

Arbeitsakte

Testakte: DSGVO-Massenscanning Mietinteressenten — VermieterCheck Solutions GmbH (Essen)

dsgvo-massenscanning-mietinteressenten-vermietercheck-app-essen

Diese Datei bündelt alle Aktenstücke in einem Dokument. Die Einzeldateien liegen im Aktenordner ebenfalls vor.

Inhaltsverzeichnis

Teil	Inhalt
Teil 1	Aktenstücke (Markdown) (22)
Teil 2	E-Mails (4)
Teil 3	Excel-Tabellen (2)
Teil 4	Word-Dokumente (3)
Teil 5	Bildanlagen und Screenshots (3)
Teil 6	PDF-Anhänge (Originaldokumente) (2)

Aktenstücke (Markdown)

Datei: 01_mandatsuebernahme-vollmacht.md

01 — Mandatsuebernahme und Vollmacht

Aktenzeichen: DSB-NW-44/26 / 18 Mass 4/26 / 4 O 244/26 / 12 Js 11.422/26

Mandantin: VermieterCheck Solutions GmbH, Ruhrallee 188, 45136 Essen

Kanzlei: Specht, Beckenbauer & Drosselberg Rechtsanwaltsgesellschaft mbH, Koenigsallee 92c, 40212 Duesseldorf

Federfuehrender Anwalt: RA Dr. Cornelius Specht (Fachanwalt Datenschutzrecht)

Datum: 14. Januar 2026

1. Mandatsbeschreibung

Die Kanzlei Specht, Beckenbauer & Drosselberg (nachfolgend „SBD“) uebernimmt die umfassende rechtliche Vertretung der VermieterCheck Solutions GmbH (nachfolgend „Mandantin“) in saemtlichen datenschutzrechtlichen, ordnungswidrigkeitsrechtlichen und strafrechtlichen Verfahren, die aus dem Betrieb der SaaS-Plattform und des KI-Profilng-Moduls „ProspectScore Pro“ erwachsen.

1.1 Mandatsumfang

Das Mandat erstreckt sich auf folgende Verfahrens- und Beratungskomplexe:

Lfd. Nr.	Komplex	Status
M-1	Aufsichtsverfahren LDI NRW (Art. 58 DSGVO), AZ DSB-NW-44/26	Laufend
M-2	Massenverfahren VDuG, LG Essen 18 Mass 4/26 (8.200 Betroffene)	Laufend
M-3	Einzelklage Dr. Tannenbruck, LG Essen 4 O 244/26	Laufend
M-4	Strafverfahren § 42 BDSG, StA Essen 12 Js 11.422/26	Laufend
M-5	Drittlandsuebermittlung Sundara Tech (Art. 44 ff. DSGVO)	Beratend
M-6	DSFA-Nachholung (Art. 35 DSGVO)	Beratend
M-7	Datenpanne CVE-2026-0188 / Art. 33 DSGVO Meldung	Beratend
M-8	Auskunftersuchen Drostermann, Kaltenbach (Art. 15 DSGVO)	Beratend

1.2 Interessenkollisionspruefung

Gemaess § 43a Abs. 4 BRAO sowie § 3 BORA wurde eine Konfliktkontrolle durchgefuehrt. Keine Interessenkollision festgestellt. Die Kanzlei SBD vertritt keine Parteien, die im vorliegenden Verfahrenskomplex als Anspruchsgegner oder Anzeigeerstatte aufreten.

2. Vollmacht

2.1 Prozessvollmacht (§ 80 ZPO)

Die Mandantin, vertreten durch Geschaefsfuehrer Karl-Heinz Schimmelpfennig-Drosthager, erteilt hiermit der Kanzlei Specht, Beckenbauer & Drosselberg Rechtsanwalts-gesellschaft mbH — sowie saemtlichen dort taetigen Rechtsanwaelten und Rechtsanwaeltinnen — unwiderrufliche Prozessvollmacht mit dem Recht zur Unterbevollmaechtigung gemaess § 80 ZPO fuer alle anhangigen und kuenftig entstehenden Verfahren im Zusammenhang mit dem vorliegenden Mandat.

Die Vollmacht umfasst insbesondere:

- Entgegennahme und Abgabe saemtlicher Erklaerungen gegenueber Behoerden, Gerichten und Dritten
- Abschluss von Vergleichen und Abgabe von Verzichtserklaerungen
- Einlegung und Ruecknahme von Rechtsmitteln
- Erhebung von Klagen, Einreichung von Schriftsaetzen
- Beantragung einstweiliger Rechtsschutzanordnungen
- Entgegennahme von Zustellungen (§ 172 ZPO)

2.2 Verwaltungsrechtliche Vollmacht

Fuer das Aufsichtsverfahren vor der LDI NRW (AZ DSB-NW-44/26) wird gesondert Vollmacht gemaess § 14 VwVfG NRW erteilt. Die Vollmacht berechtigt zur Akteneinsicht nach § 29 VwVfG NRW, zur Abgabe von Stellungnahmen gemaess Art. 58 Abs. 1 DSGVO sowie zur Erhebung von Rechtsmitteln gegen behordliche Anordnungen.

2.3 Strafprozessuale Vollmacht

Im Strafverfahren StA Essen 12 Js 11.422/26 wird Wahlverteidigervollmacht gemaess § 137 StPO erteilt. RA Dr. Cornelius Specht ist als Pflichtverteidiger bevollmaechtigt, saemtliche Verfahrenshandlungen im Namen des Beschuldigten Karl-Heinz Schimmelpfennig-Drosthager vorzunehmen.

3. Retainer und Honorarvereinbarung

Die Parteien haben folgende Honorarvereinbarung getroffen:

- **Beratungsmandat (M-5 bis M-8):** Stundenhonorar RA Dr. Specht 380 EUR/h netto; Paralegal 120 EUR/h netto
- **Prozessmandate (M-1 bis M-4):** Pauschalhonorar-Retainer zzgl. Erfolgsbeteiligung nach BORA-konformer Vereinbarung
- **Auslagen:** Reisekosten, Gerichtsgebuehren, Gutachterkosten nach Aufwand

Die Mandantin hat einen Kostenvorschuss von 85.000 EUR netto zzgl. USt. geleistet (Buchungsdatum 14.01.2026).

4. Erstinstruktionen

4.1 Sofortmassnahmen

RA Dr. Specht hat folgende Sofortmassnahmen angeordnet:

1. **Einfrieren der Datenverarbeitung** im ProspectScore-Pro-Modul bis zur Klaerung der Rechtsgrundlagen (Art. 6 Abs. 1 DSGVO-Konformitaetspruefung)
2. **Preservation Hold** saemtlicher Protokolldaten, Log-Files und Datenbankdumps (Sicherung fuer Beweiszwecke)
3. **Kommunikationsstop** — keine direkten Gespraechе der Mandantin mit LDI NRW ohne anwaltliche Begleitung
4. **Incident Response** — Beauftragung externer Forensik (SecureProof GmbH, Bochum) zur Analyse CVE-2026-0188
5. **HinSchG-Meldekanal** — Interne Meldestelle per sofort aktivieren und dokumentieren

4.2 Fristenkalender (initial)

Frist	Datum	Verfahren
Stellungnahme LDI NRW Art. 58	28.02.2026	DSB-NW-44/26
Klageerwiderung VDUG	15.03.2026	18 Mass 4/26
Auskunft Art. 15 Tannenbruck	10.02.2026	4 O 244/26
Einlassung StA Essen	05.03.2026	12 Js 11.422/26
DSFA-Entwurf intern	28.01.2026	intern M-6

