

# Datenschutz und Copyright

**Dr. Lukas Feiler, SSCP**  
**Baker & McKenzie**

Marketing und Vertrieb, MSc WS13  
19.11.2014



**Datenschutz**



## Datenschutz - Inhalt

- Wozu Datenschutzrecht?
- Zulässigkeitsprüfung
- Datensicherheit & Breach Notification
- Meldepflichten gegenüber der DSB
- Outsourcing innerhalb und außerhalb der EU
- Whistleblowing, Compliance-Untersuchungen und Videoüberwachung
- Sanktionen



## Is Privacy Dead?

- “You have zero privacy anyway, get over it”
- Milliarden von Usern haben Facebook-Profilen, viele sind öffentlich
- Schätzen Konsumenten Privatsphäre?
  - Hängt vom Kontext ab!
  - “Privacy in Context”: Konsumenten sind bereit, ihre Daten in einem Kontext zu teilen, verweigern es aber in einem anderen

# Datenschutz-Compliance

- Datenschutz-Compliance gewinnt an Wichtigkeit
  - Rechtliche Risiken: Strafen von bis zu EUR 25.000 pro Verstoß
  - Image-Risiken: Compliance-Defizite & Security Breaches gefährden Image des Unternehmens
  - Wirtschaftliche Risiken durch verlorenes Kundenvertrauen
- Jüngste Entwicklungen
  - “Hacktivists” machen Security Breaches publik (zB Anonymous)
  - Datenschutz-Aktivisten prangern Compliance-Defizite an (zB Europe v. Facebook oder Big Brother Awards)
  - Datenverarbeitungsregister ist seit 1.9.2012 online für jedermann einsehbar



# Der Rechtsrahmen in der EU

- Datenschutz-Richtlinie (RL 95/46/EG)
- ePrivacy Directive (2002/58/EG) – gilt grundsätzlich nur für Telekommunikationsunternehmen
- Am Horizont: neue Datenschutz-Grundverordnung der EU



## Datenschutz als Grundrecht

- Europäische Menschenrechtskonvention
  - Schützt Privatsphäre (Artikel 8)
- EU Grundrechtscharta
  - Schützt das Grundrecht auf Datenschutz (Artikel 8)
- Österreich: § 1 Datenschutzgesetz 2000
- USA
  - 4. Verfassungszusatz: Schutz vor unreasonable searches & seizures; gilt aber nur wenn “reasonable expectation of privacy” (Katz v. United States, 389 U.S. 347 (1967))
    - secrecy paradigm



# Was sind “personenbezogene Daten”?

## Personenbezogene Daten

- Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist

## Indirekt personenbezogene Daten

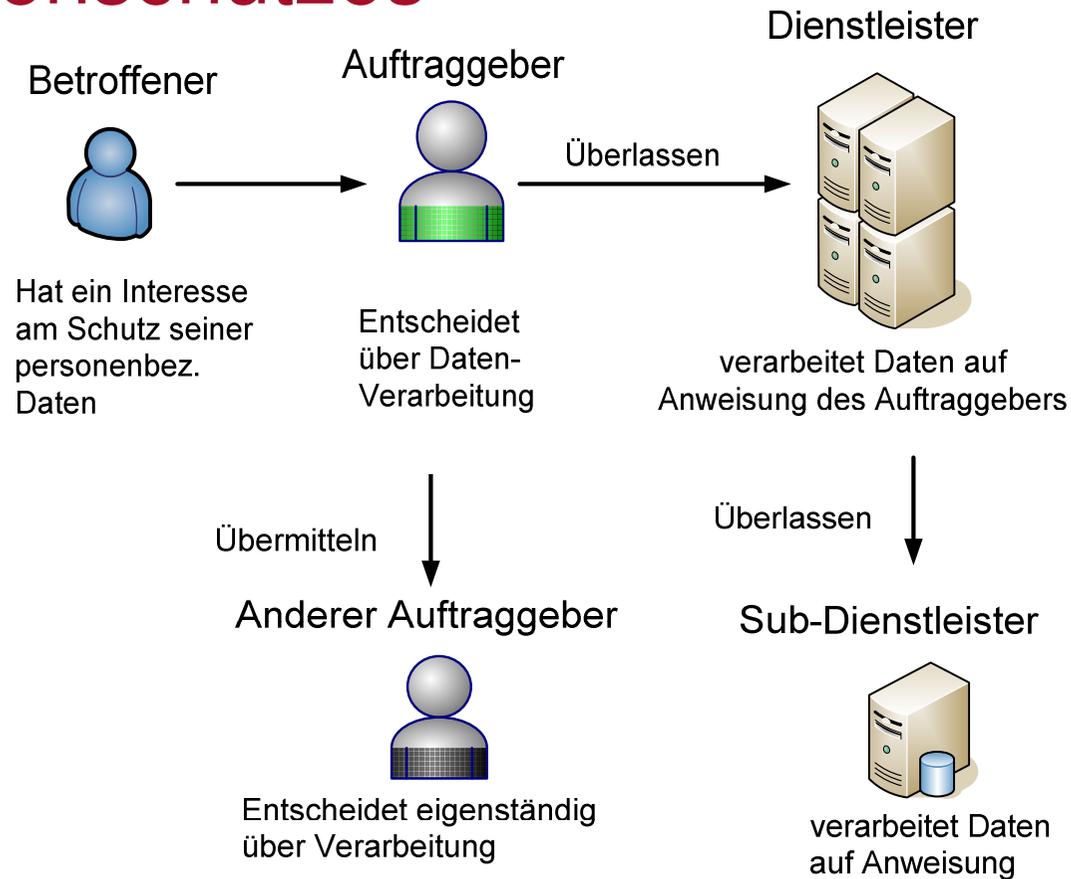
- wenn der Auftraggeber die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann
  - “personenbezogen” ist ein relativer Begriff
  - Daten können für ein Unternehmen direkt und für ein anderes nur indirekt personenbezogen sein



