INFOLAW
WWW.INFOLAW.AT

DORDA

Art 22 DSGVO

KI und automatisierte Einzelentscheidungen

4.5.2023

Nino Tlapak

Partner and Co-Head des Datenschutz Teams bei DORDA

- Universität Wien, Mag iur 2012
- Universität Wien, Universitätslehrgang Medien- und Informationsrecht, LL.M. (IT-Law) 2013
- Fachliche Schwerpunkte: Datenschutz, Cybersecurity, IT-Verträge mit Schwerpunkt auf Outsourcing und Cloud-Verträge
- ILO Clients Choice Award für Blockchain 2022
- Empfohlen als Next Generation Partner im Bereich TMT und Data Privacy im renommierten internationalen Handbuch "Legal 500" sowie in Band 4 in "Chambers Europe"
- PrivacyConnect Co-Chair Vienna
- Vortragender für Datenschutz bei Master-Lehrgängen an der Universität Wien, FH Technikum Wien und FH Campus Wien sowie Donau Universität Krems ("Datenschutz und Privacy")
- Regelmäßiger Vortragender bei einschlägigen Konferenzen und Tagungen (IT Rechtstag; ITechLaw; Privacy Symposium; APD etc)
- Mitglied von "www.it-law.at" und "Privacyofficers.at"

Nino Tlapak

nino.tlapak@dorda.at

Agenda

1. Abgrenzung Profiling/ADM und Überblick
2. Tatbestandsmerkmale von ADM
   - Entscheidung
   - Ausschließlichkeit
   - rechtliche Wirkung / Beeinträchtigung
3. Exkurs: Kreditwürdigkeits-/Bonitätsprüfung (Scoring) und Schufa-Verfahren
4. To Dos bei Vorliegen einer ADM

Abgrenzung anhand der DSGVO

- Startpunkt: **Digitalisierung**
  - iaR verbunden mit automatisierter Verarbeitung (zB KI)
- **Profiling** (Art 4 Z 4 DSGVO)
  - "*jede Art der **automatisierten Verarbeitung** […], um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, **zu bewerten**, insbesondere um **Aspekte** bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, […] **dieser natürlichen Person zu analysieren oder vorherzusagen***"
  - Use Cases: Kundensegmentierung (Marketing), personalisierte Werbung
- **ADM** (Art 22 DSGVO)
  - "*eine **ausschließlich** auf einer **automatisierten Verarbeitung** – einschließlich Profiling – beruhenden **Entscheidung** […], die ihr gegenüber **rechtliche Wirkung** entfaltet oder sie **in ähnlicher Weise erheblich beeinträchtigt***"
  - Use Cases: Bonitätsprüfungen (Schufa, CRIF, KSV), Betrugsprüfung, ADM bei Vertragsabschluss (zB Versicherung, Kredit)

Überblick Profiling

- keine spezifischen Regelungen

- **berechtigte Interessen** – relevante Kriterien (EDSA):
  - Detaillierungsgrad und Umfang der Profile
  - Auswirkungen auf Betroffene
  - Garantien für eine faire, nicht diskriminierende und korrekte Profilerstellung

- **einschlägige Rechtsprechung**
  - insbesondere zur Einwilligung und zu (weitergehenden) **Informationspflichten**

Überblick Profiling

- Beispiel: Persönlichkeitsprofile auf Basis von Webtracking
  - vgl ErwGr 24 und 30 DSGVO

- **Mindestmaß an Verknüpfung und Interpretation**
  - bloße statistische Auswertung über Käufergruppen ist keine relevante Persönlichkeitsbewertung

- aber **kein hoher Komplexitätsgrad notwendig**
  - auch Bewertung und Kategorisierung von Nutzern für Werbezwecke ausreichend

- löst detailliertere Informationspflichten aus
  - vgl ErwGr 60 DSGVO: Bestehen + Folgen