5. Rechtliche Ersteinschaetzung

Die Gesamtlage der Mandantin ist als **kritisch** einzustufen. Folgende Risikopositionen bestehen kumulativ:

1. **Bussgeldrisiko LDI NRW** — Bei Feststellung eines schwerwiegenden Verstosses gegen Art. 6, Art. 22 und Art. 35 DSGVO droht ein Bussgeld bis 20.000.000 EUR oder 4% des weltweiten Jahresumsatzes (Art. 83 Abs. 5 DSGVO). Bei einem geschaetzten Jahresumsatz von ca. 4 Mio. EUR liegt die 4%-Grenze bei 160.000 EUR; massgeblich ist der hoehere Betrag, mithin 20 Mio. EUR.
2. **Haftungsrisiko Sammelklage** — 8.200 Betroffene x 1.500 EUR = 12.300.000 EUR (Gesamtforderung). Nach BGH VI ZR 10/24 kann auch bei fehlender konkreter Schadensbeschreibung immaterieller Schaden geltend gemacht werden, sofern ein kontrollierter Datenverlust nachgewiesen ist.
3. **Strafbarkeitsrisiko § 42 BDSG** — Freiheitsstrafe bis 3 Jahre oder Geldstrafe; Beschuldigter ist GF Schimmelpfennig-Drosthager persoendlich.

Die Kanzlei SBD empfiehlt eine umfassende Compliance-Offensive (DSFA-Nachholung, AVV-Sanierung, Meldung der Datenpanne) zur Strafmilderung im Bussgeldbescheid-Verfahren (Art. 83 Abs. 2 lit. f DSGVO: Kooperationsbereitschaft als Milderungsgrund).

Quellen

- DSGVO Art. 6, 22, 33, 35, 44, 58, 83 — dejure.org/gesetze/DSGVO
- BDSG § 42 — dejure.org/gesetze/BDSG

- BRAO § 43a Abs. 4 — dejure.org/gesetze/BRAO
- ZPO § 80, § 172 — dejure.org/gesetze/ZPO
- BGH, Urt. v. 18.11.2024 — VI ZR 10/24 — [bundesgerichtshof.de](https://www.bundesgerichtshof.de)

Datei: 02_sachverhaltserfassung-erstberatung.md

02 — Sachverhaltserfassung und Erstberatung

Aktenzeichen: DSB-NW-44/26

Datum: 14.–15. Januar 2026

Bearbeiter: RA Dr. Cornelius Specht, RAin Miriam Beckenbauer

1. Hintergrund der Mandantin

1.1 Unternehmensdarstellung

Die VermieterCheck Solutions GmbH (nachfolgend „VCS“) wurde 2019 in Essen gegründet und betreibt eine B2B-SaaS-Plattform, ueber die Privatvermieter Bonitaetsauskuenfte ueber Mietinteressenten einholen koennen. Zum Stichdatum 14.01.2026 sind 12.400 Privatvermieter angeschlossen. Die Daten der Mietinteressenten werden durch das proprietäre KI-Profilng-Modul „ProspectScore Pro“ verarbeitet.

Verarbeitete Datenkategorien (lt. Erstauskunft GF):

- Bonitaetsauskunft (Schufa-Score, Negativmerkmale)
- Voreigentum / fruehere Mietverhaeltnisse
- Beruf und Einkommenssituation
- Familienstatus und Haushaltsgroesse
- Automatisch ermittelter Risiko-Score (0–100) durch ProspectScore Pro

1.2 Technische Systemarchitektur

Das Modul ProspectScore Pro ist als Microservice in einer AWS-Infrastruktur (Frankfurt, eu-central-1) betrieben. Die Entwicklung und der Second-Level-Support erfolgen durch den indischen Dienstleister Sundara Tech Pvt. Ltd. (Bengaluru, Karnataka). Nach Aussage des DevOps-Leiters (Herr Tarkan Bilgic) besteht seit Oktober 2022 ein Datenaustausch mit Sundara Tech ohne abgeschlossene Standarddatenschutzklauseln (SCC) gemaess Art. 46 Abs. 2 lit. c DSGVO.

1.3 Betriebsdauer und Verarbeitungsumfang

ProspectScore Pro wurde laut Mandantin im Maerz 2023 in den Produktivbetrieb uebernommen. Bis Januar 2026 wurden die personenbezogenen Daten von ca. 142.300 Mietinteressenten verarbeitet. Davon haben schriftlich Einwilligung erteilt: nach Angaben der Mandantin ca. 88.000 Personen; bei den verbleibenden ca. 54.300 Personen fehlen nachweisbare Einwilligungserklaerungen.

2. Chronologie der Ereignisse

Datum	Ereignis
Mrz 2023	Produktivbetrieb ProspectScore Pro startet
Okt 2022	Beginn Datentransfer an Sundara Tech Pvt. Ltd. ohne SCC
08. Nov 2025	Anonyme HinSchG-Meldung bei interner Meldestelle (unbearbeitet)
17. Nov 2025	Penetrationstest-Bericht SecureProof GmbH: SQL-Injection CVE-2026-0188 identifiziert
22. Nov 2025	Erstbestaetigter Datenleak: 142.300 Datensatze exfiltriert
29. Nov 2025	72h-Frist gemass Art. 33 DSGVO laeuft ab — keine Meldung bei LDI NRW
03. Dez 2025	LDI NRW erhaelt anonymen Hinweis; leitet Vorpruefung ein
12. Dez 2025	LDI NRW eroeffnet formales Aufsichtsverfahren, AZ DSB-NW-44/26
15. Dez 2025	Sammelklage VDuG eingereicht: LG Essen 18 Mass 4/26
22. Dez 2025	Einzelklage Tannenbruck: LG Essen 4 O 244/26
07. Jan 2026	StA Essen eroeffnet Ermittlungen § 42 BDSG: 12 Js 11.422/26
14. Jan 2026	Mandatsuebernahme durch SBD

3. Erstberatungsgespraech (Protokoll)

3.1 Gespraech mit GF Schimmelpfennig-Drosthager (14.01.2026, 14:00–17:30 Uhr)

Themen:

1. Aufklaerung ueber Zeugnisverweigerungsrecht § 52 StPO im Strafverfahren
2. Belehrung ueber Schweigerecht § 136 StPO als Beschuldigter
3. Erlaeuterung der zivilrechtlichen Haftungsrisiken Art. 82 DSGVO
4. Besprechung des Sachverhalts zur privaten Nutzung der Plattform (Wohnungen Essen-Bredeney)

Ergebnis: GF Schimmelpfennig-Drosthager bestreitet vorsaeztliches Handeln, raumt aber ein, die Plattform zur eigenen Mieterauswahl genutzt zu haben. Die strafrechtliche Beurteilung wird gesondert geprueft (s. Akte 15).