# Akteure im Bereich des Datenschutzrechts

- Betroffene
  - natürliche oder juristische Personen oder Personengemeinschaften, deren Daten verwendet werden
- Auftraggeber
  - Personen, die allein oder gemeinsam mit anderen die Entscheidung getroffen haben, Daten zu verwenden
  - unabhängig davon, ob sie die Daten selbst verwenden oder damit einen Dienstleister beauftragen
- Dienstleister
  - Personen, die Daten nur zur Herstellung eines ihnen aufgetragenen Werkes für einen anderen verwenden
- Datenschutzbehörde (DSB)

# Akteure im Bereich des Datenschutzes



# Nationale Datenschutz- gesetze differieren – Welches Recht gilt?

- Grundsatz: Ort der Niederlassung des Auftraggebers ist entscheidend
  - zB österr. Unternehmen bietet Online-Service in der ganzen EU an: es gilt österr. Recht
  - Ort der Niederlassung der Dienstleister ist unerheblich
- Wenn der Auftraggeber mehrere Niederlassungen in der EU hat:
  - Im Rahmen der Tätigkeiten welcher Niederlassung erfolgt die Datenverarbeitung?

# Welches Recht gilt?



# Zulässigkeit der Datenverarbeitung

1. Zulässiger Zweck der Datenverarbeitung?
  - festgelegt
  - eindeutig
  - rechtmäßig
2. Schutzwürdige Geheimhaltungsinteressen verletzt?
  - Rechtfertigungsgründe
  - Unterscheidung sensible / nicht-sensible Daten
  - Verhältnismäßigkeit (erforderliches Ausmaß / gelindestes Mittel)

# Schutzwürdige Geheimhaltungsinteressen

Geheimhaltungsinteressen nur dann nicht verletzt, wenn:

- 1) der Betroffene zugestimmt hat (informierte und freie Zustimmung)
  - Zustimmung ist widerruflich → “Right to be forgotten”
- 2) zulässigerweise veröffentlichte Daten
- 3) indirekt personenbezogenen Daten
- 4) gesetzliche Ermächtigung oder Verpflichtung
- 5) lebenswichtige Interessen des Betroffenen
- 6) überwiegende berechnete Interessen des AG oder eines Dritten; zB
  - zur Wahrung lebenswichtiger Interessen eines Dritten
  - zur Erfüllung einer vertragl. Verpflichtung zw. AG und Betroffenenem
  - zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde

# Geheimhaltungsinteressen bei sensiblen Daten

Sensible Daten: Daten natürlicher Personen über

- ihre rassische und ethnische Herkunft,
- politische Meinung,
- Gewerkschaftszugehörigkeit,
- religiöse oder philosophische Überzeugung,
- Gesundheit oder
- ihr Sexualleben.

Eingeschränkte Zulässigkeit der Verarbeitung; insb:

- „überwiegende berechnigte Interessen“ nicht ausreichend
- Zustimmung des Betroffenen muss ausdrücklich sein
- Jedoch Ausreichend: Arbeitsrechtliche Rechte/Pflichten + Betriebsvereinbarung

# Datensicherheit I

- Daten sind zu schützen vor (§ 14 DSGVO)
  - Verlust
    - Verfügbarkeit
  - zufälliger oder unrechtmäßiger Zerstörung
    - Integrität
  - Zugang durch Unbefugte
    - Vertraulichkeit
  - Nicht ordnungsgemäße Verwendung
    - Rechtmäßigkeit



## Datensicherheit II

- Angemessene Sicherheitsmaßnahmen: je nach
  - Art der verwendeten Daten
  - Umfang und Zweck der Verwendung
  - Stand der technischen Möglichkeiten
  - wirtschaftliche Vertretbarkeit
- Um Angemessenheit zu beurteilen:
  - Risiko-Analyse
  - Kosten-Nutzen-Analyse

# Data Security Breach Notification

- *Die Pflicht betroffene Personen von der Kompromittierung ihrer personenbezogenen Daten zu informieren.*
- Eine „Erfindung“ aus Kalifornien:
  - California Senate Bill 1386 (2002)
- Zweck:
  - Betroffene sollen reaktive Maßnahmen ergreifen können
  - Markt-Transparenz hinsichtlich Daten-Sicherheit
- Rechtsquellen in Österreich:
  - Gesetz: § 24 Abs 2a DSGVO 2000; § 95a TKG 2003
  - Verträge

## Breach Notification nach DSGVO

- § 24 Abs 2a DSGVO 2000: Notifikations-Pflicht, wenn:
  - Unternehmen bekannt wird, dass personenbezogene Daten „systematisch und schwerwiegend“ unrechtmäßig verwendet wurden und
  - den Betroffenen Schaden droht
- Ausnahme: wenn Notifikation nicht im Verhältnis zum geringfügigen drohenden Schaden steht
- Form der Notifikation: „in geeigneter Form“
- Zeitpunkt der Notifikation: „unverzögerlich“
- Rechtsfolge der Verletzung:
  - Verwaltungsstrafe: bis zu EUR 10.000 (§ 52 Abs 2 DSGVO 2000)
  - Haftung für Vermögensschäden nach allgem. Zivilrecht

## Datengeheimnis (§ 15 DSG)

- Gilt für Auftraggeber, Dienstleister und Mitarbeiter
- Gesetzliche Verpflichtung zur Geheimhaltung von Daten, die aufgrund berufsmäßiger Beschäftigung anvertraut oder zugänglich gemacht wurden
- Daten nur aufgrund Anordnung des Auftraggebers übermitteln
- Mitarbeiter sind über die Folgen der Verletzung des Datengeheimnisses belehren
- Rechtsfolge der Verletzung: bis zu EUR 25.000  
Verwaltungsstrafe (§ 52 Abs 1 DSG)

# Rechte des Betroffenen

- Recht auf Auskunft
  - Welche Daten verarbeitet?
  - Woher stammen die Daten?
  - Wozu verwendet?
  - An wen übermittelt?
  - auf schriftliches Verlangen des Betroffenen
  - binnen 8 Wochen nach Einlangen zu erfüllen
- Recht auf Richtigstellung der Daten
- Recht auf Löschung unzulässig verarbeiteter Daten

