julia Krautter and Patrícia Perinazzo (Brazil):

Not established considering the inexistence of a law in place, however I believe that fairness, respect, and law abiding.

Luis Roberto Moreno Tinoco (Mexico):

I consider that the main ethical rule that shall be consider when referring to AI is whether or not legal capacity should be granted to them by the law. This is important because according to our current laws, individuals who have legal capacity are entitled to several basic rights, whose construction have been designed from the definition of human dignity.

Under this context, it shall be determined if AI will have the same rights that we are currently entitled, or if these rights should be limited to some extent (and, in any case, the way to determine the limits). This discussion could end with important questions that should be answered before drafting any kind of national legislation, for example, if the “owners” or “designers” of the AI will be entitled to erase or eliminate this programs or software, or if, by the contrary, this could trigger liabilities of any kind.

Mari Yoli Wulf Sánchez (Mexico):

Organizations are obliged to respect the human right to the protection of personal data, in the terms established by the Federal Constitution and the law.

Miguel Ángel Aspe de la Rosa (Mexico):

I would say data protection should be the cornerstone for the use of an AI. Naturally there are other ethical topics and discussions around the decisions taken by an AI, which could include human rights awareness and protection.

Paulina Saldaña Fuentes (Mexico):

The same rules that applies for person to person work.

Ricardo Heredia (Mexico):

The regulation in Mexico for AI, should consider a chapter of specific ethic rules, such as:

- The AI should be always controlled by humans.
- AI should never breach data privacy of people.
- The goal should be in benefit of the county specific needs and the world.
- AI should never cause harm to the environment.

Fergan Tuğberk Işman (Turkey):

AI can analyse or create in accordance with the information they have given during their development but they can't develop their own moral actions. They may be capable of analysing the moral actions and learn them but this still is a product of a humane intervention.

The developer is giving the AI their desired moral codes. When the AI has developed properly they are going to act on behalf of those moral codes. While operating or when faced some dilemmas AI has to decide which outcome they are going to choose.

The AI has to make their choices after an analysis of damage it is going to give to property, to living beings or to people. The most reasonable way of solving the dilemma is keeping the people's safety a priority.

6. How will AI influence expert work and legal work?

Maria Inês Reis (Portugal):

Some legal work can be replaced but in my opinion, court decisions cannot be made by computers/robots.

Iv Fangyuan_(China):

Many paper work, searching works, writing works may be replaced by AI.

Qiu Shuang (China):

I think that artificial intelligence can only replace those replaceable work, such as court record, speech recognition, etc., which will greatly improve the efficiency of the trial. In the field of trial, litigation strategy formulation and other fields, we have to rely on people to complete.

Qiyi Zhang (China):

In my opinion, the greatest advantage of human beings is that they have infinite creativity. Before artificial intelligence cannot have "infinite possibilities" like human beings, AI can't replace human beings. Artificial intelligence can only eliminate ordinary experts and legal personnel, but cannot eliminate excellent experts and legal

personnel. Artificial intelligence can quickly carry out a large number of data analysis and future scenario simulation, which can provide great help to experts and legal personnel, and save a lot of time for retrieving cases and setting. Experts and lawyers can use the time saved to think deeply about problems and get the job done better.

Friederike Ammann (Germany):

- AI will support expert work
- Time saving / more efficient especially for standard cases and repetitive tasks
- Automatic contracts
- It will be easier and faster to get legal protection
- Alleviates the work load e.g. in courts

Rupesh Pandey (India):

Technological advancement has become an integral part of the overall development and efficiency of any organization. AI is assisting legal professional on the work related to legal research, contract management, paralegals and support, litigation etc. AI based tools like IBM's Watson Contract Management and ContractPodAI's Artificial Intelligence Contract Management Solution are providing support to legal professionals and law firms to a great extent. These tools can assist, however, they can't substitute the work like advising clients, negotiating, cross examination, appearing in court etc. Legal skills and court craft cannot be acquired and performed by coding and applying algorithms.

Arthur Horsfall (UK):

With the use of automation software, I am already using AI in my legal work to prepare base documents. This not only speeds up the process, but also ensures a reliability and uniformity with the work. Whilst this can potentially, with an increase in data input and perfecting the AI's decision process, do up to 80% of the drafting, there will always be lacking the final 20% which requires the creativity and expert opinion of the individual. I do think that this will be a trend in a lot of expert industries and will result in employees being required to input the data required. However, due to the lack of creativity and problem solving an issue for which it is not programmed, I do not see it replacing the human element entirely.