3.2 Gespraech mit Datenschutzbeauftragter Frau Hannelore Kessler-Brandt (15.01.2026, 09:00–11:00 Uhr)

Themen:

1. Stand der internen DSFA-Dokumentation (Art. 35 DSGVO) — Ergebnis: keine DSFA durchgefuehrt
2. Verarbeitungsverzeichnis (Art. 30 DSGVO) — Ergebnis: vorhanden, jedoch nicht aktuell
3. Einwilligungsmanagement — Ergebnis: keine dokumentierten Einwilligungserklaerungen fuer ca. 54.300 Betroffene
4. Meldepflicht Art. 33 DSGVO — Ergebnis: Versaeumnis bestaetigt, keine interne Eskalation erfolgt

3.3 Gespraech mit DevOps-Leiter Herr Tarkan Bilgic (15.01.2026, 11:30–13:00 Uhr)

Themen:

1. Architektur des Datentransfers zu Sundara Tech

2. API-Authentifizierungsverfahren

3. CVE-2026-0188 — SQL-Injection in der Suchanfrage-Schnittstelle des Scoring-Backends

Ergebnis: Seit Oktober 2022 werden Rohdaten der Mietinteressenten fuer Modelltraining und Support-Zwecke an Sundara Tech uebertragen. Ein AVV-Vertrag existiert seit Dezember 2023 (also nachtraeglich), SCC wurde jedoch nie unterzeichnet.

4. Einschaeztung des Gesamtrisikos

4.1 Risikomatrix (Ersteinschaeztung)

Risiko	Eintrittswahrscheinlichkeit	Finanzielles Exposure	Prioritaet
LDI-Bussgeld Art. 83	Hoch (75%)	bis 20.000.000 EUR	KRITISCH
VDuG-Sammelklage Art. 82	Mittel-Hoch (60%)	bis 12.300.000 EUR	KRITISCH
Strafverfahren § 42 BDSG	Mittel (45%)	Freiheitsstrafe GF	HOCH
Einzelklage Tannenbruck	Mittel (55%)	bis 1.500 EUR + Kosten	MITTEL
Drittlandhaftung Art. 44	Hoch (70%)	Bussgeld (kumulativ)	HOCH
Reputationsschaden NDR	Sehr hoch (90%)	Umsatzrueckgang	HOCH

4.2 Strategische Empfehlung

Die Kanzlei SBD empfiehlt eine Dreisaeulenstrategie:

Saeule 1 — Compliance-Offensive: Sofortige Nachholung der DSFA, Sanierung des AVV mit Sundara Tech, Nachmeldung der Datenpanne an LDI NRW mit Schadensbegrenzungs-Narrative.

Saeule 2 — Verfahrensverteidigung: Aktive Vertretung in allen Verfahren mit dem Ziel der Strafminderung (Art. 83 Abs. 2 DSGVO-Milderungsgruende) und Abweisung der Sammelklage mangels individueller Kausalitaet.

Saeule 3 — Kommunikationsmanagement: Koordination mit PR-Beratung zur Steuerung der Berichterstattung NDR Panorama; kein oeffentliches Eingestaendnis ohne anwaltliche Freigabe.

5. Naechste Schritte

1. DSFA-Kickoff-Workshop mit Datenschutzbeauftragter Kessler-Brandt: 20.01.2026
2. Beauftragung eines unabhaengigen Datenschutz-Gutachters fuer Art. 22 DSGVO: bis 22.01.2026
3. Anwaltsschreiben an LDI NRW zur Fristverlaengerung: 17.01.2026
4. Koordination mit Strafverteidiger Dr. Robert Ankermann (StA-Verfahren): 16.01.2026
5. Pruefung Insolvenzrisiko bei Maximalhaftung: Gespräch Steuerberater Muenster & Partner

Quellen

- DSGVO Art. 6, 22, 30, 33, 35, 44, 46, 82, 83 —
dejure.org/gesetze/DSGVO
- BDSG § 42 — dejure.org/gesetze/BDSG
- HinSchG — dejure.org/gesetze/HinSchG
- StPO §§ 52, 136 — dejure.org/gesetze/StPO
- BGH VI ZR 10/24 (DSGVO-Schadensersatz) —
[bundesgerichtshof.de](https://www.bundesgerichtshof.de)

Datei: 03_dsgvo-pruefschema-art6-verarbeitungsgrundlagen.md

03 — DSGVO-Pruefschema: Verarbeitungsgrundlagen Art. 6 DSGVO

Aktenzeichen: DSB-NW-44/26

Bearbeiter: RA Dr. Cornelius Specht

Datum: 16. Januar 2026

Betreff: Rechtmässigkeitprüfung der Datenverarbeitung durch ProspectScore Pro

1. Prüfungsgegenstand

Die LDI NRW prüft im Rahmen des Aufsichtsverfahrens DSB-NW-44/26, ob VermieterCheck Solutions GmbH (VCS) die personenbezogenen Daten von Mietinteressenten auf einer rechtmässigen Grundlage nach Art. 6 Abs. 1 DSGVO verarbeitet hat. Das vorliegende Memorandum analysiert sämtliche in Betracht kommenden Erlaubnistatbestände und kommt zu einer Bewertung der Verteidigungsposition.

2. Verarbeitungsvorgänge im Ueberblick

ProspectScore Pro verarbeitet folgende Datenkategorien:

Datenkategorie	Herkunft	Sensitivität
Schufa-Score und Negativmerkmale	Schufa Holding AG (B2B-API)	Hoch
Voreigentum / Miethistorie	Mandantin eigene Abfragen	Mittel
Beruf und Einkommenssituation	Mietinteressent (Selbstauskunft)	Mittel
Familienstatus und Haushaltsgrossesse	Mietinteressent (Selbstauskunft)	Mittel
Automatisierter Risiko-Score (0–100)	ProspectScore Pro (KI-Ausgabe)	Sehr hoch

Die Verarbeitung dient der automatisierten Entscheidungsunterstützung für Privatvermieter bei der Mietinteressenten-Auswahl.

3. Pruefschema Art. 6 Abs. 1 DSGVO — Erlaubnistatbestaende

3.1 Art. 6 Abs. 1 lit. a DSGVO — Einwilligung

Tatbestand: Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten fuer einen oder mehrere bestimmte Zwecke gegeben.

Pruefungsschritte:

Schritt 1 — Freiwilligkeit (Art. 7, ErwGr. 42, 43 DSGVO): Mietinteressenten befinden sich in einer typischen Machtasymmetrie: Sie koennen die Plattform nicht umgehen, wenn Vermieter ausschliesslich ueber VCS Auskuenfte einholen. Nach EDSA-Leitlinien 05/2020 (Consent) ist Freiwilligkeit ausgeschlossen, wenn die Verweigerung der Einwilligung zu einem erheblichen Nachteil fuehrt. Ergebnis: Freiwilligkeit zweifelhaft.

Schritt 2 — Informiertheit (Art. 13, 14 DSGVO): Die VCS-Datenschutzerklaerung (Version 2.1 vom 01.03.2023) erwaehnt den Betrieb von ProspectScore Pro nicht explizit; das Profiling wird als „Bonitaetsabfrage“ bezeichnet, ohne die KI-basierte Scoring-Komponente offenzulegen. Ergebnis: Informiertheit nicht gegeben.

Schritt 3 — Eindeutigkeit (Art. 7 Abs. 2, ErwGr. 32 DSGVO): Die Einwilligung wird ueber ein Koppelungs-Checkbox-Modell eingeholt (Einwilligung an AGB-Akzeptanz geknuepft). Nach Art. 7 Abs. 4 DSGVO ist eine solche Koppelung unzuulaessig. Ergebnis: Eindeutigkeit nicht gegeben.

Schritt 4 — Widerruflichkeit (Art. 7 Abs. 3 DSGVO): Ein Widerrufsmechanismus ist technisch nicht implementiert. Ergebnis: Widerrufsmechanismus fehlt.

