EUROPEAN DATA PROTECTION LAW INTRODUCTION

D C
K K

Foto: © 2016 Darko Todorovic

LAW FIRM FOR IT/IP AND MEDIA LAW

DR. CHRISTINE KNECHT-KLEBER LL.M.

- IT- AND SOFTWARE(LICENSE)CONTRACTS
- DATA PROTECTION LAW
- TRADEMARK AND DOMAIN LAW
- COPYRIGHT AND DESIGN LAW
- ONLINE-MARKETING / SOCIAL MEDIA LAW
- E-COMMERCE LAW / WEBSHOP / GTC
- PROTECTION OF INNOVATIONS AND KNOW-HOW
- COMMERCIAL LAW

CONTENT
INTRODUCTION

- Aim / scope of GDPR?
- Legal requirements
- Responsibilities to individual
- Responsibilities of controller

https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource

General principle, we always need a legal basis when data is processed. e.g Data collection on social networks

INITIAL SITUATION

The world's most valuable resource is no longer oil, but data

New legal framework required

GDPR

GDPR

GENERAL SCOPE / AIM

- **Regulation** enacted by the European legislator (= EU Parliament & EU commission)
- Intends to **strengthen** and **unify data protection for individuals** within the EU
- Aims to **give control back to citizens** over their personal data
- Fundamental right
- Replaces the Data Protection Directive of 1995
- Entry into force on May 25, 2018

Uber

Uber concealed massive hack that exposed data of 57m users and drivers

§

Violation of regulations cause high fines

- Firm paid hackers $100,000 to delete data and keep breach quiet
- Chief security officer Joe Sullivan fired for concealing October 2016 breach

Uber conceald massive Hack

Before May 25, 2018
No fine

Jan Philipp Albrecht

@JanAlbrecht

From 25 May 2018 #Uber will have to pay up to 4% of its yearly worldwide turnover (so around 300 Million $) to the EU #dataprotection authorities for such a breach. Thanks to the EU‘s #GDPR. Such behavior has to belong to the past. #privacy #cybersecurity twitter.com/androidauth/st…

10:27 - 22. Nov. 2017

4 38 27

After May 25, 2018
Fine EUR 400.000,--

First GDPR Fine Hospital Portugal

It was a hospital. High fine for data breach, IT workes hat access to patients data. Austrian national mail service was fined (20 Mio), the transprancy was not present, people didn't know that the data has been collected and the post had access to the political opinion.

GDPR

WHEN DOES IT APPLY?

- **Automated** and **manual** (wholly or in part) processing (if part of filing system)
- **Personal data =** any information relating to an identified or identifiable **natural person**

  GDPR focuses on natural persons, in Austria legal entities are considered as well for data protection but not GDPR

  - e.g. name, e-mail address, IP-address, date of birth, photos, sound recordings
- **Special categories of personal data:**
  - health data, genetic and biometric data, religious beliefs, political opinion, trade union membership, sexual orientation, etc.

Name of my pet is not relevant

§

GDPR

WHAT IS DATA PROCESSING?

- It includes the **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** of personal data.

  = **any activity**

GDPR

DATA PROCESSING - EXAMPLES

- staff management and payroll administration
- access to/consultation of a contacts database containing personal data
- sending promotional emails
- shredding documents containing personal data
- posting/putting a photo of a person on a website
- storing IP addresses or MAC addresses
- video recording (CCTV)

you have to inform the relevant person, if a person will be in a video. Natural person is on a photo

1. you have to have a consent (photo of the homepage)
2. posting of the picture on social media (requires a legal basis) any posting of a picture requires a consent (=Zustimmung)

GDPR
EXCLUSIONS

GDPR does **not apply**:

- Processing of **anonymous data** (= individual is no longer identifiable)
- **purely personal activity** (= not commercial or professional)
    - e.g. address book, social networking, correspondence

Pseudonymisation, matching table where you can trace back the person itself

privacy by design - mentioned from Bernd Schenk

GDPR

WHERE DOES IT APPLY?

Any processing of personal data by establishment

- domiciled **in the EU** for its purposes in the EU
- domiciled **outside the EU**, but New!
  - offering goods/services to a natural person **in the EU** or
  - monitoring their behaviour takes place **in the EU**

Powerful companies like google, facebook can not opt out.