Coral Yu (UK):

AI is developing rapidly as a support tool for repetitive, process-intensive, standardised legal work. I'm not quite sure how AI will assist with expert work.

Gary Whitehead (UK):

I think that COVID-19 pandemic has facilitate lawyers to better embrace technology and I think that should continue. It is already being used across many legal areas such as practice management and predictive coding.

Philippa Kwok (UK):

- Document automation
- Automated contract review
- Prediction of outcome of cases through application of relevant precedent and fact patterns
- Less human errors
- Overall greater efficiency and productivity, saving time and resources à helping firms be more competitive
- Leaving more time available for value-added tasks

Julia Krautter and Patrícia Perinazzo (Brazil):

AI will optimize the human work and make the job deliveries faster, completer and more accurate, always under a human attendance.

Luis Roberto Moreno Tinoco (Mexico):

I consider that AI will have a major impact in the way expert and legal work is done, since some legal controversies can be solved by applying simple syllogisms, by comparing the text of the law with the facts of each case in order to get to a conclusion. Although part of our work is the interpretation of laws that could be confusing or that could admit different interpretations, there is no reason to believe that this task could not be performed by a computer, designed with the ability to analyse legal texts.

In addition, some of the work that is done by the major law firms of the world (such as drafting agreements, shareholders meetings, etc.) could be easily replaced by a software designed to draft this documents, with the ability to prevent any further controversy based on the probabilities obtained from past experiences.

Mari Yoli Wulf Sánchez (Mexico):

That would allow people not to go to lawyers, but I think that human work will never be compared to that of a computer since they are based on algorithms and many times they do not find all the options.

Miguel Ángel Aspe de la Rosa (Mexico):

In the years to come we will see a great influence of AI in expert work and in the legal practice. The ability of increasingly sophisticated AIs will lead to almost perfect contracts, for instance.

Paulina Saldaña Fuentes (Mexico):

The lawyers drafting contracts and due diligence will be decreased, and lawyers practice shall be exploring new areas with this AI support.

Ricardo Heredia (Mexico):

I believe that the main influence would be in an ethic part. Notwithstanding, even though many machines could be able to do legal work, the human part or intuition in a negotiation could never be substituted.

Fergan Tuğberk İşman (Turkey):

AI's capability of thinking is linked directly to the information they have given during development. If an AI has given case precedents of supreme courts they can learn and come up with rules about the issues they have given. Highly analysed and righteous rules, regulations, laws and even case decisions may be created this way.

This capability can be used at any field of expertise. Any information, examples or methods the AI has given will shape their way of thinking and also products they produce. Unique AI's developed specifically for a field of work shall have the ability to analyse almost every work in that specific field.

This pool of knowledge is almost impossible to achieve by a human. But an AI has no limit on learning and processing. Any comment that AI has made will be an analysis from every other work previously made in that field.

Materials | Compact

Artificial Intelligence and Law

*Ulrich Herfurth, Rechtsanwalt, Hanover and Brussels
January 2019*

If you book a flight via a travel portal, you will quickly find that prices change - depending on when you book. Simple variable pricing, depending on how far in advance you book, is certainly common. But fluctuations within hours and minutes are a new development. This dynamic pricing is based on comprehensive observation and evaluation of competitors' market prices. Is it worthwhile for the provider to enter into particularly low prices or does he prefer to sell fewer trips but at better margins? The result is based on many individual decisions made by algorithms. Until now, people defined the decision criteria for the algorithms, but now increasingly the machines themselves - with artificial intelligence.

So what is artificial intelligence?

Artificial intelligence is a highly developed electronic systematics, which is no longer defined and programmed by human beings, but which gains and develops its own knowledge from collected information and patterns (Deep Learning). It uses extensive electronic networking structures for this purpose. An AI system is self-learning and makes independent decisions based on self-developed algorithms.