## Meldepflicht gegenüber der DSB

- AG hat Datenanwendung vor Inbetriebnahme bei der DSB zu melden (§ 18 Abs 1 DSG)
- Meldung muss enthalten (§ 19 DSG)
  - Name und Anschrift des Auftraggebers
  - Zweck der Datenverarbeitung
  - Nachweis der rechtlichen Befugnis
  - Kreise der Betroffenen & verarbeiteten Datenarten
  - Kreise der Übermittlungsempfänger
  - Allgemeine Beschreibung der Datensicherheitsmaßnahmen
- Alle registrierten Meldungen sind öffentlich einsehbar:  
<https://dvr.dsb.gv.at>

# Ausnahmen von der Meldepflicht

Meldepflicht entfällt, wenn (§ 17 Abs 2 DSGVO)

- nur veröffentlichte oder nur indirekt personenbezogene Daten
- Standard-Datenanwendung gemäß Standard- und Musterverordnung 2004; zB
  - Rechnungswesen und Logistik
  - Personalverwaltung für privatrechtliche Dienstverhältnisse
  - Bonus- und Beteiligungsprogramme im Konzern

Vereinfachte Meldepflicht für sog. Muster-Anwendungen

- zB Zutrittskontrollsysteme (für physischen Zugang zu Gebäuden)
- nur Name des Auftraggebers, Art der Muster-Anwendung & rechtliche Befugnis sind zu melden

## Vorabkontrolle

- Datenanwendung darf erst nach erfolgter Genehmigung in Betrieb genommen werden, wenn (§ 18 Abs 2 DSGVO)
  - Sensible Daten
  - Strafrechtlich relevante Daten
  - Videoüberwachung (§ 50c DSGVO)
  - Auskunftserteilung über die Kreditwürdigkeit der Betroffenen
  - Informationsverbundsystems (gemeinsame Verarbeitung von Daten in einer Datenanwendung durch mehrere Auftraggeber; beide haben Zugriff auf alle Daten)

# Outsourcing – Datenüberlassung an Dienstleister

- Auftraggeber kann sich zur Datenverarbeitung eines Dienstleisters bedienen (§ 10 DSGVO)
  - Dienstleister muss ausreichende Gewähr für rechtmäßige und sichere Datenverwendung bieten
  - Vereinbarung muss folgende Pflichten enthalten:
    - Daten nur im Rahmen der Aufträge des AG verwenden
    - Datensicherheitsmaßnahmen gem § 14 DSGVO sind zu treffen
    - Sub-Dienstleister nur mit Billigung des Auftraggebers
    - Voraussetzungen für Erfüllung d. Pflichten gegenüber Betr.
    - nach Beendigung: Daten an AG übergeben oder vernichten
    - AG Informationen zur Verfügung zu stellen, die zur Kontrolle notwendig sind

# Outsourcing an ausländische Dienstleister I

- Dienstleister in der EU
  - Keine Meldung/Genehmigung erforderlich
- Dienstleister außerhalb der EU
  - Nur Genehmigungsfrei, wenn Drittstaat angemessenen Datenschutz bietet
    - Lt. Europ. Kommission zB Kanada, Schweiz und
    - die USA:
      - Safe Harbor Program
      - “angemessener” Datenschutz, wenn
        - Sich der Dienstleister nach Safe Harbor Rules selbst-zertifiziert hat → [safeharbor.export.gov/list.aspx](http://safeharbor.export.gov/list.aspx)
        - Rechtsdurchsetzung: FTC Act § 5

# Outsourcing an ausländische Dienstleister II

- Outsourcing an Dienstleister in Drittland ohne angemessenen Datenschutz
  - Genehmigungsfrei, wenn (u.a.; § 12 Abs 3 DSGVO)
    - im Inland zulässigerweise veröffentlichte Daten;
    - für Empfänger nur indirekt personenbezogene Daten od.
    - Zustimmung der Betroffenen
  - Ansonsten besteht ein Genehmigungsvorbehalt
    - Genehmigung ist zu erteilen, wenn Dienstleister-Vertrag Standardvertragsklauseln der Europ. Kommission enthält