Praxisbeispiel: Leistungsüberwachung

- **Einwilligung** der Mitarbeiter zur Nutzung eines **GPS-Systems für firmeneigene Fahrzeuge**
- Zweck:
  - Schutz/Sicherheit des Firmeneigentums
  - Erleichterung der monatlichen Abrechnung mit der Leasinggesellschaft
  - Routenplanung und -optimierung
  - Versicherungsbonus
- Speicherdauer: 93 Tage
  - laut DSB ermöglicht GPS-Tracking die Erstellung von Leistungsprofilen (dh wie effizient/pünktlich der Mitarbeiter arbeitet)
  - aber: Kein Fall von ADM (Art 22)
- DSB (DSB-D213.658/0002-DSB/2018):
  - **kein klar erkennbarer Nutzen für den Arbeitnehmer**
  - Einwilligung daher **nicht freiwillig und unwirksam**

Überblick ADM

- **generell unzulässig** ohne Intervention eines Menschen
  - **Ausnahmen für nicht-sensible Daten**:
    - erforderlich für Abschluss/Erfüllung eines Vertrags;
    - legitimiert durch EU oder nationales Recht; oder
    - ausdrückliche Einwilligung
      - nicht jedoch berechtigte Interessen
  - **Ausnahmen für sensible Daten**:
    - nur ausdrückliche Einwilligung oder öffentliche Gesundheitsinteressen
    - Zugang zu Gesundheitsdiensten = jedenfalls einschlägige Entscheidung

- Informationspflichten + weitere geeignete Maßnahmen

Wann liegt eine "Entscheidung" iSv Art 22 vor?

- keine Legaldefinition
  - ErwGr 71: auch "*Maßnahmen*"

- Verständnis des allgemeinen Sprachgebrauchs:
  - Treffen einer Wahl zwischen mehreren Alternativen
  - nach Bewertung, Abwägung, Ermessensausübung

- GA *Pikamäe* (C-634/21, SCHUFA):
  - verbindliche "*Auffassung*" oder "*Stellungnahme*" zu bestimmten Sachverhalt
  - **weit zu verstehen**: rechtliche, wirtschaftliche, soziale Auswirkungen
  - **einzelfallabhängige Prüfung** erforderlich

- bloße maschinelle Abarbeitung von zwischen Verantwortlichen und Betroffenen vereinbarten Wenn-dann-Regeln daher grds **keine ADM**

Abgrenzungsbeispiel zur "Entscheidung"

1. **Mitarbeiter** entscheidet anhand einer 10-Punkte-Checkliste, ob er einen Reiseversicherungsvertrag mit einem bestimmten Kunden abschließen darf. Er darf nicht abweichen und hat keinen Spielraum.
   - Mitarbeiter "*entscheidet*", Art 22 ist nicht anwendbar

2. **automatisiertes System** verwendet dieselbe 10-Punkte-Checkliste.
   - inhaltliche "*Entscheidung*" bereits vor der Automatisierung (dh durch die Erstellung der Liste) getroffen, Art 22 daher wohl nicht anwendbar
   - bei (zu) strenger Interpretation würden selbst triviale Prozesse darunter fallen
     - **auch überwiegende Ansicht in der Lehre**, wenngleich mit divergierenden Zugängen
     - auch die DSB thematisierte in ihrer Entscheidung zu Handvenenscannern als Mittel der Zutrittskontrolle Art 22 DSGVO nicht

Wann beruht die Entscheidung "ausschließlich" auf einer automatisierten Verarbeitung?

Frage nach relevanter Schwelle menschlicher Intervention:

- dass Algorithmus von natürlicher Person programmiert wurde und nach deren Regeln "*handelt*", schließt Tatbestandsmäßigkeit nicht aus
- Parlamentsentwurf: "*based solely or predominantly on automated processing*" → nicht in endgültige Fassung übernommen
- Telos: Verbot von Entscheidungen "*ohne jegliches menschliches **Eingreifen***" (ErwGr 71)
  - pro forma-Prozesse reichen nicht aus (WP215 rev 01, 22)
  - ebenso wenig bloße ex post-Kontrolle auf Antrag (Art 22 Abs 3 DSGVO e contrario)
  - Eingreifen – dh **Einwirken auf Ergebnis** – **durch den Menschen muss dennoch gewährleistet sein**:
    - zB mit Handlungsanweisungen, Richtlinien und Schulungen (BVwG)
    - Fach- und Entscheidungskompetenzen und Spielraum des Mitarbeiters
    - Funktionsweise und Logik des Algorithmus muss er jedoch nicht im Detail kennen

