



D O R D A
otto group

Profiling/Advertising/Dark Patterns (Deep Fakes)

7 March 2024

Simon Menke (Otto Group, Germany) and Nino Tlapak (DORDA, Austria)



Head Group IP & Data-Protection (Otto Group Holding)

- Focus: data protection, competition law, direct marketing, new media and e-commerce, copyright and trademark law, license agreements, IT law
- Head of Group IP & Data Protection since March 2019
- Before joining Otto in 2012: lawyer in a Hamburg-based firm specializing in Intellectual Property and Data Protection
- Regular speaker at relevant international conferences and meetings (eg OMR Legal Update, Datenschutzkongress)
- Frequently publishes articles, books and similar contributions on privacy hot topics

Simon Menke

Simon.Menke@ottogroup.com

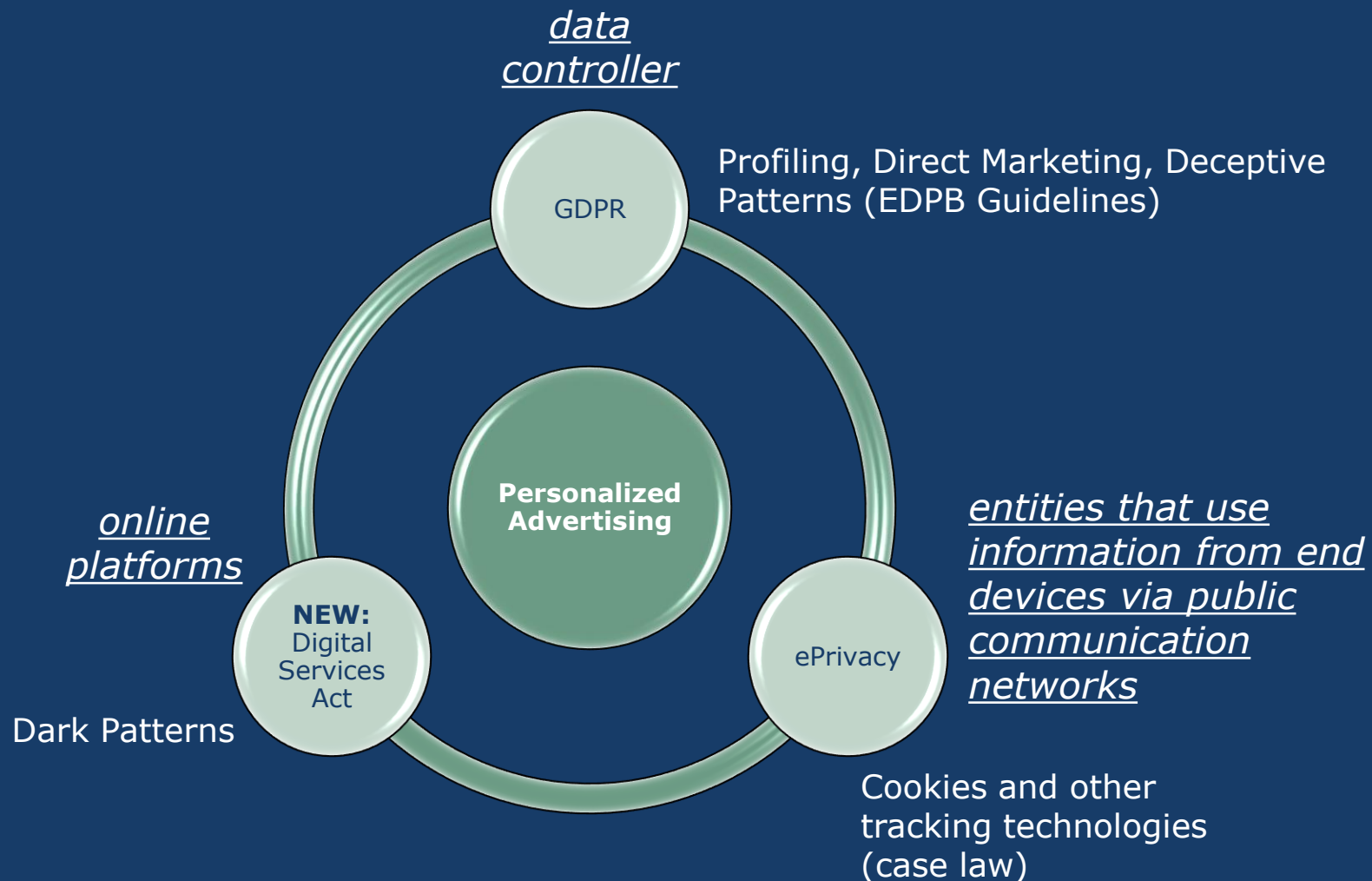


Partner and Co-Head of the Data Protection Team

- Focus: data protection, cybersecurity, IT-contracts with a focus on outsourcing and cloud contracts
- ILO Clients Choice Award for Blockchain 2023
- Recommended as Next Generation Partner in TMT and Data Privacy in the international legal directory "Legal 500" as well as Band 4 in "Chambers Europe"
- PrivacyConnect Co-Chair Vienna