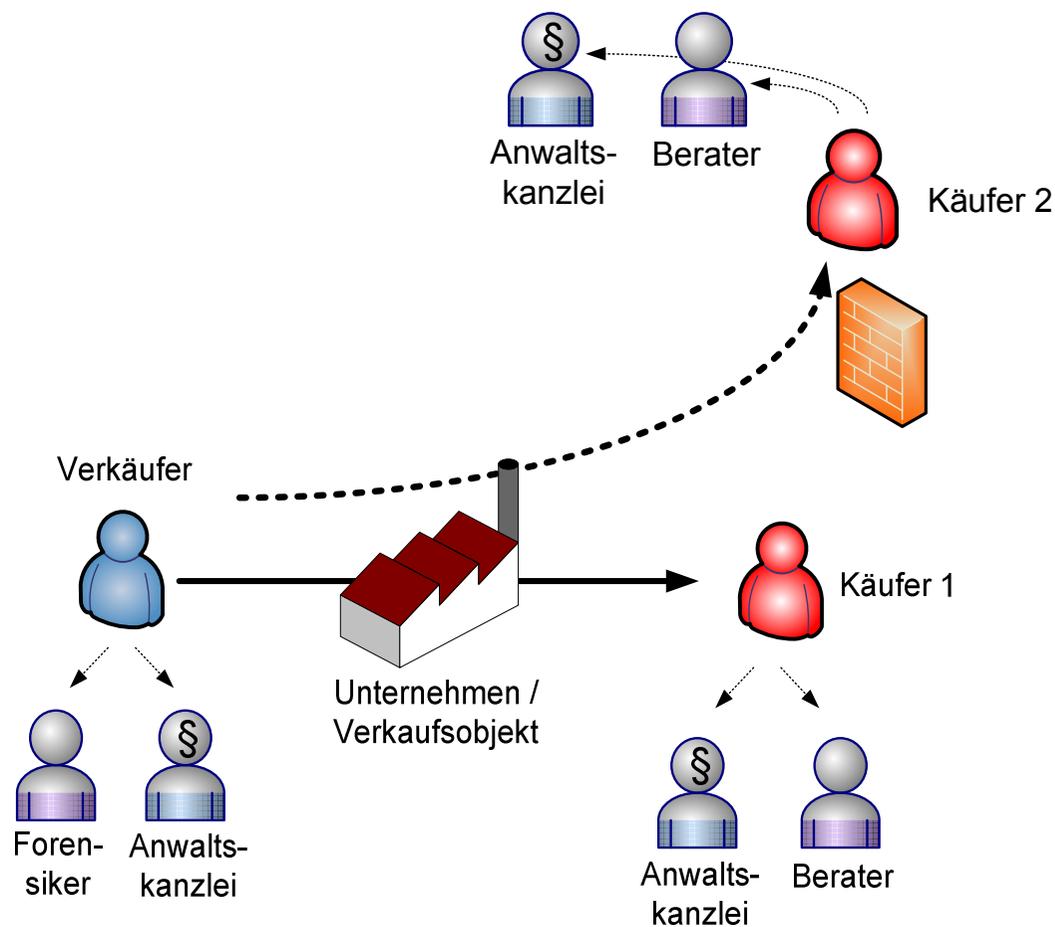
# Whistleblowing Hotlines

- Internes Verfahren zur Meldung von Missständen im Unternehmen
- Überwiegendes berechtigtes Interessen des AG
- Zahlreiche Einschränkungen durch Rsp der DSB
- Strafrechtlich relevante Daten werden verarbeitet:
  - Vorabkontrolle durch DSB → Inbetriebnahme erst nach Genehmigung
- Bei Übermittlung der Daten ins Ausland – Genehmigung der DSB

# Interne Compliance-Untersuchungen

- Bei Verdacht eines schweren Compliance-Verstoßes idR
  - geheime Auswertung der E-Mails des Verdächtigen
  - Auswertung der Browser-History
- Rechtsgrundlage:
  - Verfolgung von Rechtsansprüchen vor einer Behörde
  - Rechte & Pflichten im Arbeitsrecht + Betriebsvereinbarung
- Jedenfalls strafrechtlich relevante Daten
  - Vorabgenehmigung erforderlich
    - Problem: dauert Monate & Registrierung ist öffentlich
    - Einzige Lösung: prophylaktische Meldung

# Untersuchungen in der Praxis – ein Beispiel



- 1,5 TB E-Mails
- >40 Interviews
- 2 Käufer, je 1 Berater, je 1 Anwalts-Kanzlei

# Videoüberwachung I

- Keine Verletzung schutzwürdiger Geheimhaltungsinteressen wenn
  - lebenswichtiges Interesse einer Person
  - öffentlich wahrnehmbares Verhalten
  - Verwendung der Daten ausdrücklich zugestimmt
  - Annahme, das überwachte Objekt / die überwachte Person könnte Ziel oder Ort eines gefährlichen Angriffs werden
- Verboten: höchstpersönlicher Lebensbereich (zB WC)
- Arbeitsrechtliche Erfordernisse:
  - Betriebsvereinbarung (§ 96 ArbVG)
  - Wenn kein Betriebsrat vorhanden: Individualvereinbarung (§ 10 AVRAG)



## Videoüberwachung II

- Vorabkontrolle durch die Datenschutzkommission
  - Videoüberwachung erst nach der Durchführung der Prüfung durch die DSB aufnehmen
- Kennzeichnung der Videoüberwachung
- Auskunftsrecht bei Videoüberwachung (Mitwirkung des Betroffenen – genauer Zeitraum und Ort; sonst nur schriftliche Auskunft / Unkenntlichmachung Dritter)

## Sanktionen nach DSGVO I

- § 51 DSGVO: Datenverwendung in Gewinn- oder Schädigungsabsicht
  - Berufsmäßig anvertraute oder zugänglich gemachte oder widerrechtlich verschaffte Daten – einem anderen zugänglich machen oder veröffentlichen, obwohl schutzwürdige Geheimhaltungsinteressen an Daten
  - Strafraum bis zu einem Jahr Freiheitsstrafe

## Sanktionen nach DSGVO II

- § 52 Abs 1 DSGVO: Verwaltungsstrafbestimmung
  - Verwaltungsstrafe bis EUR 25.000,-:
    - widerrechtlicher Zugang zu Daten verschaffen
    - **Daten in Verletzung Datengeheimnis übermitteln**
    - entgegen rechtskräftigem Urteil nicht löschen/korrigieren
    - widerrechtlich löschen
    - sich Daten unter Vortäuschung falscher Tatsachen verschaffen
      - Verletzung von Rechten bereits stattgefunden

## Sanktionen nach DSGVO III

### –§ 52 Abs 2 DSGVO: Verwaltungsstrafbestimmung

- Verwaltungsstrafe bis EUR 10.000,-:
  - ohne Meldung od. von Meldung abweichend Daten ermitteln, verarbeiten, übermitteln
  - ohne Genehmigung ins Ausland übermitteln / überlassen
  - gegen Zusagen / Auflagen der DSB verstoßen
  - Offenlegungs- und Informationspflichten verletzen
  - Sicherheitsmaßnahmen außer Acht lassen oder nicht innerhalb Löschungsfrist löschen
  - noch keine Verletzung von Rechten, aber Unterlassungen, die Rechte des Betroffenen gefährden



## Ausblick

- Datenschutz-Grundverordnung der EU
  - Einheitliches Datenschutzrecht in allen Mitgliedstaaten
  - Betrieblicher Datenschutzbeauftragter für größere Unternehmen
  - Weitgehender Entfall von Meldepflichten
  - Vereinfachte Konzern-interne Datenübermittlungen, sofern Binding Corporate Rules
  - Datenportabilität
  - Strafen von bis zu 5% des Jahresumsatzes