Gesamtergebnis Art. 6 Abs. 1 lit. a DSGVO: Einwilligung rechtmassig nicht erteilt. Die vorhandenen Einwilligungserklaerungen sind nicht DSGVO-konform und daher unwirksam. **Ergebnis: Keine wirksame Einwilligung.**

3.2 Art. 6 Abs. 1 lit. b DSGVO — Vertragserfuellung

Tatbestand: Die Verarbeitung ist fuer die Erfuellung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchfuehrung vorvertraglicher Massnahmen, die auf Anfrage der betroffenen Person erfolgen, erforderlich.

Pruefung: Zwischen VCS und den Mietinteressenten besteht kein Vertrag. VCS unterhalt Vertraege mit den Privatvermietern (B2B-SaaS-Abonnement). Die Mietinteressenten sind keine Vertragsparteien. Das EDSA-Leitlinien 02/2019 (Art. 6 Abs. 1 lit. b) stellt klar, dass der Betroffene selbst Vertragspartei sein muss.

Gesamtergebnis Art. 6 Abs. 1 lit. b DSGVO: Tatbestand nicht erfuellt. **Ergebnis: Nicht anwendbar.**

3.3 Art. 6 Abs. 1 lit. c DSGVO — Rechtliche Verpflichtung

Tatbestand: Die Verarbeitung ist zur Erfuellung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt.

Pruefung: Keine rechtliche Verpflichtung zur Erstellung von Bonitaets-Profilen fuer Dritte erkennbar. § 505a BGB (Kreditwuerdigkeitspruefung) gilt nur fuer Kreditinstitute, nicht fuer Vermietungsplattformen.

Gesamtergebnis Art. 6 Abs. 1 lit. c DSGVO: Tatbestand nicht erfuellt. **Ergebnis: Nicht anwendbar.**

3.4 Art. 6 Abs. 1 lit. f DSGVO — Berechtigtes Interesse

Tatbestand: Die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.

Dreistufiger Prüfungstest (LIA — Legitimate Interest Assessment):

Stufe 1 — Legitimes Interesse: VCS und angeschlossene Vermieter haben ein wirtschaftliches Interesse an Mietausfallprävention. Das Bundesverwaltungsgericht (BVerwG 6 C 12.18) erkennt Bonitätsprüfungen im Mietrecht als grundsätzlich legitim an. Ergebnis: Legitimes Interesse besteht.

Stufe 2 — Erforderlichkeit: Die Erhebung von Familienstatus und Haushaltsinformationen für ein Risiko-Scoring überschreitet den Umfang einer klassischen Bonitätsprüfung. Weniger einschneidende Mittel (z.B. einfache Schufa-Anfrage ohne KI-Profiling) stehen zur Verfügung. Ergebnis: Erforderlichkeit teilweise verneint.

Stufe 3 — Interessenabwägung: Die automatisierte Profilerstellung (Risiko-Score 0–100) greift erheblich in die Grundrechte der Mietinteressenten ein (Art. 8 GRCh, Recht auf informationelle Selbstbestimmung). Die Betroffenen haben keine Möglichkeit der Kenntnisnahme oder des Widerspruchs. Ergebnis: Interessen der Betroffenen überwiegen.

Besonderheit Art. 22 DSGVO: Bei automatisierten Einzelentscheidungen (Scoring als alleinige Grundlage für Vermieter-Entscheidung) ist Art. 6 Abs. 1 lit. f DSGVO als alleinige Grundlage in der Regel nicht ausreichend (s. Akte 04).

Gesamtergebnis Art. 6 Abs. 1 lit. f DSGVO: Interessenabwägung fällt zugunsten der Betroffenen aus. **Ergebnis: Nicht ausreichend.**

4. Gesamtbewertung

Erlaubnistatbestand	Ergebnis
Art. 6 Abs. 1 lit. a (Einwilligung)	Unwirksam — Koppelung, fehlende Informiertheit
Art. 6 Abs. 1 lit. b (Vertrag)	Nicht anwendbar — kein Vertrag mit Betroffenen
Art. 6 Abs. 1 lit. c (Rechtspflicht)	Nicht anwendbar — keine Rechtspflicht
Art. 6 Abs. 1 lit. f (Berechtigtes Interesse)	Nicht ausreichend — LIA negativ

Gesamtergebnis: Die Verarbeitung durch ProspectScore Pro entbehrt einer wirksamen Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO. Dies stellt einen schwerwiegenden Verstoß dar, der eine Ordnungswidrigkeit nach Art. 83 Abs. 5 lit. a DSGVO begründet.

5. Verteidigungsstrategie

Angesichts des klaren Befundes empfiehlt RA Dr. Specht folgenden Ansatz gegenüber der LDI NRW:

1. **Einräumen des Verstosses** gegenüber LDI NRW (Milderungsgrund Art. 83 Abs. 2 lit. f — Kooperationsbereitschaft)

2. **Nachtraegliche Sanierung:** Einwilligungsmanagement reformieren, Datenschutzerklärung aktualisieren, OptIn-Mechanismus implementieren
3. **Argumentation Art. 83 Abs. 2 lit. b:** Schaden fuer Betroffene gering (keine nachgewiesene missbilligende Nutzung des Scores durch Vermieter)
4. **Beantragung einer angemessenen Frist** zur Implementierung konformer Verarbeitungsgrundlagen vor Verhangung eines Bussgeldescheids

Quellen

- DSGVO Art. 6, 7, 13, 14, 22, 83 — dejure.org/gesetze/DSGVO
- EDSA-Leitlinien 05/2020 zur Einwilligung — [edpb.europa.eu](https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/guidelines-052020-consent-under-regulation_de)
- EDSA-Leitlinien 02/2019 zu Art. 6 Abs. 1 lit. b — [edpb.europa.eu](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-article-61b-gdpr_de)
- BVerwG, Urt. v. 27.09.2019 — 6 C 12.18 — openjur.de
- OLG Hamm, Urt. v. 15.08.2023 — 7 U 19/23 — openjur.de

Datei: 04_art22-automatisierte-einzelentscheidung-prospectscor.md

04 — Art. 22 DSGVO: Automatisierte Einzelentscheidung durch ProspectScore Pro

Aktenzeichen: DSB-NW-44/26

Bearbeiter: RA Dr. Cornelius Specht, RA Lars Drosselberg

Datum: 17. Januar 2026

Betreff: Rechtmassigkeit automatisierter Einzelentscheidungen und Profiling

1. Regelungsinhalt Art. 22 DSGVO

Art. 22 Abs. 1 DSGVO gewahrt betroffenen Personen das Recht, nicht einer ausschliesslich auf einer automatisierten Verarbeitung — einschliesslich Profiling — beruhenden Entscheidung unterworfen zu werden, die ihr gegenueber rechtliche Wirkung entfaltet oder sie in aehnlicher Weise erheblich beeintraehtigt.

Art. 22 Abs. 2 DSGVO regelt Ausnahmen: Die automatisierte Entscheidung ist zulaessig, wenn sie (a) fuer den Abschluss oder die Erfuellung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist, (b) aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten zulaessig ist oder (c) mit ausdruecklicher Einwilligung der betroffenen Person erfolgt.

Bei besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO) ist Art. 22 Abs. 4 DSGVO zu beachten.