- Lecturer for data protection law at master courses at the University of Vienna, FH Technikum Wien and FH Campus Wien as well as Vienna University for Business and Economics ("*Data Protection and New Technologies*") and Danube University Krems ("*Datenschutz und Privacy*")
- Regular speaker at relevant international conferences and meetings (IT Rechtstag; ITechLaw; Privacy Symposium; APD etc)
- Member of "*it-law.at*" and "*Privacyofficers.at*"

Nino Tlapak

nino.tlapak@dorda.at



1. Overview: New legal framework

Interplay of GDPR/e-Privacy Directive/DSA

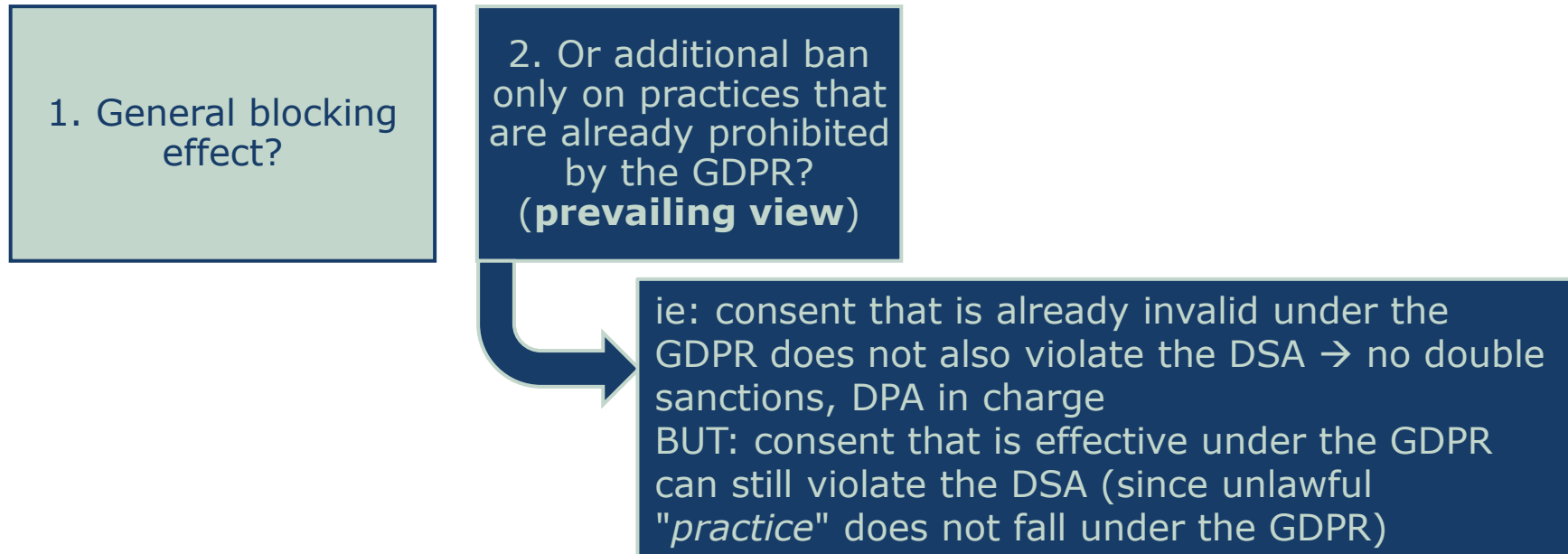
- DSA, applicable since 17 February 2024 to all in-scope entities, inter alia prohibits **Dark Patterns**:
 - **online interfaces of online platforms**
 - = hosting service providers that store and publicly disseminate information on behalf of users (eg social networks)
 - "*practices that materially distort or impair, either on purpose or in effect, the ability of recipients of the service to make autonomous and informed choices or decisions*" (Recital 67, Art 25 para 1 DSA)
 - restrictions on practices to encourage users to behave in certain ways

Key question:

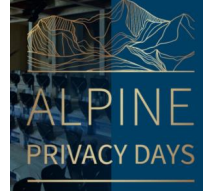
Does this also apply to the design of consent forms for direct marketing (GDPR) and cookies (ePrivacy)?