**Copyright**



## Copyright - Inhalt

- Was ist ein Werk urheberrechtlich geschützt?
- Welche Rechte hat man nach dem Urheberrecht?
- Wem stehen diese Rechte zu und wie können sie übertragen werden?
- Copyright vs. Urheberrecht
- Rechtsfolgen von Urheberrechtsverletzungen
- Rechtsdurchsetzung in der digitalen Welt
  - Auskunftsansprüche gegen ISPs
  - Website-Sperren

# Wann ist ein Werk urheberrechtlich geschützt?

## Schutz setzt voraus

- eigentümliche
  - erforderliche Eigenart ist sehr gering (zB OGH 4 Ob 179/01d – Eurobike)
- geistige Schöpfung
  - von Maschinen automatisch generierte Werke nicht geschützt (zB OGH 4 Ob 105/11m – 123people)

auf den Gebieten der Literatur, der Tonkunst, der bildenden Künste, der Filmkunst.

Registrierung nicht erforderlich (≠ Patentrecht)

# Geschützt?



# Geschützt?

The screenshot shows the tele.ring website in a Microsoft Internet Explorer browser window. The address bar displays the URL: <http://web.archive.org/web/20000617063113/http://www.1012privat.at/>. The website header features the tele.ring logo and a search bar with the text "Gibt es Antworten auf häufige Fragen?". Below the header is a navigation menu with links for "Produkte", "Service", "Support", "Nachrichten", "Shopping", and "E-tainment".

The main content area includes a "Herzlich willkommen!" banner with a photo of a man sitting on a Motorola T 2288 mobile phone. Below this is a "tele.ring News" section with two items:

- Shop-Eröffnung in GRAZ: tele.ring kommt - vieles geht weiter!
- Für Fremdsprachen: geWAPnet!

There are also sections for "Messen & Events" and "Preisübersicht". The bottom of the page features several promotional tiles:

- Flash**: Twist the Night away
- 3 x gut haben!**: Im Festnetz 30 Minuten pro Monat
- 3 x gut haben!**: Im Internet 60 Minuten pro Monat
- Business**: tele.ring office - einfach professionell
- Handys Online**: Die besten Handys gibt's im Online Shop!
- Gratis Services**: Alles im Griff - vom Kino bis zur Verkehrsinfo ...

The footer of the website reads "Site by Pixelwings".



## Rechte nach dem Urheberrecht – 1/2

### Exklusive Verwertungsrechte

- Vervielfältigung
- Verbreitung – Werkstücke in körperlicher Form zugänglich machen
- Vermieten und Verleihen von Werkstücken
- Senden
- Öffentlich zur Verfügung stellen (auf individuellen Abruf)
- Öffentlich Vortragen/Aufführen/Vorführen
- Bearbeiten



## Rechte nach dem Urheberrecht – 2/2

### Urheberpersönlichkeitsrechte

- Recht auf Nennung als Urheber
- Schutz vor Verunstaltung

Sind nicht übertragbar → Urheberrecht als solches nicht übertragbar

## Wer ist Rechteinhaber?

Das Urheberrecht entsteht immer beim Schöpfer des Werks

- Jene natürliche Person, die das Werk geschaffen hat
- Auch Miturheberschaft mehrerer Personen möglich

Verwertungsrechte können allerdings übertragen werden

- Durch Gesetz: Verwertungsrechte an Software stehen Arbeitgeber zu
- Im Arbeitsverhältnis durch Kollektivvertrag
- Durch individuelle Vereinbarung (Lizenz)



# Lizenzarten

## Persönlicher Umfang

- Exklusive Lizenz: Nur Lizenznehmer darf nutzen
- Allein-Lizenz: Nur Lizenznehmer und Lizenzgeber dürfen
- Nicht-exklusive Lizenz: keine ausschließlichen Rechte

## Räumlich

- Weltweit vs. regional Beschränkt

## Sachlich

- Nur für best. Zwecke / nur best. Verwertungsarten

## Weitergabe

- Sub-Lizenzierbarkeit / Übertragbarkeit

# Ausnahmen vom Urheberrecht

## Die „Privatkopie“ (§ 42 UrhG)

- Zum eigenen (dh auch beruflichen) Gebrauch: Kopien auf Papier
  - Zum privaten Gebrauch: digitale Kopien (sofern Vorlage rechtmäßig – EuGH C-435/12 – ACI Adam)
- Festplattenabgabe: Als „gerechter Ausgleich“, sofern „bedeutender Nachteil“ (EuGH C-467/08b – Padawan)

## Flüchtige und begleitende Vervielfältigung (§ 41a UrhG)

- zB im Cache eines Web-Browsers (EuGH C-360/13 - Meltwater)
- Streaming von raubkopierten Filmen legal?



# Copyright vs. Urheberrecht

## U.S.-amerikanisches Copyright

- Urheberrecht als solches ist übertragbar
- „Works Made for Hire“ Doctrine: Dienstgeber ist Urheber
- Sehr schwache Urheberpersönlichkeitsrechte
- Betrachtungsweise des Urheberrechts
  - Ökonomische Perspektive: Monopolrechte als Anreiz
  - Urheberrecht als Eigentumsrecht

## Kontinentaleuropäisches Urheberrecht

- Als Ausfluss des Persönlichkeitsrechts

# Rechtsfolgen von Urheberrechtsverletzungen

- Unterlassungsanspruch
  - Wiederholungsgefahr muss nicht bewiesen werden
- Beseitigungsanspruch
  - Eingriffsgegenstände müssen vernichtet werden
- Anspruch auf Urteilsveröffentlichung
  - setzt ein berechtigtes Interesse voraus
- Anspruch auf angemessenes Entgelt
  - unabhängig vom Verschulden des Verletzers
- Schadenersatzanspruch
  - setzt Verschulden voraus
  - in Höhe der 2-fachen Lizenzgebühr □ Höhe des Schadens muss nicht bewiesen werden!