GDPR
PARTICIPANTS

- **Data subject**
  natural person to whom the personal data refers = individual
- **Controller**
  If a data violation happens, the responsibility of the controller is to choose a trustful and reliable provider. The controller is liable. Usually the controller is in the position to get insight into the measures.
  natural or legal person **deciding** if / how / for what purpose personal data are processed
- **Processor** Cloud Service, Hosting Provider
  natural or legal person processing personal data **on behalf** of the controller
  e.g. cloud provider

GDPR

SCOPE – INTERIM RESULT

- Data protection rules apply whenever personal data is processed
- GDPR grant rights to natural persons solely (no legal entities)
- Enterprises outside the EU must abide by GDPR
- Manual processing of personal data included (file system)
- No significant changes to legal framework of Data Protection Directive

and processing of data of personal data

every person who lives in the EU, not related to the citizenship

European Union: Directive has to be implemented in a certain period of time (1,5 years) to implement in to national law
Regulation is usually (aims to unify european law) applicable as soon as it is published.

§

GDPR

GENERAL RULE

Principle of prohibition

= personal data may only be processed

when allowed by the law

GDPR

LAWFULNESS OF PROCESSING (ART. 6)

If non of these legal bases are met, no data processing should take place —> general rule applies (principle of prohibition)

- **Consent**

  Cookies - popular legal basis, right of withdrawal (at any time with any time, the individual can withdraw the consent

- **Performance of a contract**

  Whenever you purchase goods, the goods have to be sent to your home (address is relevant), disclosing of data takes place, the legal basis is the performance of a contract

- **Compliance with legal obligation**

  A tax advisor has to forward certain personal data because they establish the payroll, they have to do it because of a legal obligation

- Protection of vital interests
- Public interest
- **Legitimate interests (balancing of interests)**

  Google Analytics, legitimate interest of the controller, you have to balance interest, my interest to the interest of the individual. If the individual interests is violated, right of withdrawal

Exhaustive list!

GDPR

LAWFULNESS OF PROCESSING – SPECIAL CATEGORIES (ART. 9) (1)

Data processing is lawful if:

- **Explicit Consent**
- Purposes related to **social protection/security** and **employment law**
- Protection of vital interests and individual is physically incapable
- Association (NGO) with political, religious, trade union aim
- Data **manifestly made public** by **individual** itself

Exhaustive list!

GDPR

LAWFULNESS OF PROCESSING – SPECIAL CATEGORIES (ART. 9) (2)

Data processing is lawful if:

- Exercise/defence of legal claims
- Substantial public interest
- Purposes of preventive or **occupational medicine**, **health and social care**
- Public interest related to public health, serious cross border threats
- Archiving / statistic / research / statistical purposes in public interest

Exhaustive list!

GDPR

CONSENT – CONDITIONS (ART. 7)

- **Burden of proof** for valid consent by **controller** (= written form advisable)
- Written declaration:
  - clearly distinguishable from other matters
  - easily accessible
  - clear and plain language
- Individiual has **right to withdraw at any time**

Requirement:
Freely given!

witten form, in implicit form (doing a sign), if you don't do it in written form, you maybe do not fulfill the burden of proof

GDPR
CONSENT

PRACTICAL ADVICE

A consent is not a consent, if you don't have the choice to choose.

- No data protection matters in General Terms & Conditions ➡ Privacy statement
- Consent in written form (burden of proof)
- Children: at least 16 years old (Austria: 14 years)

Asked question about the age of a child

GDPR

LEGAL PRINCIPLES (ART. 5)

Processing personal data is subject to these principles

- Lawfulness (legal basis) Art. 6 and 9
- Fairness
- Transparency the individual has the right to know what happens with the data
- Purpose limitation
  taking a picture and use it for a different purpose
- Data minimisation torch example, US is free to process, EU different
- Accuracy
- Storage limitation big issue, when they will delete the data - difficult issue
- Integrity and confidentiality
  whenever you process your data it has to be secure

Note: Controller (CEO) shall be responsible for compliance with GDPR!