How the DSA and the **GDPR** interact:

- general disclaimer: DSA without prejudice to GDPR (Recital 10)
- specific disclaimer (Recital 67, Art 25 para 2):
 - *"rules on dark patterns should be interpreted as covering prohibited practices falling within the scope of this Regulation to the extent that those practices are not already covered" under the GDPR; and*
 - *"prohibition shall not apply to practices covered" by the GDPR*



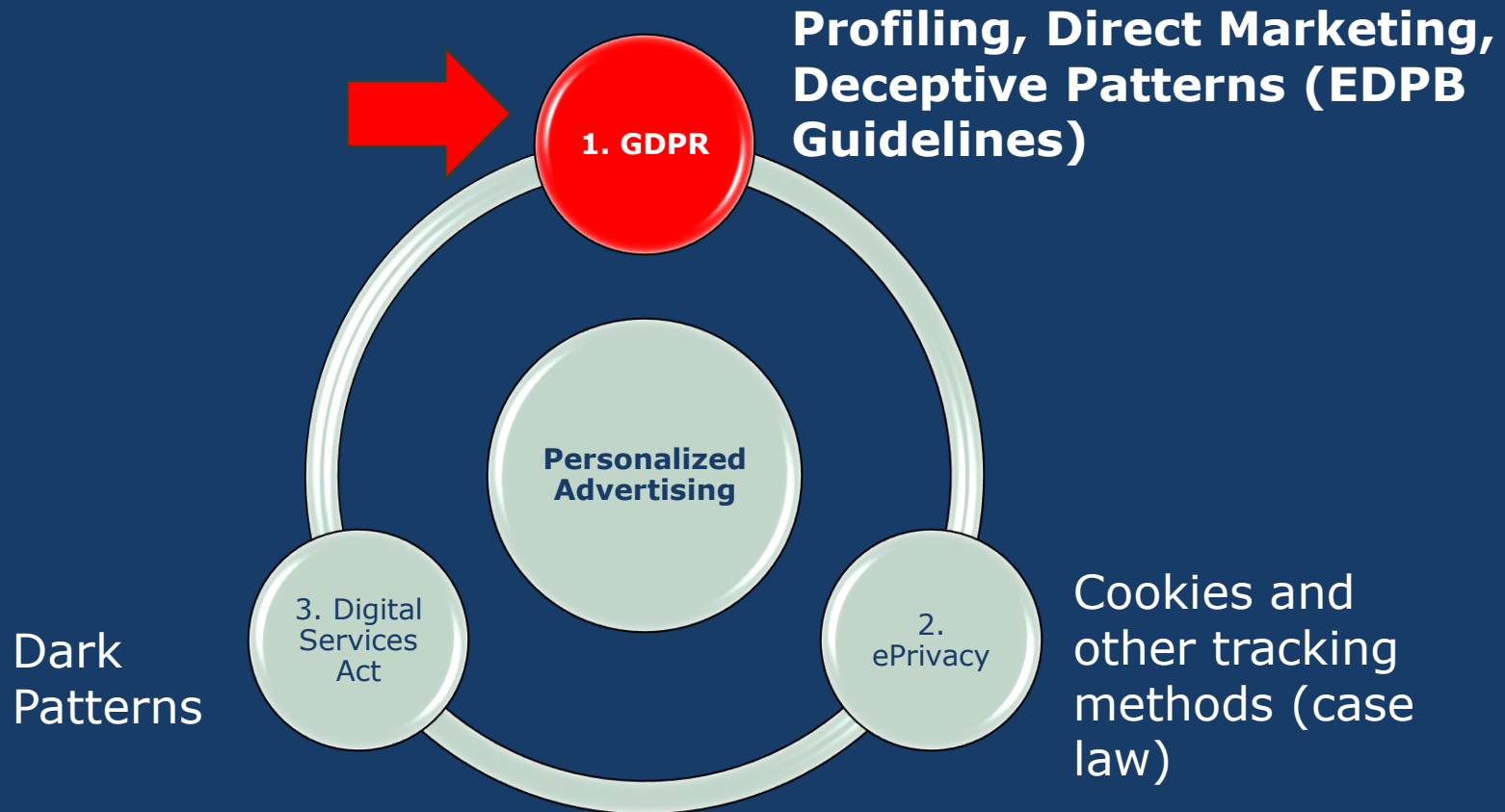
How the DSA and the **ePrivacy Directive** interact:



- not explicitly mentioned in the DSA
- **prevailing opinion thus** assumes that the **DSA does apply to cookie banners** of online platforms

Result:

YES, the DSA basically applies to the design of consent forms for direct marketing (GDPR) and cookie banners (ePrivacy) (of online platforms).



2. **GDPR**: Profiling and Direct Marketing

Landmark decision Meta/Bundeskartellamt

- **legitimate interests** are subject to balancing of interests (Recital 47 GDPR)
 - criteria (EDPB): intensity of **profiling** (Art 4 no 4 GDPR – level of detail and scope), extent to which data sources are linked, consequences for data subjects, etc

Findings CJEU C-252/21:

1. personalization of content is **not required to offer users the services of the social network** → fulfillment of contract thus **not** applicable
2. **legitimate interests**: compliance with the principle of necessity and data minimization, **user expectations are decisive**: (i) users cannot reasonably expect their data to be processed for the purpose of personalizing advertising without their consent; and (ii) particularly extensive processing

Norwegian Datatilsynet:

Meta must obtain the **voluntary consent of users**
 immediate action, responsibility lies with Irish DPC
confirmed by EDPB
 decision of the Irish DPC of 10 November 2023

Deceptive Patterns under the GDPR

- **EDPB has issued guidelines** on "*deceptive design patterns in social media platforms*" in March 2022 (Guidelines 3/2022 of 14 February 2023)

= "*attempt to influence users into making unintended, unwilling and potentially harmful decisions, often toward a decision that is against the users' best interests and in favour of the platforms interests*"

- EDPB specifies its interpretation of the **voluntariness and transparency of consent** in accordance with Art 7 GDPR
 - prohibition therefore does not result directly from the legal text or Recitals of the GDPR
 - as opposed to DSA (general explicit prohibition)

Inadmissible deceptive Patterns

Overloading: continuous mass of requests, information, options or possibilities to deter users from going further and make them keep or accept certain data practice

Skipping: interface or user journey that users do not think about data protection aspects

Stirring: affecting the choice by appealing to emotions or using visual nudges

Obstructing: hindering or blocking users in their process of obtaining information or managing their data

Fickle: unstable and inconsistent design, making it hard to figure out nature of processing, how to make a choice, and to find controls

Left in the dark: hide information or controls or leave users unsure of how data is processed and which controls they have

- **Best practices:** cross-device consistency, coherent wordings, providing definitions, use of examples, explaining consequences, etc

Examples of Deceptive Patterns:

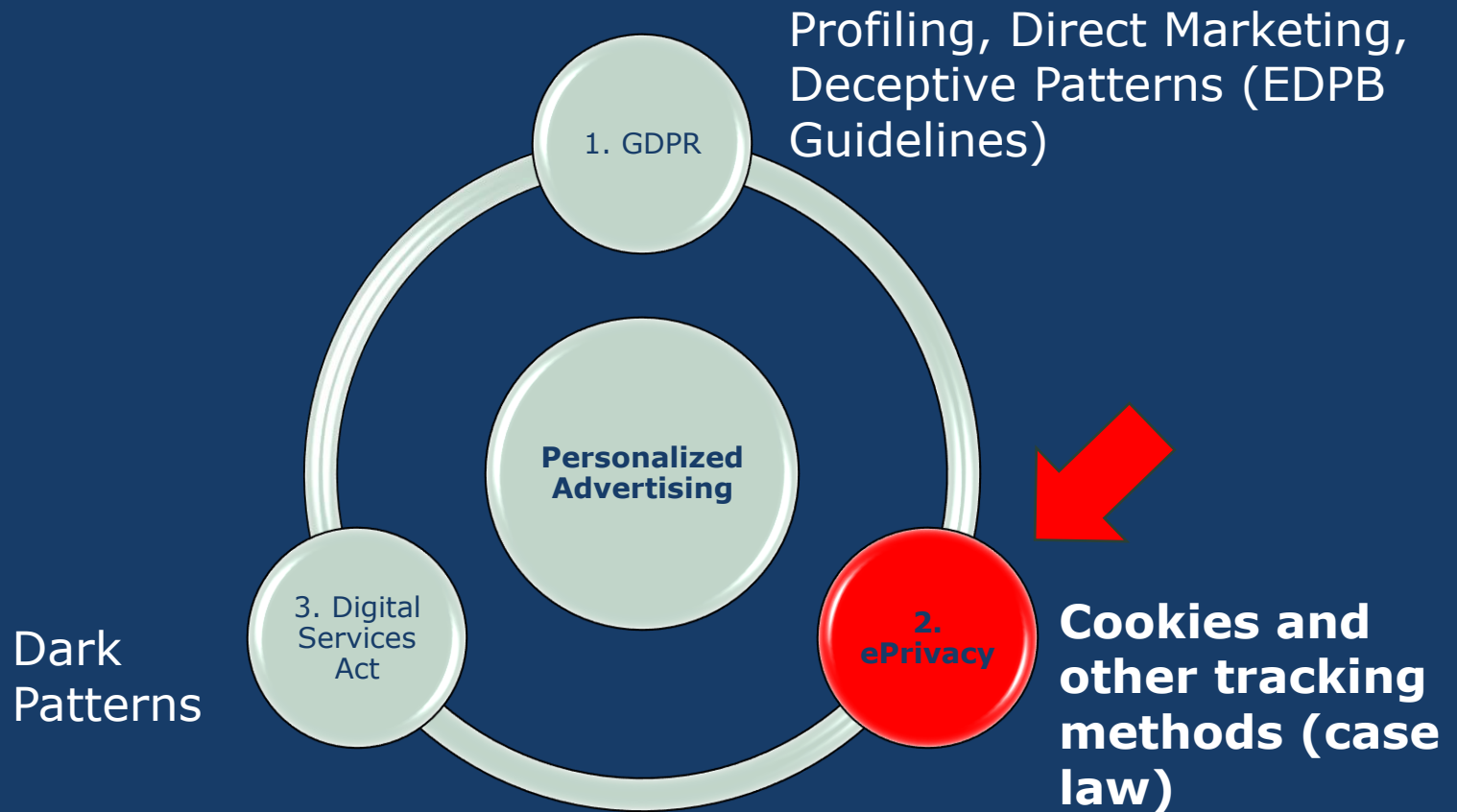
Example 31: Users want to manage the permissions given to the social media platform based on consent. They have to find a page in the settings related to those specific actions and wish to disable the sharing of their personal data for research purposes. When users click on the box to untick it, nothing happens at the interface level and they get the impression that the consent cannot be withdrawn.

Example 33: A social media provider does not provide a direct opt-out from a targeted advertisement processing even though the consent (opt-in) only requires one click.

Example 34: Information to withdraw consent is available from a link only accessible by checking every section of their account and information associated to advertisements displayed on the social media feed.

Example 35: In this example, when users create their account, they are asked if they accept their data to be processed to get personalised advertising. In case users do not consent at sign-up to this use of their data, they regularly see – while using the social network – the prompting box illustrated above, asking if they want personalised ads. This box is blocking them in their use of the social network. Being displayed on a regular basis, this **Continuous prompting** is likely to fatigue users into consenting to personalised advertisement. Furthermore, in this interface the **Hidden in plain sight** pattern⁶² is also used, as the action to accept ads is far more visible than the refusing option.

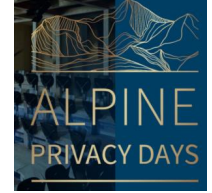
Example 50: The social media platform offers different versions (desktop, app, mobile browser). In each version, the settings (leading to access/objection etc.) are displayed with a different symbol, leaving users who switch between versions confused.