# Rechtsfolgen von Urheberrechtsverletzungen

- Inhaber eines Unternehmens haftet im Fall von Verletzungen in seinem Betrieb
  - Für angemessenes Entgelt (§ 88 Abs 1 UrhG)
  - Für Schadenersatz, wenn (1) Verletzung durch Bedienstete oder Beauftragte im Betrieb und (2) Unternehmensinhaber Verletzung bekannt war oder bekannt sein musste (§ 88 Abs 2 UrhG).

# Strafrechtliche Rechtsfolgen von Urheberrechtsverletzungen

- Gerichtliche Strafbarkeit
  - Urheberrechtsverletzungen sind grds strafbar (§ 91 UrhG)
  - Ausnahme:
    - unbefugte Vervielfältigung oder
    - unbefugtes Festhalten eines Vortrags oder einer Aufführung
    - jeweils zum eigenen Gebrauch oder unentgeltlich auf Bestellung zum eigenen Gebrauch eines anderen
  - Strafdrohung: bis 6 Monate; wenn „gewerbsmäßig“: bis 2 Jahre
  - Ist ein sog. Privatanklagedelikt: Opfer führt die Anklage

## Digitale Rechtsdurchsetzung – Auskunftspflichten von ISPs – 1/2

- Auskunftspflichten von Hosting-Providern (§ 18(4) ECG)
  - haben Name und Adresse eines Nutzers auf Verlangen dritten Personen zu übermitteln, sofern diese ein überwiegendes rechtliches Interesse an der Feststellung der Identität eines Nutzers glaubhaft machen
  - OGH 4 Ob 7/04i: Analoge Anwendung auf Access Provider
  - OGH 6 Ob 119/11k: Keine analoge Anwendung (§ 99 Abs 5 TKG 2003 nF)

# Digitale Rechtsdurchsetzung – Auskunftspflichten von ISPs – 2/2

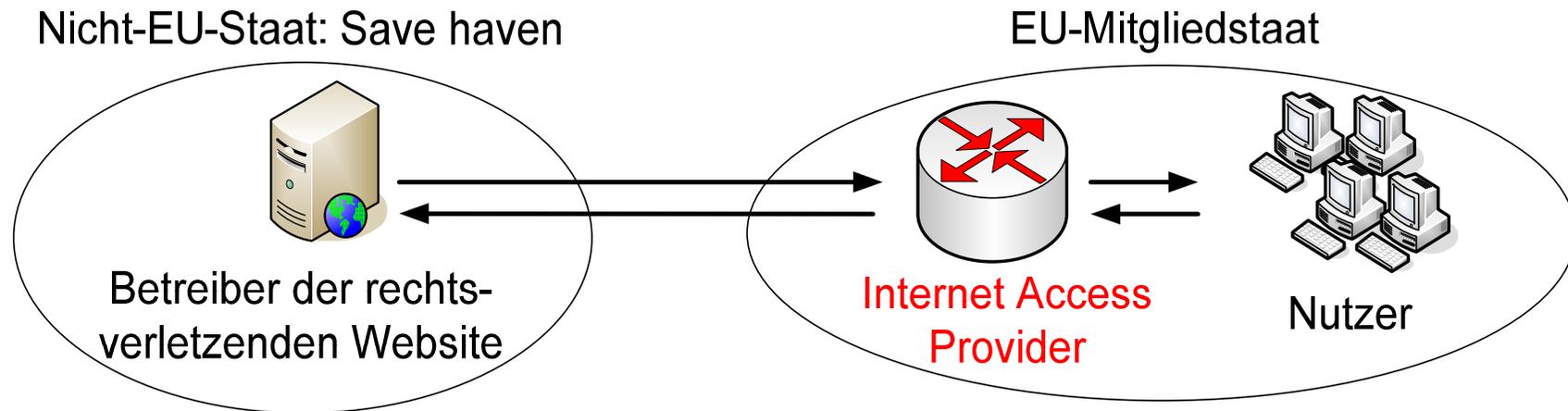
- Auskunftspflichten von Vermittlern (§ 87b Abs 3 UrhG)
  - bei Urheberrechtsverletzungen haben “Vermittler” dem Verletzten Auskunft über die Identität des Verletzers zu geben
  - EuGH C-557/07 – LSG v. Tele2: Auch Access Provider sind „Vermittler“
  - OGH 4 Ob 41/09x - MediaSentry II: Wenn Daten nicht mehr rechtmäßig vorhanden sind, dürfen sie nicht zu auskunftszwecken verarbeitet werden
    - Unterscheidung zwischen dynamischen und statischen IP-Adressen

# Digitale Rechts- durchsetzung – Website-Sperren

- Technische Rahmenbedingungen
- Rechtsgrundlagen
- Umsetzungsstand in den Mitgliedstaaten