From a technical point of view, artificial intelligence (AI) is a branch of computer science. It deals with the automation of intelligent behaviour and so-called machine learning. As is often the case with new developments, the concept and content of the definition cannot be clearly defined. It is already unclear what exactly is to be understood by "intelligence". In any case, artificial intelligence is regarded as one of the decisive driving forces of the digital revolution. The term is not new; research on artificial intelligence began in the 1980s. However, computer performance was far too weak at the time to achieve any significant results. Today, on the other hand, processors and computers are exorbitantly more powerful: a supercomputer performs more computing operations than all PCs in Germany, and components for the application of AI are already installed in smartphones. This means that practical and affordable results can already be achieved today. Technically, an AI process involves billions comparisons of existing data with new data in grouped circuits, the results of which are again compared in many test steps.

Thus the system with AI recognizes a cat picture as cat and not as dog - or in the picture of a skin part a certain skin disease.

Today, experts differentiate between two dimensions of artificial intelligence: the weak artificial intelligence is an advanced tool of man, the strong AI develops a not really predictable life of its own with a neuronal functionality similar to the human brain, but presumably with a different cognitive structure - and without consciousness, essence and feelings. All this is only simulated, like in chatbots.

Applications and Markets

In the meantime, there are numerous application areas for AI in almost all industries. It starts with Data Mining and the analytical evaluation of large amounts of data, Big Data. This is the basis for target group-oriented marketing, especially in social media and e-commerce. It is not without reason that the internet companies Google, Amazon, Facebook, but also Uber, are the largest investors in the development of AI.

KI understands and masters languages, no longer just as a translation database, but with semantic understanding. It therefore delivers machine translations into foreign languages and reacts and communicates as voice-controlled assistants (Alexa, Siri) and communicates with users as social bots.

Intelligent systems can also be found in stock trading and in electronic investment consulting, the Robo Advisory for securities investments.

Machines also automatically design and generate contracts in the mass business, Smart Contracts, and could document these without a notary with the Blockchain technology counterfeit-proof. Systems such as eBay are already replacing state court proceedings in eCommerce by carrying out an electronic conciliation procedure for defect claims - as so-called softlaw.

In medicine, AI enables the evaluation of complex laboratory data. Diagnostic software with AI now often recognizes clinical pictures more accurately than a doctor, for example from the image of the iris or appearances on the skin. The same applies to animal diseases and plant diseases, also as disease control.

In the Smart Home, systems with AI take over the intelligent building control: energy, climate, ventilation, lighting and sun protection, supply with media, survey and access control.

On a larger scale, AI also supports energy supply and consumption in the Smart City, but also mobility and traffic control in the private sector and public transport, waste disposal, emergency systems, e-government and more.

Last but not least, AI enables autonomous driving through intelligent and interconnected vehicles that are not only able to find their way, but also to react appropriately to traffic situations in order to avoid accidents, damage and injuries.

On a large scale, AI applications can of course also be found in manufacturing: in the networked production under Industry 4.0, the machines and systems not only work through predefined tasks, but also communicate and react continuously to changes in their digital community - across operations, companies and national borders. The monitoring and optimization of processes is the goal, right up to early detection and automatic supply of requirements, for example through predictive maintenance or distance production with additive manufacturing.

And last but not least, military warfare in cyberwar scenarios and in autonomous wafer systems is also being upgraded with AI: moving and flying weapon systems are developing into autonomous units that can act in battle without human intervention.

All in all, it becomes clear to what extent AI, as a cross-sectional technology, can bring about technological, operational, economic and social changes. This is why the race for AI developments is in full swing not only in the economy, but also between states in order to achieve strategic and geopolitical advantages. The USA and China are the most important players, while Europe and Germany are far behind - albeit with special competence in industrial applications.

AI in state and society

Developments in artificial intelligence are not only about technical or economic goals, but also about ethical, social and legal aspects. What rank do we want to give to AI-controlled systems, and how do we secure our social order and our legal system in interaction with non-human actors? In recent years, a number of activities have emerged in Germany and Europe to this end, including robotics and autonomous driving. The Ethics Commission has submitted guidelines for autonomous driving and conflict cases to the Federal Government. Associations such as Bitkom are intensively involved in the discussion on issues of economic significance, social challenges and human responsibility. The Federal Government is currently pursuing the goal of massively promoting this area with its AI initiative. And the work of the Europeans Commission's High-Level Expert Group on Artificial Intelligence on its "Ethic Guidelines for a trustworthy AI" is currently underway.

Artificial intelligence in the legal framework

The use of artificial intelligence poses new challenges to the legal system. This is not just because systems are faster and more powerful than previously known systems and technically seen by the individual - but because they are able to make decisions instead of humans and without immediate predictability and human control.