2. Pruefung: Liegt eine automatisierte Einzelentscheidung vor?

2.1 Tatbestandsmerkmal „ausschliesslich automatisiert“

Der EDSA hat in seinen Leitlinien 01/2022 zu automatisierten Einzelentscheidungen (Art. 22 DSGVO) klargestellt, dass eine Entscheidung dann als „ausschliesslich automatisiert“ gilt, wenn kein menschlicher Eingriff mit substanziellem Einfluss auf das Ergebnis stattfindet. Ein bloss formales Review (Mensch bestaetigt maschinell vorgeschlagenes Ergebnis ohne eigene Pruefung) genuegt nicht.

Sachverhalt VCS:

- ProspectScore Pro generiert einen Risiko-Score (0–100)
- Privatvermieter erhalten den Score und eine abgeleitete Empfehlung (GRUEN / GELB / ROT)
- Laut Aussage von 127 Vermietern (Klaeger im VDuG-Verfahren) haben diese ausschliesslich auf Basis der Ampelfarbe entschieden
- Interne Nutzungsstatistiken belegen: 94% aller Mietabsagen korrelieren mit ROT-Einstufung
- Kein Prozess zur menschlichen Ueberpruefung des Scores implementiert

Ergebnis: Die Entscheidung ueber die Vermietung basiert faktisch ausschliesslich auf dem automatisierten Score. Das Tatbestandsmerkmal ist erfuellt.

2.2 Tatbestandsmerkmal „erhebliche Beeintraechtigung“

Die Verweigerung einer Wohnungsanmietung aufgrund des ROT-Scores stellt eine erhebliche Beeintraechtigung im Sinne des Art. 22 Abs. 1 DSGVO dar. Der Europaeische Datenschutzausschuss (EDSA, Leitlinien 01/2022, Rn. 15) nennt als Beispiel ausdruecklich den Ausschluss vom Zugang zu Wohnraum.

Ergebnis: Erhebliche Beeintraechtigung liegt vor.

2.3 Zwischenergebnis

Der Tatbestand des Art. 22 Abs. 1 DSGVO ist erfuellt. Die Verarbeitung ist grundsaeztlich verboten, soweit keine Ausnahme nach Art. 22 Abs. 2 DSGVO greift.

3. Pruefung der Ausnahmetatbestaende Art. 22 Abs. 2 DSGVO

3.1 Art. 22 Abs. 2 lit. a — Vertragserfuellung

Wie bereits in Akte 03 (Art. 6 lit. b) festgestellt: Zwischen VCS und den Mietinteressenten besteht kein Vertrag. **Ergebnis: Nicht einschlaegig.**

3.2 Art. 22 Abs. 2 lit. b — Gesetzliche Grundlage

Eine spezialgesetzliche Grundlage, die automatisiertes Profiling fuer Mietbonitaetszwecke erlaubt, existiert im deutschen Recht nicht. § 34 BDSG betrifft Auskunftspflichten, nicht Erlaubnisse fuer automatisiertes Scoring. **Ergebnis: Nicht einschlaegig.**

3.3 Art. 22 Abs. 2 lit. c — Einwilligung

Wie in Akte 03 (3.1) festgestellt: Die erteilten Einwilligungen sind wegen Koppelung und mangelnder Informiertheit unwirksam. Zudem war die ausdrueckliche Einwilligung in automatisierte Einzelentscheidungen (Art. 22 Abs. 2 lit. c DSGVO i.V.m. ErwGr. 71) gesondert erforderlich — dies erfolgte nicht. **Ergebnis: Nicht einschlaegig.**

4. Schutzpflichten bei zulaessiger automatisierter Entscheidung (Art. 22 Abs. 3 DSGVO)

Auch wenn — hypothetisch — eine Ausnahme greifen wuerde, haette VCS folgende Garantien gemaess Art. 22 Abs. 3 DSGVO implementieren muessen:

Garantie	Status bei VCS
Recht auf menschliche Ueberpruefung	Nicht implementiert
Recht auf Darlegung des eigenen Standpunkts	Kein Beschwerdemechanismus vorhanden
Recht auf Anfechtung der Entscheidung	Keine Einspruchsmoeglichkeit
Transparente Information (Art. 13 Abs. 2 lit. f DSGVO)	Profiling in Datenschutzerklaerung nicht explizit

5. Profiling und besondere Datenkategorien

5.1 Familienstatus als Diskriminierungsmerkmal

Der Familienstatus (mit/ohne Kinder) zaehlt nicht zu den besonderen Kategorien nach Art. 9 DSGVO. Jedoch kann das Profiling auf Basis des Familienstatus eine mittelbare Diskriminierung nach dem Allgemeinen Gleichbehandlungsgesetz (AGG) § 19 Abs. 1 Nr. 1 darstellen: Familien mit Kindern koennen systematisch schlechter bewertet werden.

5.2 Gesundheitliche Indikatoren im Score

Laut Penetrationstest-Bericht (s. Akte 07) verarbeitete ProspectScore Pro in einer frueheren Modellversion (v2.1 bis v2.4) Daten aus Krankenversicherungsstatusdaten, die im Rahmen der Schufa-Abfrage mitgeliefert wurden. Soweit Gesundheitsdaten (Art. 9 Abs. 1 DSGVO) in den Score eingeflossen sind, gilt Art. 22 Abs. 4 DSGVO: Die ausdrueckliche Einwilligung gemaess Art. 9 Abs. 2 lit. a DSGVO oder ein Rechtfertigungsgrund nach Art. 9 Abs. 2 DSGVO waere zusaetzlich erforderlich. Beides lag nicht vor.

6. Haftungsfolgen

6.1 Ordnungswidrigkeitenrecht

Ein Verstoss gegen Art. 22 DSGVO ist gemaess Art. 83 Abs. 4 DSGVO mit einem Bussgeld bis 10.000.000 EUR oder 2% des weltweiten Jahresumsatzes bedroht. In Kombination mit dem Verstoss gegen Art. 6 DSGVO (Art. 83 Abs. 5 lit. a, bis 20 Mio. EUR) koennen gemaess Art. 83 Abs. 3 DSGVO Geldbussen kumuliert werden, wobei der Hoechstbetrag nicht ueberschritten werden darf.

Anwendbarer Hoechstbetrag: 20.000.000 EUR (Art. 83 Abs. 5 DSGVO: hoehere Sanktion).

6.2 Zivilrechtliche Haftung

Betroffene, die nachweislich aufgrund eines fehlerhaften ROT-Scores eine Wohnung nicht erhalten haben, koennen gemaess Art. 82 DSGVO Schadensersatz verlangen. Der immaterielle Schaden liegt nach BGH VI ZR 10/24 bereits im Kontrollverlust ueber eigene Daten (s. Akte 11).