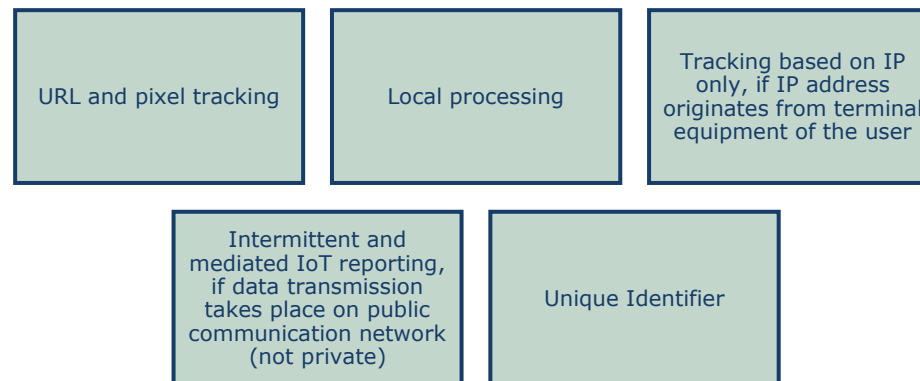
3. ePrivacy: Cookies and other tracking methods

Cookies and other tracking methods

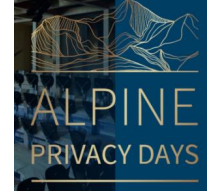
(Art 5 para 3 ePrivacy Directive)



- *lex specialis* vis a vis GDPR (Art 95 GDPR)
 - key elements: information, terminal equipment, public communication network, gaining access or storage
 - however, consent requirements are not regulated → GDPR applies
- → all marketing, tracking and analysis cookies **require consent** (eg meta pixels)
- ePrivacy addresses **initial data collection**: permissibility of further processing is also assessed on the basis of the GDPR
- ePrivacy also applies to **other tracking methods**:
 - see EDPB Guidelines 2/2023 on Technical Scope of Art 5(3) of ePrivacy Directive of 14 November 2023
 - inter alia:



EDPB Guidelines on design of cookie banners



- EDPB has set up **cookie banner task force** for coordination purposes – final report of January 2023

1. No reject Button on the first layer

2. Pre-ticked boxes

3. Deceptive button colours and contrast

4. Legitimate interest claimed, list of purposes

5. Inaccurately classified essential cookies

6. No withdraw icon

- Findings on **deceptive button colours and contrast**:
 - general banner standard concerning colour and/or contrast cannot be imposed on data controllers → **case-by-case verification**
 - whether contrast and colours used are **not obviously misleading** for the users and do not result in an unintended and, as such, invalid consent
 - inadmissible in any case: contrast between the text and the button background is so minimal that the text is **unreadable to virtually any user**
- → overall, **only general guidelines, no specific requirements**

Lessons learnt based on AT cookie banner decisions

- Austrian DPA:
 - **FAQ on cookies**: no nudging, reject button must not be less visible
 - however, **case law significantly stricter** than FAQ and EDPB Guidelines:
- thousands of warning letters since May 2021 and numerous (copy paste) complaints/DPA procedures, lessons learnt:

"Accept" button on **first level** of cookie banner

- user must be able to recognize "Reject" option → first layer
- **visually equivalent option** ([exact] same colour, contrast, size of buttons)
- obvious **rejection of the link design**

reference to **right of withdrawal**

- implementation in the **footer or as a floating symbol and**
- **direct reference in the cookie banner** where the right of revocation can be exercised (eg *"You can revoke your consent at any time without giving reasons, eg in the footer of the website under 'Manage website cookies'"*)

- But: **inconsistent case law in Europe**
 - **identical (!) cookie banner** was assessed differently in AT (not compliant) and DE (admissible)

Pay or OK

- choice when visiting the website for the first time: either consent to data processing through marketing cookies or paid "*PURE*" subscription
- Austrian DPA basically has confirmed permissibility
- prerequisites:

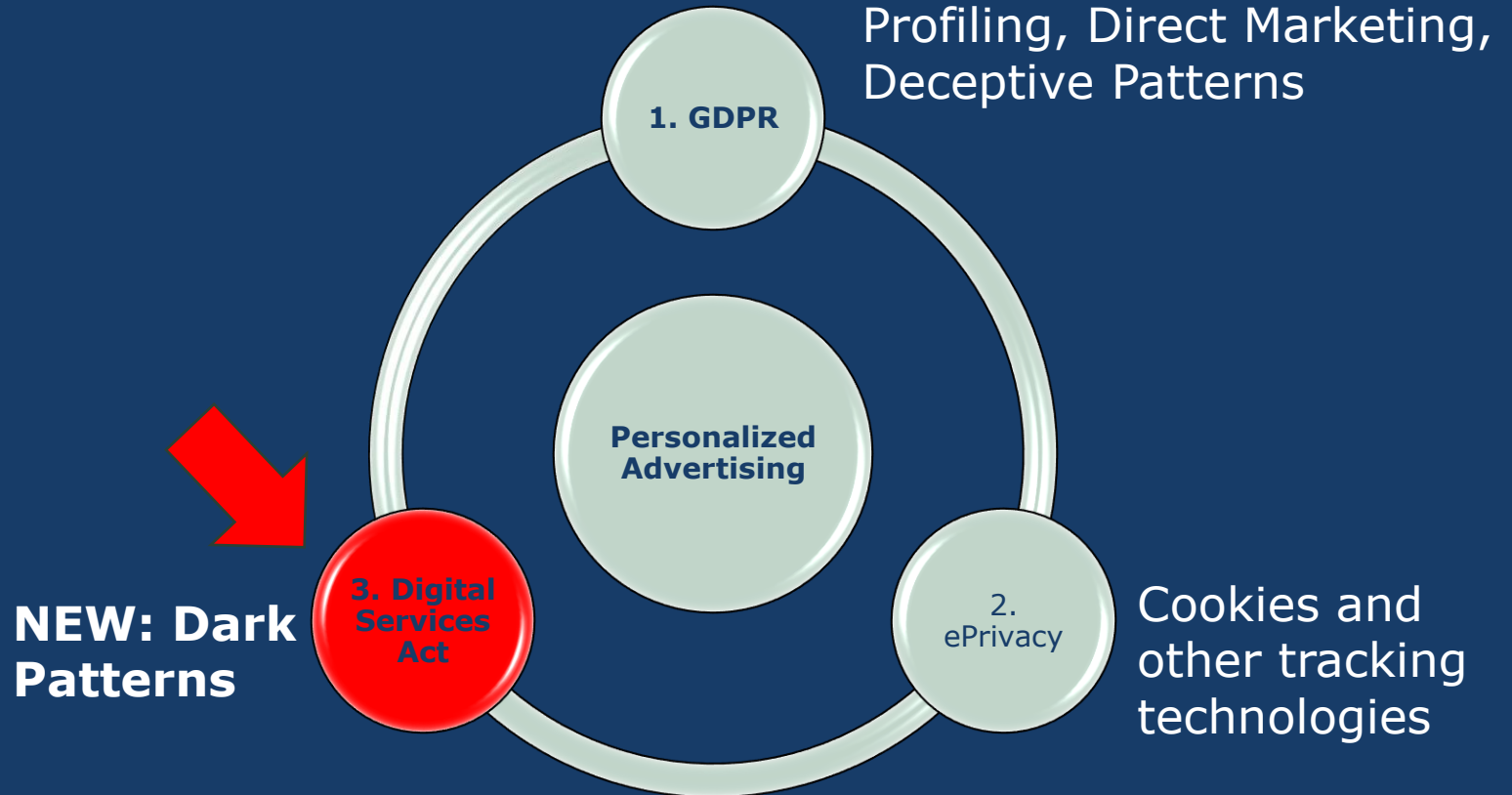
1. equivalence of the services → reasonable and fair price for the paid option, not a completely unrealistically high price

2. no data may be processed for advertising purposes with the paid alternative

- consent is only not voluntary if there are **significant negative consequences** or a risk of deception, intimidation or coercion in the event of refusal
 - *lower standard compared to dark patterns?*
- **pending procedure against Meta:** consent to personalized advertising or paid subscription costs EUR 12.99 per month – equivalence?

(Third-party) Cookieless future?

- companies are currently preparing for **abolition of third-party cookies**
 - eg Google will gradually discontinue support for third-party cookies as early as 2024, Apple has already done so
- **focus on first-party data**
 - **Server-side-tracking** instead of client-side-tracking (without cookies)
 - **Data Clean Rooms** for the comparison of first-party data and planning of personalized campaigns (only first-party cookies)
 - however, various alternative tracking technologies such as unique identifier are regarded equivalent to cookies (see EDPB Guidelines)



4. DSA: Ban on dark patterns

Overview: **DSA prohibits Dark Patterns**

- = "*practices that materially distort or impair, either on purpose or in effect, the ability of recipients of the service to make autonomous and informed choices or decisions*" (Recital 67, Art 25 para 1 DSA)
- **three examples**, but European Commission will issue **guidelines**
- inadmissible "*exploitative*" design patterns:

emphasizing certain choices through visual, acoustic or other elements when users are asked to make a choice;

repeatedly asking users to make a choice when that choice has already been made;

making the termination of a service significantly more cumbersome than the registration;