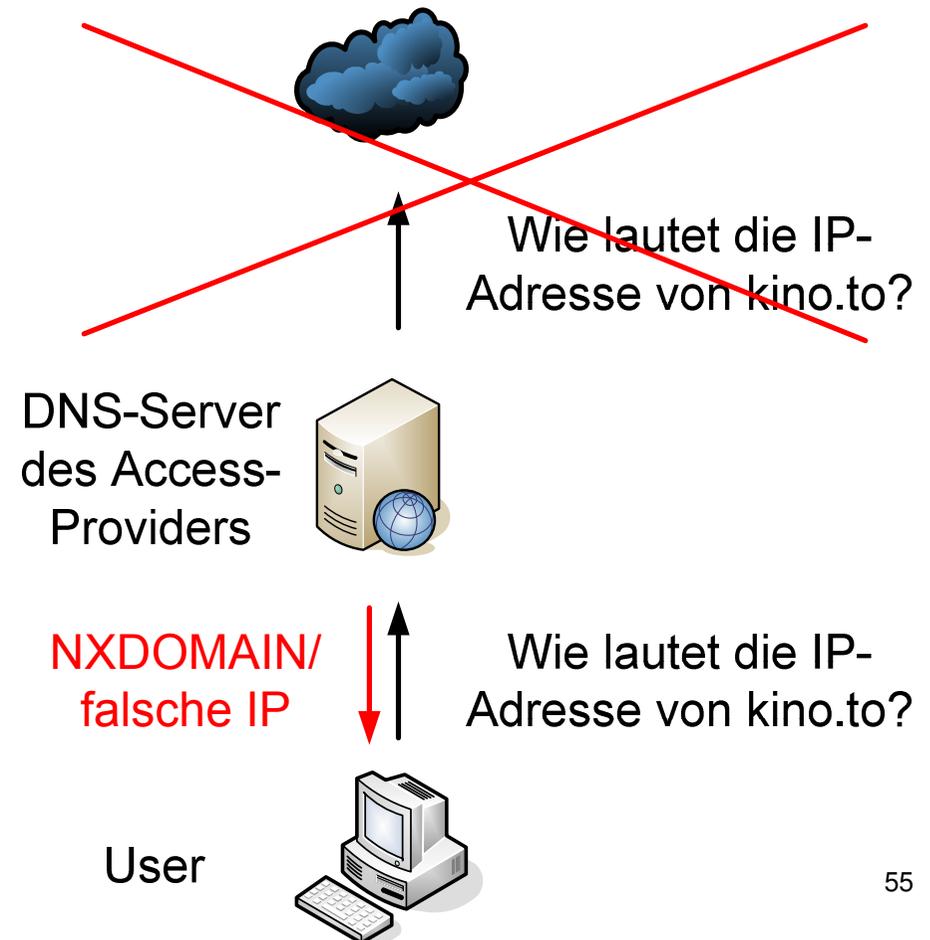


# Rechtsdurchsetzung gegen nicht greifbare Verletzer



# Funktionsweise von Website Blocking – Variante 1: DNS-Sperren

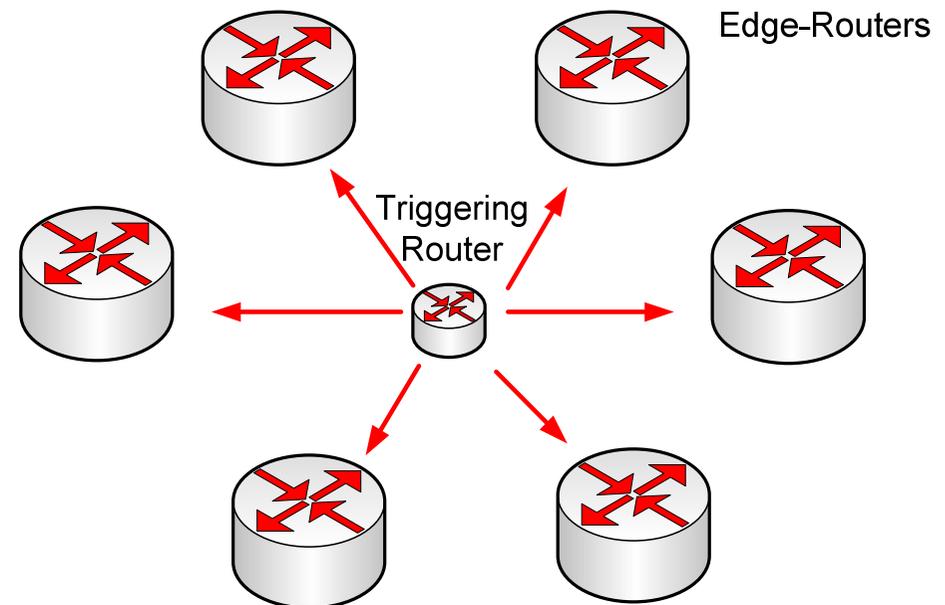
- DNS-Server des Access-Providers muss rekonfiguriert werden
- Umgehungsmöglichkeiten:
  - für User:
    - anderer DNS-Server
    - /etc/hosts
  - für Website
    - andere Domain



# Funktionsweise von Website Blocking – Variante 2: IP-Sperren

## IP-Sperre mittels Remote-Triggered Black Hole Filtering

1. Static Route zu Null0 Interface auf allen Edge Routers (zB für 192.0.2.0/24)
2. Am Triggering Router zB 192.0.2.1 als next hop für die zu sperrende IP konfigurieren
3. Verteilung der Route per iBGP an alle Edge Router

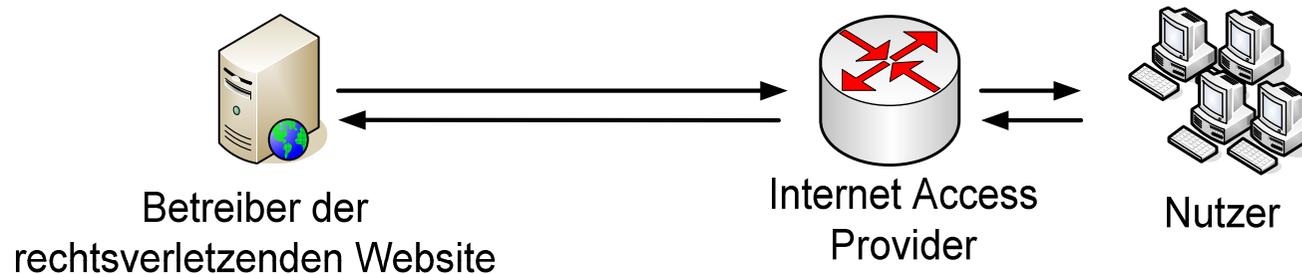


## Rechtsgrundlage für Website-Sperren – 1/3

- § 13 ECG: Access-Provider haften nicht für übermittelte Inhalte, wenn
  - die Übermittlung nicht veranlasst;
  - den Empfänger der übermittelten Informationen nicht auswählt &
  - die übermittelten Informationen weder auswählt noch verändert.
- § 19 Abs 1 ECG: § § 13 bis 18 ECG gelten nicht für Unterlassungsansprüche (vgl OGH 6 Ob 178/04a – Online-Gästebuch)
- § 81 Abs 1a UrhG (in Umsetzung von Art 8 Abs 3 Info-RL)
  - *Bedient sich [ein Urheberrechtsverletzer] der Dienste eines Vermittlers, so kann auch dieser auf Unterlassung nach Abs. 1 geklagt werden.*

## Rechtsgrundlage für Website-Sperren – 2/3

- Nutzung des Dienstes durch Dritten zur Urheberrechtsverletzung?
  - Wer ist Dritter?
  - “Nutzt” dieser den Dienst?