EXCLUSIVE

Google collects Android users' locations even when location services are disabled

By Keith Collins | November 21, 2017

Google collects location data

German competition authority orders Facebook to change data collection procedures

Facebook has twelve months to implement the new decision

By **SIMON VAN DORPE** | 2/7/19, 10:35 AM CET | Updated 2/7/19, 3:41 PM CET

Facebook booth during the World Economic Forum (WEF) annual meeting in Davos | Fabrice Coffrini/AFP via Getty Images

https://www.politico.eu/article/german-competition-authority-orders-facebook-to-change-data-collection-procedures/

§

RESPONSIBILITIES

OVERVIEW

- Measures to **provide information** to individual = **Transparency**
- Processing requests of individuals in due course = **Rights for citizens**
- Data breach notification duty of individual (if high risk)

RESPONSIBILITIES

TRANSPARENCY (ART. 12)

- Obligation to provide information relating to rights of individual (Art. 15 – 22)
- Provision of requested information within **1 month** of receipt (electronically)
- Free of charge
- Refusal if identity is unclear or excessive/manifestly unfounded request
- Possibility of lodging a complaint

RESPONSIBILITIES

OBLIGATION TO INFORM (ART. 13)

- **Controller must provide information to individual of any data collection,** namely
  - Name and contact details of controller
  - Purpose and legal basis of processing
  - Recipient of the data (regarding transfers to third countries)
  - Existence of automated decision-making, incl. profiling
  - Individual‘s rights
  - Possibility to lodge an complaint with the supervisory authority

Privacy statement!

RESPONSIBILITIES

RIGHTS OF CITIZENS

- **Obligation to inform** (e.g. privacy statement)
- **Obligation to give access**
- Obligation to rectify
- Obligation to erase
- **Obligation to withdraw consent** (right of objection)
- Obligation to restrict processing (new!)
- Obligation to data portability (new!)

As a system provider, the best way would be to provide a button to extract all information of an individual user in a system - comment from Bernd Schenk

RESPONSIBILITIES

RIGHT OF ACCESS (ART. 15)

- Confirmation of controller of data processing
- Purpose of processing
- Categories of personal data
- Period of storage

Within 1 month, the individual should receive the information about the data

- Recipients of personal data incl. third countries
- Existence of right of rectification, erasure and restriction
- Right to lodge a complaint with supervisor authority

RESPONSIBILITIES

RIGHT TO OBJECT (ART. 21)

- Legal basis:
  legitimate interests pursued by controller incl. profiling
- Interests of individual override interests of controller, unless controller demonstrates compelling legitimate grounds
- at any time

- Legal basis:
  Direct marketing purposes
- at any time

Whenever we gave a consent, we have the right to refuse it and this is meant for the future and not for the past. If we talk about the right to object (counterpart of the legitimate interest) very often tracking tools are based on the legitimate interest and this is why a controller has to provide the right to object.

Data shall no longer be processed for such purposes

RESPONSIBILITIES

RIGHT OF ERASURE = „RIGHT TO BE FORGOTTEN“ (ART. 17)

- Data are no longer necessary
- Individual withdraws consent
- Individual objects to processing
- Data are unlawfully processed

BUT if data is necessary for

- Compliance with legal obligation
- Reasons of public interest (public health)
- Archiving, scientific purposes in the public interest

- Right of erasure cannot be exercised

Right to be forgotten - has been existing for a long time, if the controller is obliged to store the data (due to financial provisions), the deletion of the private data can not be done due to the law.

RESPONSIBILITIES

DATA BREACH NOTIFICATION DUTY (ART. 34)

What is a high risk? Health data has been disclosed, they should have informed the individual. This obligation is new, formerly only the data authority has to be informed.

- Controller must inform individual if a **high risk** to individual is given without undue delay if data is encrypted, you might not have to inform the data authority and you won't be fined. And you don't have to inform individual.
- Data breach:
  - Breach of security (eg intentionally or by chance) and
  - leading to the destruction, loss, alteration or unauthorized disclosure of personal data

Which responsibilities does a controller have when a data breach has happened based on GDPR regulations?

Answer: must inform the individual

§

OBLIGATIONS / TO DOs of CONTROLLER

OBLIGATIONS OF THE CONTROLLER

OVERVIEW

- Implementation of **technical and organisational measures** (TOMs)
  - Privacy by design / default

New!