Abgrenzungsbeispiele zur "Ausschließlichkeit"

Keine ADM:

- **Richtigkeits- und Plausibilitätskontrolle** durch einen Menschen, der die maschinell generierte Entscheidung auch adaptieren kann
- **Bloße Vorauswahl** durch System (Predictive Analytics)

ADM:

- **Entscheidung** über Vertragsabschluss **ohne jedwede menschliche Intervention**
- **Cut off-Entscheidungen**: Ausführung Score- oder sonstiger maschinell generierter Wert durch Mitarbeiter ohne eigene Überlegungen, kein Eingriffswille und keine Eingriffsmöglichkeit

Abgrenzungsbeispiele zur "Ausschließlichkeit"

- Arbeitsmarktchancen Assistenz-System des AMS, Rechtsgrundlage: **AMSG**
  - berechnet die **Wahrscheinlichkeit** der Wiedereinstellung
  - berechnet aus 13 Merkmalen (ua Altersgruppe, Geschlecht, Ländergruppe)
  - drei Kategorien: hohe, mittlere und niedrige Chancen (**Profiling**)
- **Ausrichtung der Fördermaßnahmen** auf mittlere Chancen
- Ergebnisse sind jedoch nur Ausgangspunkt, endgültige Entscheidung wird von Beratern getroffen
  - gemäß den internen Leitlinien **müssen Berater** bei ihrer Entscheidung **zusätzliche Kriterien berücksichtigen** (zB Motivation und Selbsthilfepotenzial des Arbeitssuchenden)
- DSB: unzulässig; **BVwG: zulässig, Art 22 nicht anwendbar**
  - BVwG 27.1.2021, W256 2235360-1

Wann liegt eine "rechtliche Wirkung oder äquivalente erhebliche Beeinträchtigung" vor?

1. **Rechtliche Wirkung:**
   - Entscheidung beeinträchtigt rechtlichen (**insb gesetzlichen/vertraglichen**) Status des Betroffenen
   - Auswirkung auf vertragliche Rechte (WP251 rev.01, 23)
     - zB automatische Vertragsbeendigung bei Zahlungsverzug
   - automatisierte Ablehnung von Gewerbeberechtigungen oder anderen behördlichen Genehmigungen

2. **Äquivalente erhebliche Beeinträchtigung:**
   - Potential, die Umstände, das Verhalten oder die Entscheidungen eines Betroffenen erheblich zu beeinflussen
     - zB Berufs- oder Privatleben, Vermögensverhältnisse
   - "*erheblich*" → **nicht jede geringfügige Veränderung** von faktischen Verhältnissen
     - EDSA: "***umfassend bzw erwähnenswert***" (WP251 rev 01, 23)
   - (zB Preis-)Diskriminierung; automatisierte Ablehnung eines Online-Kreditantrags oder einer Online-Bewerbung

Abgrenzungsbeispiele zur "Beeinträchtigung"

- **EDSA**
  - erhebliche Beeinträchtigung der Umstände, des Verhaltens oder der Entscheidungen des Betroffenen;
    - Beeinträchtigung über längeren Zeitraum oder dauerhaft **oder**
    - im worst case Ausschluss/Diskriminierung

- Grenzziehung auch lt EDSA schwierig

- Parameter / Beispiele:
  - wirken sich auf finanzielle Lage einer Person aus (zB Kreditwürdigkeit)
  - betreffen Zugang zu Gesundheitsdienstleistungen
  - verwehren Zugang zu Arbeitsplätzen oder benachteiligen Personen ernsthaft
  - wirken sich auf Zugang zu Bildung aus (zB Hochschulzulassungen)

Abgrenzungsbeispiele zur "Beeinträchtigung"

- ob auch Entscheidungen mit (ausschließlich) **positiven** Auswirkungen unter Art 22 DSGVO fallen, ist **noch offen**
  - keine Rechtsprechung, keine Guidelines
  - unterschiedliche Ansichten in der Lehre
  - Wortinterpretation: DE "*beeinträchtigen*"
    - im allgemeinen Sprachgebrauch iZm Verschlechterung/negativer Wirkung gebraucht
    - so auch Wortlaut ErwGr ("*Ablehnung*", "*Absage*")
  - **ABER**: EN "*affect*" vs FR "*afecter*" – offenerer Wortlaut