- EuGH C-314/12 - kino.to:
- Website-Betreiber ist rechtsverletzender Dritte
  - Dieser “nutzt” den Dienst der Access Provider seiner User

## Rechtsgrundlage für Website-Sperren – 3/3

- Vereinbarkeit von Sperr-Verfügungen mit
  - Grundrecht auf Erwerbsfreiheit der Access Provider (Art 16 GRC)
    - Rs C-70/10, Scarlet Extended v. SABAM: Kosten für Deep Packet Inspection sind unverhältnismäßig
    - Rs C-314/12, kino.to: auch Erfolgsverbot zulässig
  - Grundrecht auf Informationsfreiheit der Nutzer (Art 11 GRC)
    - Problem “Overblocking”
    - Rs C-314/12, kino.to: Nutzer müssen Rechtsbehelf gegen Sperre haben, sobald sie von dieser erfahren (in Österreich: Exszindierungsklage gem § 37 EO)

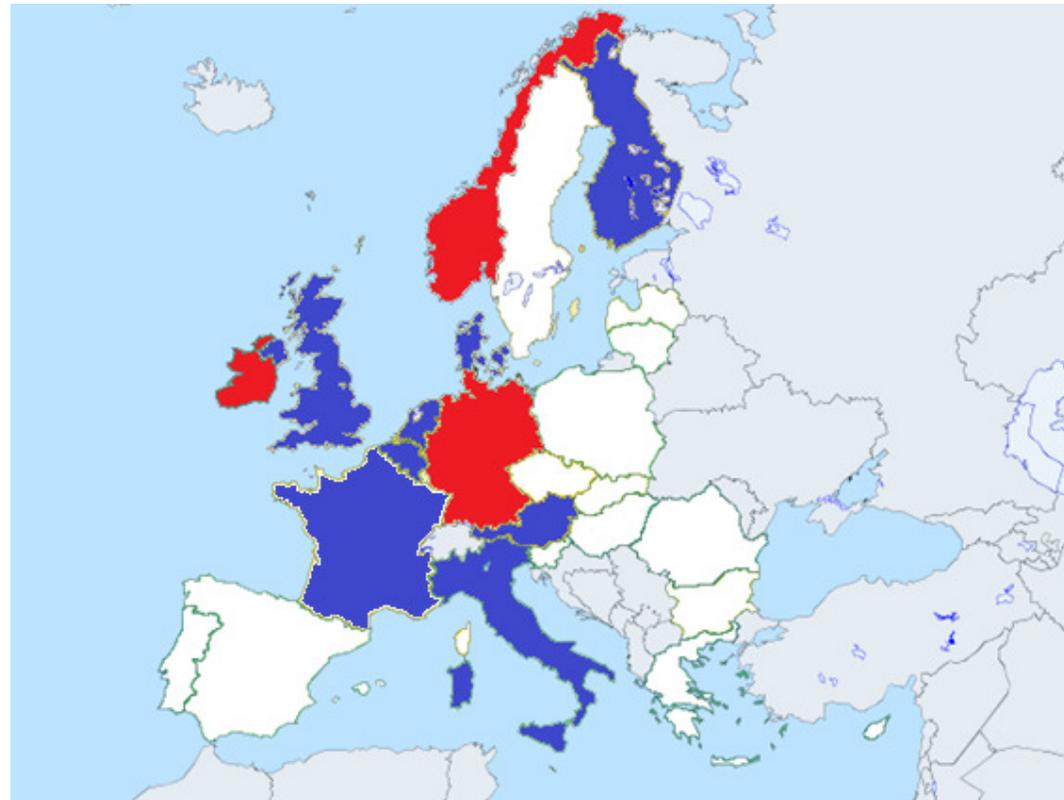
# Website-Sperrverfügungen in der EU

## Verfügung erlassen

- Österr. (4 Ob 71/14s)
- Belgien
- Dänemark
- Finnland
- Italien
- Niederlande
- Frankreich
- U.K.

## Anträge abgewiesen

- Deutschland
- Irland
- Norwegen (Nicht-EU)



## Kontakt

Baker & McKenzie  
Schottenring 25  
1010 Vienna  
Tel.: +43 (0) 1 24 250  
Fax: +43 (0) 1 24 250 600

**Dr. Lukas Feiler, SSCP**  
**[lukas.feiler@bakermckenzie.com](mailto:lukas.feiler@bakermckenzie.com)**

Die Baker & McKenzie - Partnerschaft von Rechtsanwälten, Wirtschaftsprüfern, Steuerberatern und Solicitors ist eine im Partnerschaftsregister des Amtsgerichts Frankfurt/Main unter PR-Nr. 1602 eingetragene Partnerschaftsgesellschaft nach deutschem Recht mit Sitz in Frankfurt/Main. Sie ist assoziiert mit Baker & McKenzie International, einem Verein nach Schweizer Recht. Mitglieder von Baker & McKenzie International sind die weltweiten Baker & McKenzie-Anwaltsgesellschaften. Der allgemeinen Übung von Beratungsunternehmen folgend, bezeichnen wir als "Partner" einen Freiberufler, der als Gesellschafter oder in vergleichbarer Funktion für uns oder ein Mitglied von Baker & McKenzie International tätig ist. Als "Büros" bezeichnen wir unsere Büros und die Kanzleistandorte der Mitglieder von Baker & McKenzie International.