7. Handlungsempfehlungen

1. **Sofortige Abschaltung** des ProspectScore-Pro-Moduls bis zur Erlangung konformer Rechtsgrundlagen
2. **Implementierung Human-in-the-Loop (HITL)** — obligatorische menschliche Ueberpruefung vor jeder Entscheidungsweitergabe an Vermieter
3. **Aktualisierung der Datenschutzerklärung** mit expliziter Information ueber Profiling (Art. 13 Abs. 2 lit. f, Art. 14 Abs. 2 lit. g DSGVO)
4. **Einspruchsmechanismus** fuer betroffene Mietinteressenten (Art. 22 Abs. 3 DSGVO)
5. **DSFA** fuer das KI-Profiling-Modul (Art. 35 DSGVO, s. Akte 05)

Quellen

- DSGVO Art. 9, 13, 14, 22 — dejure.org/gesetze/DSGVO
- EDSA-Leitlinien 01/2022 zu automatisierten Einzelentscheidungen — [edpb.europa.eu](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012022-data-subject-rights-automated-decision_de)
- BDSG § 34 — dejure.org/gesetze/BDSG
- AGG § 19 — dejure.org/gesetze/AGG
- BGH VI ZR 10/24 — [bundesgerichtshof.de](https://www.bundesgerichtshof.de)
- OLG Koeln, Urt. v. 14.07.2022 — 20 U 168/21 — openjur.de

Datei: 05_dsfa-pruefung-art35-hochrisiko-ki.md

05 — Datenschutz-Folgenabschaetzung (DSFA) nach Art. 35 DSGVO

Aktenzeichen: DSB-NW-44/26

Bearbeiter: RAin Miriam Beckenbauer, RA Dr. Cornelius Specht

Datum: 20. Januar 2026

Betreff: DSFA-Versaumnis fuer ProspectScore Pro und Nachholungsplan

1. Rechtliche Grundlage und Pflicht zur DSFA

Art. 35 Abs. 1 DSGVO verpflichtet den Verantwortlichen, vor der Verarbeitung eine Abschaetzung der Folgen der vorgesehenen Verarbeitungsvorgaenge fuer den Schutz personenbezogener Daten durchzufuehren, wenn eine Verarbeitung voraussichtlich ein hohes Risiko fuer die Rechte und Freiheiten natuerlicher Personen zur Folge hat.

1.1 Regelbeispiele nach Art. 35 Abs. 3 DSGVO

Art. 35 Abs. 3 DSGVO nennt als typische Hochrisikoverarbeitungen:

- **lit. a:** Systematische und umfassende Bewertung persoenerlicher Aspekte natuerlicher Personen durch automatisierte Verarbeitung einschliesslich Profiling (explizit: Bonitaetsermittlung)
- **lit. c:** Systematische Ueberwachung oeffentlich zugaeenglicher Bereiche (hier nicht einschlaegig)

Ergebnis: ProspectScore Pro faellt unmittelbar unter Art. 35 Abs. 3 lit. a DSGVO. Die DSFA-Pflicht war von Beginn an gegeben.

1.2 Negativlisten und Positivlisten der LDI NRW

Gemaess Art. 35 Abs. 4 und Abs. 5 DSGVO haben Aufsichtsbehoerden Listen der Verarbeitungen zu erstellen, die einer DSFA beduerftig sind (Muss-Listen) bzw. nicht beduerftig sind (Ausnahmelisten). Die LDI NRW hat in ihrer aktuellen Muss-Liste (Stand Oktober 2025) ausdruecklich „KI-gestuetzte Scoring-Verfahren zur Mietinteressenten-Beurteilung“ aufgefuehrt.

2. DSFA-Checkliste: Ist eine DSFA erforderlich?

Kriterium (DSK-Standard 2017)	Befund bei VCS	Punkte
Bewertung oder Einstufung	Ja (Score 0–100, Ampel)	1
Automatisierte Entscheidung mit Rechtswirkung	Ja (Mietabsagen)	1
Systematische Ueberwachung	Mittel (kein Tracking, aber Massenverarbeitung)	0,5
Sensitive oder hochpersoenliche Daten	Ja (Schufa, Familienstatus)	1
Grosse Mengen / Betroffene	Ja (142.300 Datensaeetze)	1
Verknuepfung verschiedener Datensaeetze	Ja (Schufa + Selbstauskunft + Profiling)	1
Innovative Technologie	Ja (KI-Modell ohne DSFA-Vorlage)	1
Hinderung der Ausuebung von Rechten	Ja (Wohnungszugang)	1

Gesamtbewertung: 7,5 von 8 Punkten. Ab 2 Punkten ist eine DSFA erforderlich. **DSFA-Pflicht eindeutig bejaht.**

3. Dokumentiertes Versaeumnis

3.1 Zeitlinie

Datum	Ereignis
Jan 2023	Interne Entwicklung ProspectScore Pro (v1.0)
Mrz 2023	Go-Live Produktivbetrieb — keine DSFA durchgefuehrt
Jun 2023	Upgrade auf v2.0 (neues ML-Modell) — keine DSFA
Feb 2024	Upgrade auf v3.0 (erweiterte Datenkategorien) — keine DSFA

Datum	Ereignis
Nov 2025	Erste interne Kenntnis des DSFA-Versäumnisses (Whistleblower-Meldung)
Jan 2026	Mandatsübernahme SBD — DSFA noch immer ausstehend

3.2 Interne Warnsignale

- Datenschutzbeauftragte Frau Kessler-Brandt hat laut eigener Aussage zweimal (Mai 2023, Oktober 2024) intern auf die DSFA-Pflicht hingewiesen — ohne Ergebnis
- Diese internen Warnhinweise wurden nicht dokumentiert (fehlende Schriftform)
- Der Geschäftsführer wurde mündlich informiert und hat die DSFA als „nicht praxisrelevant“ abgetan

4. Inhalt einer nachzuholenden DSFA

Die DSFA muss gemäß Art. 35 Abs. 7 DSGVO mindestens enthalten:

4.1 Systematische Beschreibung der Verarbeitungsvorgänge (Art. 35 Abs. 7 lit. a)

`` Verarbeitungsvorgang: Automatisiertes Profiling von Mietinteressenten Zweck: Risikobeurteilung für angeschlossene Privatvermieter Datenkategorien: Schufa-Score, Negativmerkmale, Beruf, Einkommen, Familienstatus, Haushaltsgroesse Verarbeitung: ML-Modell ProspectScore Pro v3.0 (Random Forest + Neural Net) Empfänger: Privatvermieter (B2B-Kunden, 12.400+) Drittlandtransfer: Sundara Tech Pvt. Ltd. (Bengaluru) – Entwicklung/Support Speicherdauer: 24 Monate nach letzter Abfrage ``

4.2 Beurteilung der Notwendigkeit und Verhältnismässigkeit (Art. 35 Abs. 7 lit. b)

Die Erhebung des Familienstatus und der Haushaltsgroesse ist für den legitimen Zweck der Bonitätsprüfung nicht erforderlich (Verhältnismässigkeit verletzt). Ausreichend wäre: Schufa-Score + Einkommensnachweise. Alle weiteren Datenkategorien sind zu entfernen.

4.3 Risikobewertung (Art. 35 Abs. 7 lit. c)

Risiko	Eintrittswahrscheinlichkeit	Schwere	Gesamtrisiko
Fehlerhafte Bonitätsbewertung für Betroffene	Hoch	Hoch	KRITISCH
Diskriminierung aufgrund Familienstatus	Mittel	Hoch	HOCH
Datenleak sensibler Scoring-Daten	Realisiert (CVE-2026-0188)	Sehr hoch	KRITISCH
Drittlandtransfer ohne SCC	Hoch	Hoch	KRITISCH
Nichtbeachtung Widerruf / Löschung	Mittel	Mittel	MITTEL

4.4 Geplante Massnahmen zur Risikominimierung (Art. 35 Abs. 7 lit. d)

1. Human-in-the-Loop (HITL) Implementierung: Obligatorische menschliche Pruefung
2. Datenminimierung: Streichung Familienstatus und Haushaltsgroesse
3. Auftragsverarbeitungsvertrag (AVV) mit SCC fuer Sundara Tech
4. Technische Sicherheitsmassnahmen: Behebung CVE-2026-0188, End-to-End-Verschlüsselung
5. Betroffenenrechte: Implementierung Auskunfts-, Widerspruchs- und Loeschungsportal
6. Regelmäßige Pruefung des ML-Modells auf Diskriminierungseffekte (Bias-Audit)

5. Konsultationspflicht bei LDI NRW (Art. 36 DSGVO)

Gemaess Art. 36 Abs. 1 DSGVO ist der Verantwortliche verpflichtet, vor Beginn der Verarbeitung die Aufsichtsbehoerde zu konsultieren, wenn aus der DSFA ein hohes Risiko hervorgeht und der Verantwortliche keine geeigneten Massnahmen zur Eindaeimmung des Risikos trifft.