Contracts

First of all, the question of legally secure contracts comes to the fore. If machines or systems are to trigger rights and obligations between the parties involved through their data transmission, it must also be possible to create a binding legal basis without a human declaration of intent. In addition, jurisprudence now attributes such "machine declarations" to the owners of the machines and systems as an offer and acceptance, because they move within the decision-making channels set by their owners. However, they are not referred to as representatives, but as machine agents. It is questionable whether this view can also be applied when machines no longer make their decisions only functionally but also intellectually autonomously.

After all, in conventional systems the algorithms are laid out and the criteria for decision-making are determined - in the AI, however, the system develops its own decision criteria, without any preliminary planning by the owner. Strictly speaking, the action of the system is no longer covered by its will, perhaps not even by its general idea of acting and the results of the system. Nevertheless, his business partner should probably be able to rely on the binding nature of the system's behaviour, for example according to the principle of toleration power of attorney or prima facie power of attorney, in which the represented person has to allow himself to be attributed the declarations of his representative, who is unauthorized in individual cases.

Liability

If damage or injury occurs, the question of liability arises. In contractual liability for the provision of a defect-free service, hardly any new aspects arise: The contractual partner is the owner for whom the system has established the contract, and the latter is liable for performance and freedom from defects. He will hardly be able to invoke the fact that his system did not work properly or in its sense in the event of service disruptions such as delay, non-fulfilment, defects or violation of non-obligations. System errors can probably not be regarded as a case of force majeure any more than a failure of the IT system today. Also the use of AI in quality control and in the execution of commercial inspection and complaint obligations should not differ in principle from conventional systems.

Another consideration applies to cases in which AI-controlled machines and systems, but also vehicles, cause damage or loss of rights during autonomous driving, to third parties or to contractual partners, which are not covered by a contractual liability. To this end, our legal system distinguishes between fault-based liability (due to intent or negligence) and strict liability (e.g. product liability of the manufacturer, liability of the vehicle owner and liability of the property owner). In this area, jurisprudence discusses who exactly is to be seen as responsible: Whose decision and behaviour is relevant for the assessment of fault? Who should be the liable party for the machines and systems used, for example the owner, the holder, the operator or the supplier of the system? As a result, a liability principle would probably make sense in which the person who actually controls the use of the system is liable, recourse against internal responsibilities not excluded. The extent to which the responsible party can cover risks by means of business and product liability insurance depends on the individual case. It is also under discussion whether AI systems should not be liable for themselves.

Data protection

In principle, data protection raises the same questions as before: personal data may not be processed without further ado, whereas anonymised or pseudonymised data without allocation to persons may. However, a new situation may arise if AI-supported systems from the aggregation of anonymous data can then assign data to individuals with sufficient certainty. Then machine data becomes personal data again and they are subject to data protection.

Intellectual property

The protection of intellectual property can also play an important role in the use of AI:

The AI itself is an intelligent system that suggests copyright protection. However, in most cases it does not have the quality of a work creation as it does with software. As a rule, AI systems do not constitute a database under copyright protection. Like software, AI as such is not patentable as a technical invention unless it is embodied in a technical product. Whether the AI is protected as a trade secret with its original and then self-developed processes and specifications depends again on its concrete use and, recently, according to European law on trade secrets, on whether it is the subject of concrete protective measures.

A second question is whether the results obtained by AI constitute protectable intellectual property. These can be analysis results, but also other "creative" works such as music, texts, images or software. Machine analyses with AI do not fall under copyright protection. And in the case of creative works it is already recognised today that the

creator (composer, author, photographer, software developer) may also use sophisticated instruments - as long as he contributes an important part and has the decision-making power over the design of his work, the result can be protected by copyright. If, however, a system generates a result without human input alone, the work cannot be protected under the existing copyright law.

Whether an intellectual property right should also exist in the future for creations by machines will certainly be the subject of fundamental legal policy discussion. Just like the AI system itself, however, the results achieved by AI can also be protected as trade secrets, a protection that does not apply if the results are published. Possibly the accessible results can then be used in reverse engineering with AIs to develop the structures of other AIs.