- Engagement of processors – conclusion of a contract required

data protection management system

- Records of processing activities

New!

company has to take records for each activity (e.g. HR department) you only have to provide it for the data protection authority (audits), no individuals, law doesn't tell you how to do it, there is no hint on the level of detail

- Data breach notification duty to supervisory authority/individual
- Data protection impact assessment for high risk data

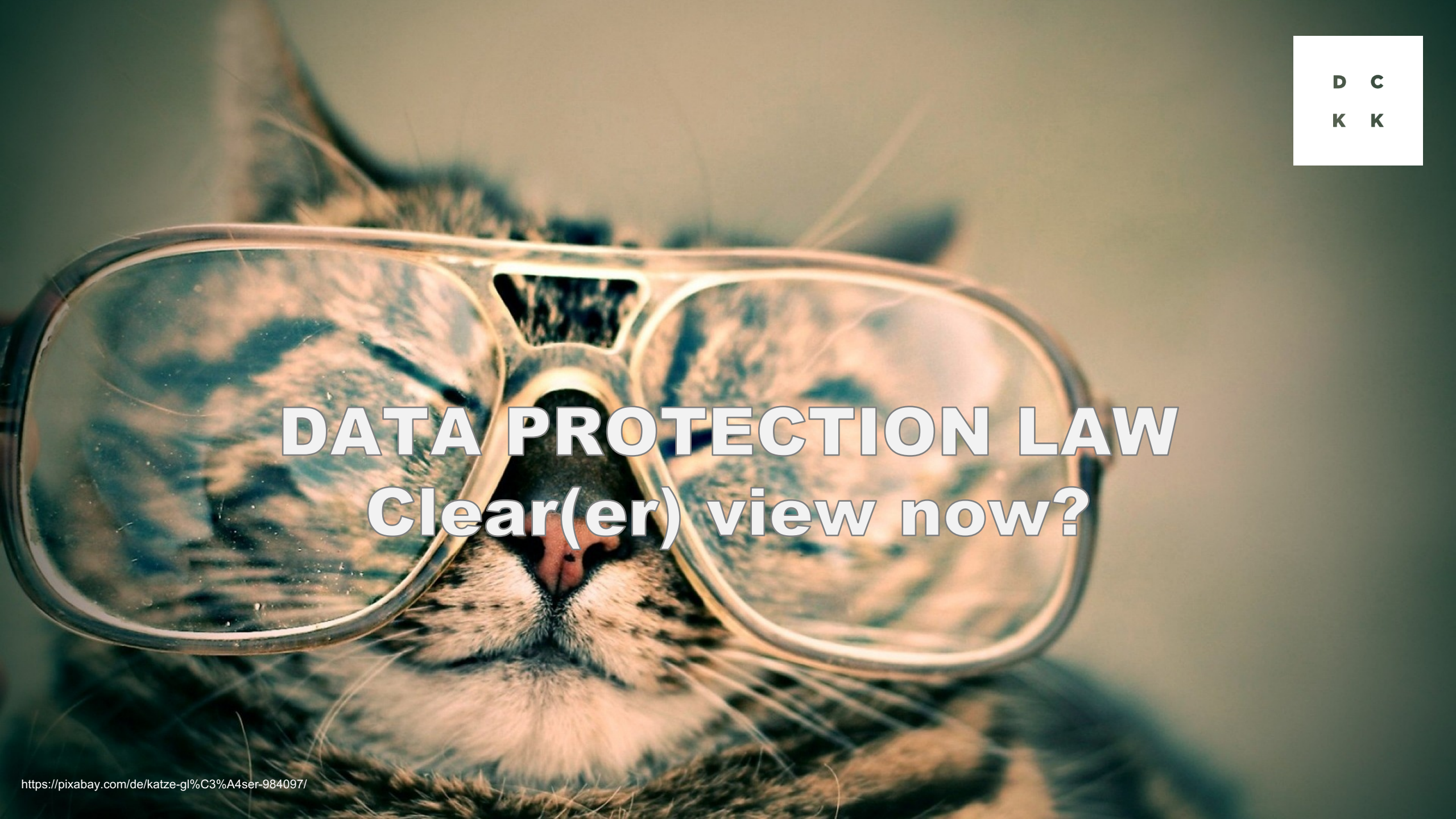
New!

- Designation of data protection officer (if required by the law)

New!

GDPR complete new field in law, currently it is more about guessing and trying to do the right stuff in terms of law

Danger of overachieving, we do more than necessary. In case of doubt, do more, than less!



DATA PROTECTION LAW
Clear(er) view now?

https://pixabay.com/de/katze-gl%C3%A4ser-984097/

THANK YOU!

Dr. Christine Knecht-Kleber LL.M.
Attorney at law

Campus V - Hintere Achmühlerstraße 1
6850 Dornbirn
+43/5572 93 18 00

kanzlei@dckk.at
www.dckk.at