Da die DSFA nachtraeglich durchgefuehrt wird und das Risiko als KRITISCH eingestuft wurde, ist eine Vorabkonsultation (Art. 36 DSGVO) bei der LDI NRW obligatorisch. Dies wird gleichzeitig zur Entlastung im Aufsichtsverfahren DSB-NW-44/26 genutzt.

6. Zeitplan DSFA-Nachholung

Meilenstein	Verantwortlich	Frist
DSFA-Kickoff-Workshop	Dr. Specht + Kessler-Brandt	20.01.2026
Technische Beschreibung ProspectScore Pro	DevOps-Leiter Bilgic	27.01.2026
Risikobewertung (extern: SecureProof GmbH)	SecureProof GmbH	31.01.2026
Entwurf DSFA-Dokument	RAin Beckenbauer	07.02.2026
Freigabe durch DSB Kessler-Brandt	DSB Kessler-Brandt	10.02.2026
Einreichung bei LDI NRW (Art. 36 DSGVO)	RA Dr. Specht	14.02.2026

Quellen

- DSGVO Art. 35, 36 — dejure.org/gesetze/DSGVO
- DSK-Kurzpapier Nr. 5 (DSFA) — [datenschutzkonferenz-online.de](https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf)
- LDI NRW Muss-Liste gemass Art. 35 Abs. 4 DSGVO — [ldi.nrw.de](https://www.ldi.nrw.de)

- EDSA-Leitlinien 09/2022 (DSFA) — [edpb.europa.eu](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-092022-personal-data-breach-notification_de)
- BGH VI ZR 10/24 — [bundesgerichtshof.de](https://www.bundesgerichtshof.de)

Datei: 06_drittlandsuebermittlung-art44-sundara-tech.md

06 — Drittlandsuebermittlung Art. 44 ff. DSGVO: Sundara Tech Pvt. Ltd. (Bengaluru)

Aktenzeichen: DSB-NW-44/26

Bearbeiter: RA Lars Drosselberg, RA Dr. Cornelius Specht

Datum: 18. Januar 2026

Betreff: Rechtmässigkeit der Datenuebermittlung nach Indien ohne SCC

1. Sachverhaltsdarstellung

1.1 Dienstleister Sundara Tech Pvt. Ltd.

- **Firma:** Sundara Tech Pvt. Ltd.
- **Sitz:** No. 42, 4th Floor, Prestige Tech Park, Sarjapur Road, Bengaluru, Karnataka 560103, Indien
- **Tätigkeit:** Softwareentwicklung und Second-Level-Support fuer ProspectScore Pro
- **Vertragsbeziehung:** Entwicklungsvertrag seit Oktober 2022; Auftragsverarbeitungsvertrag (AVV) seit Dezember 2023 (nachträglich)
- **Datenzugang:** Zugriff auf Produktionsdaten fuer Debugging und Modelltraining (Rohdaten der Mietinteressenten)

1.2 Art der uebermittelten Daten

Datenkategorie	Uebermittlungsweg	Verschlüsselung
Mietinteressenten-Rohdaten (Scoring)	API-Call (REST)	TLS 1.2
ML-Trainings-Datensätze	S3-Bucket (shared)	Ja (S3-SSE)
Support-Log-Daten mit Personenbezug	VPN-Tunnel	Ja
Staging-Datenbankdump (anonymisiert?)	SFTP	Nein

Laut Penetrationstest-Bericht (s. Akte 07) enthielt der Staging-Datenbankdump nicht vollständig anonymisierte Datensätze — eine Re-Identifizierung war technisch möglich.

2. Rechtsrahmen Drittlanduebermittlung

2.1 Grundsatz Art. 44 DSGVO

Gemaess Art. 44 DSGVO darf eine Uebermittlung personenbezogener Daten, die gerade verarbeitet werden oder nach ihrer Uebermittlung in ein Drittland verarbeitet werden sollen, nur erfolgen, wenn der Verantwortliche und der Auftragsverarbeiter die in Kapitel V DSGVO niedergelegten Bedingungen einhalten.

2.2 Angemessenheitsbeschluss fuer Indien?

Stand Januar 2026: Fuer Indien existiert kein Angemessenheitsbeschluss der Europaeischen Kommission genaess Art. 45 DSGVO. Das Digital Personal Data Protection Act (DPDPA) Indiens (2023) wurde bislang nicht als gleichwertig mit der DSGVO eingestuft.

Folge: Jede Datenuebermittlung nach Indien bedarf geeigneter Garantien genaess Art. 46 DSGVO.

2.3 Geeignete Garantien Art. 46 DSGVO

Moegliche geeignete Garantien:

Garantie	Art. 46 Abs.	Status bei VCS
Standarddatenschutzkl auseln (SCC) — EU-Kommission 2021	Abs. 2 lit. c	**Nicht abgeschlossen**
Verbindliche interne Da tenschutzvorschriften (BCR)	Abs. 2 lit. b	Nicht anwendbar (kein Konzern)
Genehmigter Verhaltenskodex mit Zusatzmassnahmen	Abs. 2 lit. e	Nicht vorhanden
Zertifizierung mit verbindlichen Verpflichtungen	Abs. 2 lit. f	Nicht vorhanden
Ad-hoc-Vertragsklausel n (Genehmigung LDI)	Abs. 3	Nicht beantragt

Ergebnis: Keine der moeglichen Garantien wurde implementiert. Die Datenuebermittlung an Sundara Tech erfolgte seit Oktober 2022 ohne Rechtsgrundlage nach Kapitel V DSGVO.

3. Zusaetzliche Anforderungen an SCC (EDSA-Empfehlung 01/2020)

Selbst bei Abschluss von SCC waere nach der Schrems-II-Rechtsprechung (EuGH C-311/18 — Schrems II) eine Transferfolgenabschaetzung (Transfer Impact Assessment, TIA) erforderlich, da das Rechtssystem des Empfaengerlandes (Indien) auf seine Eignung bewertet werden muss.

3.1 Rechtslage Indien (TIA-Punkte)

Pruefkriterium	Bewertung
Geheimdienstzugriff auf Daten	Potenziell gegeben (Section 69 IT Act)
Rechtsstaatlichkeit bei Datenschutz	Teilweise (DPDPA 2023, noch nicht vollstaendig in Kraft)
Effektive Rechtsbehelfe	Eingeschraenkt (kein EuGH-Aequivalent)

Pruefkriterium	Bewertung
Unabhaengige Aufsicht	DPBI (Data Protection Board of India) — noch nicht voll operativ

Ergebnis TIA: Erhoehte Risiken; Zusatzmassnahmen erforderlich (End-to-End-Verschluesselung, Pseudonymisierung vor Transfer).