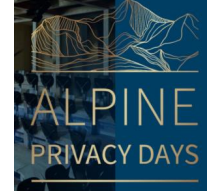
making certain choices more difficult or time-consuming than others;

make it disproportionately difficult to cancel purchases or unsubscribe from a particular online platform;

disproportionately influence users' decision-making through default settings that are very difficult to change; or

distort and impair choices

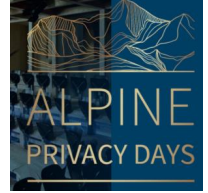
Prohibition of greater emphasis (Art 25 para 3 lit a DSA)



- addresses, among other things, the design of consent management platforms
- **misdirection pattern:**

A screenshot of the OTTO website's homepage. The browser address bar shows 'https://www.otto.de'. The OTTO logo is in the top left. A search bar with the placeholder 'Wonach suchst du?' is in the top center. Navigation links for 'Service', 'Mein Konto', 'Merkzettel', and 'Warenkorb' are in the top right. A horizontal menu lists various product categories like 'Weihnachten', 'Damen-Mode', 'Herren-Mode', etc. A prominent red banner across the middle of the page reads '20% auf ausgewählte Wäsche und Homewear'. Below this, a large white cookie consent banner is displayed. The banner has the title 'Cookies und andere Technologien erlauben?' and a paragraph of text explaining the use of cookies. At the bottom of the banner are three buttons: a large red 'OK' button, and two smaller links, 'Einwilligung ablehnen' and 'Mehr Informationen'.

Repeated request to make a selection (Art 25 para 3 lit b DSA)



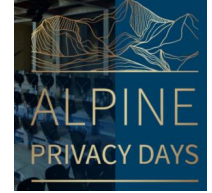
- addresses the repeated display of cookie consent options where users have already rejected web tracking
- such display could have the consequence that consent given is invalid due to the lack of "*voluntariness*" (Art 4 para 11 GDPR)
 - GDPR applies in addition to the DSA (Art 2 para 4 lit g DSA)

5. Open questions and legal uncertainties

Unclear relationship of DSA/GDPR/DSA

1. Why is the European legislator creating a legal requirement in the DSA that addresses the design of eg cookie consent banners when this is **already regulated** by the GDPR (and ePrivacy Directive) (with the same content) and expressly states that the requirements of Art 26 DSA go beyond those of the GDPR?
2. Prohibited practices of the DSA are similar to EDPB's Deceptive Patterns, but **not identical**
 - it is thus possible that practices are permitted under the GDPR and prohibited under the DSA and vice versa
3. furthermore: "legitimate practices, for example in advertising, that are in compliance with Union law should not in themselves be regarded as constituting dark patterns"
 - What is to be regarded "*legitimate*"? → **unclear**

Problematic interplay of DSA/GDPR/ePrivacy Directive



- if Art 25 DSA was applicable alongside the ePrivacy Directive and the GDPR, this would result in a **fragmentation of requirements**
 - eg different requirements would apply to cookie banners of online stores than to cookie banners of online marketplaces
- the legislator intended to avoid such fragmentation:
 - overall, the GDPR shall remain unaffected
 - practices already covered by the GDPR should not be prohibited
 - what is otherwise permitted under Union law should not "*per se*" be considered a dark pattern
- nevertheless, **reciprocal influence** deceptive/dark patterns will take place
- in addition, the relationship will become **even more complex** in the future because the DMA and the AI Act also contain corresponding regulations on dark patterns

THANK YOU FOR YOUR ATTENTION

D O R D A

Mag Nino Tlapak, LL.M.

T: +43 1 533 47 95 – 23

nino.tlapak@dorda.at



Client Choice Award Lexology 2023: Blockchain

TIER 1 Legal500 2007-2023: TMT

TIER 1 Legal500 2020-2023: Data Privacy & Data Protection

TIER 1 Legal500 2021-2023: Intellectual Property

BAND 1 Chambers Europe 2008-2023: TMT:IT

DORDA Rechtsanwälte GmbH · Universitätsring 10 · 1010 Wien · www.dorda.at

otto group

Dr. Simon Menke

Head Group IP & Data-Protection

Otto Group Holding

Simon.Menke@ottogroup.com