- keine äquivalente erhebliche Beeinträchtigung:
  - § 4g EpiG: Versand von Erinnerungen an Auffrischungsimpfungen
  - marketingbezogenes Profiling, Kundensegmentierung

  → daher: (bloßes) Profiling, um Entscheidungsfindung zu unterstützen, ist weder verboten noch eingeschränkt durch Art 22

Abgrenzungsbeispiele zur "Beeinträchtigung"

Kundensegmentierung unstrittig "*nur*" Profiling, das Gleiche gilt grds für **personalisiertes Marketing**:

- EDSA:
  - nur individualisierte – dh auf Profiling beruhende – Werbemaßnahmen und individualisierte Social-Media-Kommunikation **mangels Beeinträchtigung iaR keine ADM** (WP215 rev01, 24)
  - **nur in Ausnahmefällen** durch zB:
    - eingreifenden Charakter des Profiling-Prozesses (zB Tracking über mehrere Websites);
    - die Erwartungen und Wünsche des Betroffenen;
    - die Art und Weise der Werbeanzeige;
    - die Ausnutzung von Schwachstellen des Betroffenen (zB gezielte Ansprache von finanziell schutzbedürftigen Personen)
- **daher iaR "*nur*" transparente Einwilligung und Information durch werbenden Verantwortlichen erforderlich**

Zusammenfassung Abgrenzung

Prozess:	(bloße) Kategorisierung	Verknüpfung und Interpretation von Daten	Treffen von Entscheidungen
	Art 4 Z 2 DSGVO	Art 4 Z 4 DSGVO	Art 22 DSGVO
Ergebnis:	Überblick über Käufergruppen	Persönlichkeitsprofile inklusive Wahrscheinlichkeitswerte zB für personalisierte Werbung	zu Konditionen, Preisen, Vertragsschluss und -beendiung, etc

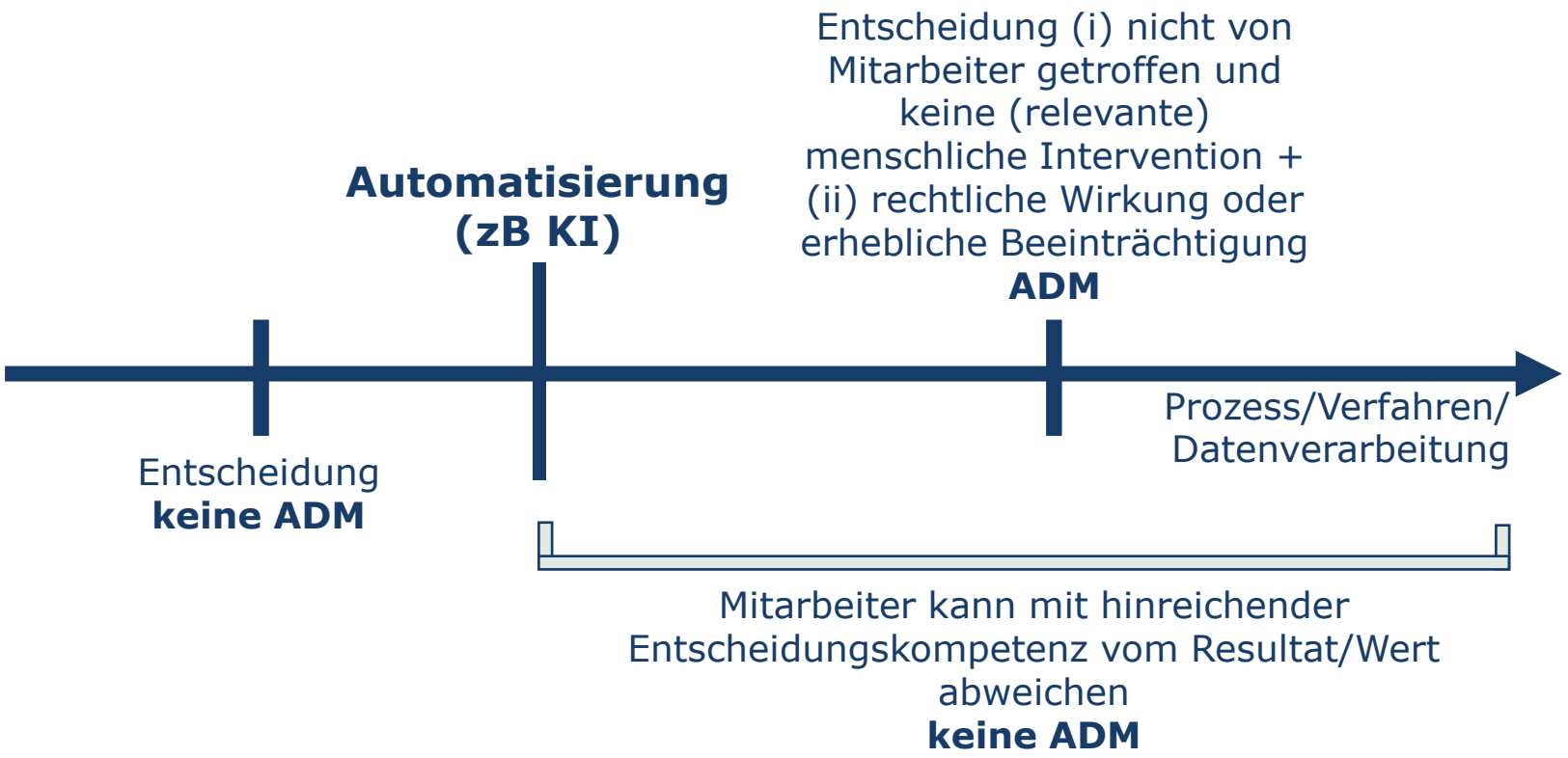
Ausblick Use Cases:

- Aufzeichnung des Wasserverbrauchs durch **analoge Wasserzähler** und **Unterbrechung der Wasserversorgung durch (menschlichen) Mitarbeiter** (BVwG 3.2.2022, W214 2224204-1)

- Berechnung und Zuordnung von **Geomilieu-Wahrscheinlichkeiten** zu für Marketing- und Werbezwecke
- **Arbeitnehmer Leistungsüberwachung** (GPS Monitoring)
- **Jö Bonus Club** (CRM)

- **AMS Algorithmus**
- **Interne/externe Kreditwürdigkeits-prüfung** (Scoring, Schufa)

Relevanz von Zeitpunkt und Auswirkung



Exkurs: Kreditwürdigkeits-/Bonitätsprüfung (Scoring)

- **Internes Scoring** = automatisierte **interne Ermittlung** eines Wahrscheinlichkeitswerts bzgl der Fähigkeit des Betroffenen, den Kaufpreis zu zahlen/einen Kredit in der Zukunft zu bedienen (**keine Außenwirkung**)
  - **BVwG:** bloßes internes Scoring **per se keine ADM**
  - Score-Werte **können ADM iSv Art 22 DSGVO aber vorausgehen**
  - dh: wird auf Grundlage des so ermittelten Score-Werts einschlägige Entscheidung (zB über Vertragsschluss oder Preis) ausschließlich automatisiert getroffen, ist Art 22 DSGVO anwendbar

Exkurs: Kreditwürdigkeits-/Bonitätsprüfung (Scoring)

- Score-Wert stammt von Dritten
  - insb Kreditauskunftei (zB KSV, Schufa)
  - Verantwortlicher trifft auf dieser Grundlage einschlägige Entscheidung

- **Findet Art 22 DSGVO auch auf Kreditauskunftei Anwendung?**
  - Score-Wert hat **nur indirekte Außenwirkung**
  - Lit: **divergierende Meinungen**
  - **BVwG (2018):** Erstellung und Bereitstellung eines Score-Wertes erfolgt im Auftrag eines Kunden, die endgültige Entscheidung wird erst durch den Kunden (und nicht durch die Auskunftei) getroffen
  - jedoch **zwei anhängige Vorabentscheidungsverfahren**: DE C-634/21, AT 6 Ob 48/21h