Competition law

With its powerful potential, artificial intelligence is capable of fundamentally changing markets and competition. In the interest of a functioning competition system, current competition law therefore concentrates on the control of processes in which market power does not arise through performance but through mergers of companies. Whether or not new market power arises is first assessed by merger control on the basis of the size of the small businesses. It aims at processes in which already powerful companies strategically buy up new start-ups with potential, such as Google did with Deep Mind (developer of the AI for the game GO). This would enable the Cartel Office to limit the concentration of AIs in the hands of powerful and financially strong players and thus their strengthening of market power.

If market power already exists, the company must not abuse it and, for example, discriminate against other market participants or bind them unjustifiably. AI can, however, help to create highly intelligent mechanisms which, due to their massive information advantage (information asymmetry), result in competitors, customers or suppliers making less favourable arrangements than with a balanced information situation.

Ultimately, AI is also used in systems for market observation and pricing. Already today, algorithms without AI control pricing on the basis of information on demand, interests (e.g. on search engines), social data (place of residence, mobile phone model, buying behaviour), times of day and others (dynamic pricing). With KI, the systems are even more powerful. Therefore, the control of the abuse of market power also applies here. However, as soon as the systems follow and react to the prices of competitors, they can constitute an inadmissible exchange of information in the sense of a price cartel. The legal problem now lies in the allocation of the action to persons - the actual reaction to

the exchange of information is not a human being, but an autonomous system that has even given itself its own rules for reacting to price changes when using AIs. Therefore, the Monopolies Commission rightly proposes to treat the implementation of an algorithm based price system in advance as a restrictive and inadmissible exchange of information. This idea should also take effect if systems with AI are strengthened.

Management liability

In corporate management, the question of management liability arises as to whether and to what extent management and the Executive Board are responsible for the behaviour of the systems they use, including those with artificial intelligence. In principle, it is their duty to use only those instruments that are technologically secure and do not cause any legal infringements. If these systems operate autonomously and their decision-making mechanisms cannot be reconstructed, the responsibility of the company's executive bodies in the event of infringements and damages remains the same. Conversely, the question arises as to the extent to which the management and executive board can rely on AI in their decision-making in corporate matters and, above all, can rely on it (business judgement rule). AI is certainly advantageous as an auxiliary instrument, but management must not transfer decision-making to technology alone and thus cannot shift its responsibility for the company onto it.

Structural classification

In addition, there are many legal discussions on the structural classification of AIs: Does a Generator for contract texts provide a legal service? Are Robo Advisory Platforms subject to financial supervision? May soft law, supported by AI, take the place of state courts? May the public administration have its discretionary decisions made by AIs?

Legal personality

In view of the far-reaching functional autonomy of AI systems, a discussion has arisen on the question of a legal personality of robots and AI systems and thus whether they should be given legal capacity as legal persons. Currently robots are treated as objects, there is no legal classification for immaterial systems, even for simple machine data our law knows no classification, for example in the sense of data ownership. With regard to the decision-making autonomy of AI systems in terms of content, there are voices in favour of an "electronic person" (ePerson). Such a figure is not inconceivable, for example in analogy to foundations as an ownerless and holder-less legal person. The responsibility would then lie solely with the robot or the system. Misconduct can then be sanctioned by switching off the system and imposing financial fines. As an intelligent

system, AI should even avoid misconduct if it learns from sanctions. The demand for an AI system liability fund for damages is quickly leads the the question of the appropriate and necessary amount of funds. Compulsory insurances and other security systems with solid guarantees are more suitable for this purpose. Legally an encapsulation of the liability is not necessary, the liability for an AI system can be isolated also over corporations such as GmbH, AG and foundation. However, a far-reaching decoupling of damage and liability does not seem desirable from the point of view of prevention.

AI and ethics

Many of the legal issues raised by AI on new issues can only be considered from an ethical perspective: May there be an identification of people in mass proceedings, e.g. by facial recognition, without their consent? Does the human being have to be able to recognize them in dialogue with AI? Do unknown social bots violate fundamental rights and human dignity in dialogue with humans? How must the system decide in the dilemma between alterntaive impending damages? May autonomous systems, in particular medical diagnoses, autonomous vehicles and autonomous weapons systems, decide the lives of humans? Ultimately, it is a question of whether machines may only use their functionally similar or even superior capabilities in the service of human beings, or whether they may be given a status legally comparable to that of human beings. This discussion will accompany us in the coming years.

+++