Automatisiertes Kreditwürdigkeitsprofil (C-634/21 – Schufa)

- SCHUFA erstellt automatisiert einen Score-Wert, der in Form eines **Wahrscheinlichkeitswerts** über Kreditwürdigkeit Auskunft gibt

- wird Banken und anderen Finanzdienstleistern als **Entscheidungsinstrument bei der Kreditvergabe** zur Verfügung gestellt

- Betroffener, dessen Kreditanfrage abgelehnt wurde, verlangte von SCHUFA **Informationen über genaue Zusammensetzung und Berechnung** des Score-Werts

- Hintergrund zur dt Rechtslage:
  - laut stRsp des BGH ist **Berechnungsmethode ein Geschäftsgeheimnis**
  - § 31 BDSG sieht **ausdrückliche Erlaubnis für Scoring** vor

Automatisiertes Kreditwürdigkeitsprofil (C-634/21 – Schufa)

Fragen an den EuGH:

1. Ist bereits die automatisierte Erstellung zur Kreditrückzahlungsfähigkeit eines Score-Wahrscheinlichkeitswerts eine ADM iSv Art 22 Abs 1 DSGVO, wenn dieser einem Dritten übermittelt wird und dieser Dritte auf dieser Grundlage über die Begründung/Durchführung/Beendigung eines Vertragsverhältnisses entscheidet?
2. Können nationale Normen (wie etwa § 31 BDSG) eine Ausnahme von den strengen Vorgaben für ADM vorsehen?

Schlussanträge GA (C-634/21 – Schufa)

- bereits das **Erstellen von Wahrscheinlichkeitswerten kann eine ADM iSd Art 22 Abs 1 DSGVO** sein, auch wenn "*erhebliche Beeinträchtigung*" erst durch die Verwendung durch Dritten
  - entscheidend, ob Verfahren der Entscheidungsfindung so ausgestaltet ist, dass **Scoring der Auskunftei Entscheidung des Kreditinstituts vorbestimmt**, dh ohne menschliches Dazwischentreten (Rz 42)
  - Auskunftei muss de facto endgültige Entscheidung für Finanzinstitut treffen → abhängig von internen Regeln und Praktiken des Finanzinstituts (Rz 44)
  - Beeinträchtigung finde schon auf Ebene der Kreditauskunftei statt
  - ob Score-Wert intern oder extern ermittelt, sei nicht relevant
- Betroffener hat **volles Auskunfts-, Berichtigungs- und Löschungsrecht** gegen Scoring-Anbieter
- Ausnahmen sind möglich, **aber § 31 BDSG wohl unionsrechtswidrig** und lediglich auf "*Verwendung*", nicht auf "*Erstellung*" eines Score-Werts bezogen
- Entscheidung des EuGH noch abzuwarten

To Dos bei Vorliegen einer ADM

- **Ausnahme vom Verbot**:
  - ausdrückliche Einwilligung
  - für Abschluss/Erfüllung eines Vertrags erforderlich
  - aufgrund von EU-/nationalem Recht zulässig (zB § 49a VStG Anonymverfügung)
  - sensible Daten: ausdrückliche Einwilligung oder erhebliches öffentliches Interesse + rechtliche Grundlage
- **Rechtsgrundlage für Verarbeitung** erforderlich, vgl ErwGr 72 – keine Regelung der Datenverarbeitung, sondern der Art der Entscheidungsfindung
- **Informationspflichten** zur Entscheidungslogik, den Kriterien, der Tragweite und den angestrebten Auswirkungen der ADM, Rechte des Betroffenen (vgl unten), ex post auch zur konkreten Entscheidung
- **geeignete Maßnahmen**, um zumindest folgende Rechte der Betroffenen zu gewährleisten:
  - Recht auf **Intervention durch einen Menschen**
  - Recht, seinen **Standpunkt zu äußern**
  - Recht auf **Anfechtung der Entscheidung**

DANKE FÜR IHRE AUFMERKSAMKEIT

DORDA

Mag Nino Tlapak, LLM

T: +43 1 533 47 95 – 23

nino.tlapak@dorda.at

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


DORDA
We deliver clarity.