4. Bewertung des HinSchG-Hinweises

Die anonyme HinSchG-Meldung vom 08.11.2025 thematisiert explizit den fehlenden SCC-Abschluss. Der Hinweisgeber — vermutlich ein ehemaliger DevOps-Mitarbeiter — beschreibt den Sachverhalt detailliert und zutreffend.

Rechtliche Bewertung der VCS-Reaktion:

- Die Meldung wurde laut interner Dokumentation als „nicht pruefrelevant“ eingestuft und nicht weitergeleitet
- Versaeumnis der Bearbeitung einer HinSchG-Meldung stellt eine Pflichtverletzung nach § 14 HinSchG dar
- Kein Rueckmeldefristversaeumnis nach § 17 HinSchG: Keine Rueckmeldung an Hinweisgeber innerhalb von 3 Monaten

5. Ordnungswidrigkeitenrechtliche Bewertung

Der Verstoss gegen Art. 44 ff. DSGVO ist gemass Art. 83 Abs. 5 lit. c DSGVO eine schwerwiegende Ordnungswidrigkeit (Bussgeld bis 20.000.000 EUR oder 4% des weltweiten Jahresumsatzes).

Nach dem EuGH-Urteil C-311/18 (Schrems II, 16.07.2020) und dem darauf basierenden EuGH-Urteil C-645/19 (Facebook Ireland, 15.06.2021) ist die Aufsichtsbehoerde bei Kenntnis eines solchen Verstosses verpflichtet, die Uebermittlung zu untersagen und Sanktionen zu verhaengen.

6. Sanierungsplan Drittlandtransfer

Sofortmassnahmen (bis 31.01.2026)

1. **Datentransfer-Stop** — Keine weiteren Datenuebermittlungen an Sundara Tech bis zur SCC-Implementierung
2. **Loeschung Staging-Datenbankdumps** bei Sundara Tech — nachweislich dokumentiert
3. **Verschluesselung saemtlicher API-Calls** auf TLS 1.3 angehoben

Mittelfristige Massnahmen (bis 28.02.2026)

4. **SCC-Abschluss** gemass EU-Kommissionsbeschluss 2021/914 (Modul 2: Controller-to-Processor)
5. **Transfer Impact Assessment (TIA)** fuer Indien mit externer Expertise (RA Kanzlei Mehta & Associates, Mumbai)
6. **Pseudonymisierungsprotokoll** fuer ML-Trainingsdaten vor Weitergabe an Sundara Tech
7. **Update AVV** — Einbeziehung der SCC-Konformitaetsanforderungen

7. Stellungnahme gegenueber LDI NRW

Im Rahmen des Aufsichtsverfahrens DSB-NW-44/26 wird VCS folgende Position einnehmen:

- Einräumen des Verstosses mit Verweis auf Sanierungsplan
- Begrenzung des Bussgelds durch Hinweis auf:
 - Freiwillige Offenlegung (Art. 83 Abs. 2 lit. e DSGVO) - Kooperationsbereitschaft (Art. 83 Abs. 2 lit. f DSGVO) - Kein vorsätzliches Handeln (Art. 83 Abs. 2 lit. b DSGVO — blosses Unkenntnis der SCC-Pflicht) - Umsatz des KMU (Art. 83 Abs. 2 DSGVO — wirtschaftliche Lage)

Quellen

- DSGVO Art. 44, 45, 46, 83 — dejure.org/gesetze/DSGVO
- EuGH C-311/18 (Schrems II), Urt. v. 16.07.2020 — [eur-lex.europa.eu](https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62018CJ0311)
- EU-Kommissionsbeschluss 2021/914 (SCC) — [eur-lex.europa.eu](https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32021D0914)
- EDSA-Empfehlung 01/2020 (Zusatzmassnahmen) — [edpb.europa.eu](https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_de)
- HinSchG §§ 14, 17 — dejure.org/gesetze/HinSchG

Datei: 07_datenpanne-art33-sql-injection-cve-2026-0188.md

07 — Datenpanne Art. 33/34 DSGVO: SQL-Injection CVE-2026-0188

Aktenzeichen: DSB-NW-44/26

Bearbeiter: RA Dr. Cornelius Specht, Sachverständige SecureProof GmbH (Bochum)

Datum: 20. Januar 2026

Betreff: Analyse der Datenschutzverletzung, 72h-Meldepflichtverletzung, Schadensausmass

1. Technischer Sachverhalt

1.1 Schwachstelle CVE-2026-0188

Am 17. November 2025 identifizierte das externe Penetrationstestunternehmen SecureProof GmbH (Bochum) im Rahmen eines vereinbarten Black-Box-Tests eine kritische SQL-Injection-Schwachstelle (CVSS v3.1 Score: 9.8 — Kritisch) im Scoring-Backend von ProspectScore Pro.

Technische Details:

- **CVE-Nummer:** CVE-2026-0188
- **Komponente:** REST-API Endpoint `/api/v3/prospect/search` (ProspectScore Pro v3.0.4)
- **Typ:** Blind-Time-Based SQL Injection (PostgreSQL 14.2)
- **Ausnutzbarkeit:** Remote, keine Authentifizierung erforderlich
- **Angriffsvektor:** HTTP-Parameter `q` (Suchanfrage) ohne Eingabebereinigung

Angriffsmuster: `` GET /api/v3/prospect/search?q=1'%20OR%20'1'%3D'1 Host: api.vermietercheck.de (Beispiel-Payload fuer Demonstration) ``

1.2 Ausnutzung und Datenleak

Die Schwachstelle wurde laut Forensik-Bericht SecureProof (Bericht-Nr. SP-2025-4417) in der Zeit vom 22. November bis 24. November 2025 von einem externen Akteur ausgenutzt:

Datum	Ereignis
17.11.2025	SecureProof identifiziert CVE-2026-0188
18.11.2025	Interner Penetrationstest-Bericht an VCS-Leitung
22.11.2025	Erstes Anzeichen externer Ausnutzung in Server-Logs (retrospektiv festgestellt)
22.-24.11.2025	Exfiltration von 142.300 Datensatzen ueber Staging-API
24.11.2025	Anomalieerkennung schlaegt an (AWS GuardDuty)
24.11.2025	DevOps-Leiter informiert — Patch eingespielt (CVE-2026-0188-Fix)
25.11.2025	DevOps-Leiter informiert GF — keine Meldung an LDI NRW
29.11.2025	Ablauf der 72h-Meldefrist (Art. 33 Abs. 1 DSGVO) ohne Meldung
03.12.2025	LDI NRW erhaelt anonymen Hinweis

1.3 Betroffene Datensatze

Datenkategorie	Anzahl betroffene Datensatze	DSGVO-Sensitivitaet
Name + Adresse	142.300	Personenbezogen
Schufa-Score	98.400	Hoch
Negativmerkmale	41.200	Hoch
Berufsangabe	139.100	Mittel
Familienstatus	88.700	Mittel
ProspectScore (0–100)	142.300	Sehr hoch
E-Mail-Adresse	142.300	Mittel

2. Rechtliche Bewertung der Meldepflichtverletzung

2.1 Meldepflicht Art. 33 DSGVO

Art. 33 Abs. 1 DSGVO verpflichtet den Verantwortlichen, im Falle einer Verletzung des Schutzes personenbezogener Daten unverzueglich — und wenn moeglich binnen 72 Stunden — die zustaeendige Aufsichtsbehoerde zu benachrichtigen.

Fristberechnung:

- Zeitpunkt der Kenntniserlangung: 24.11.2025 (DevOps-Leiter informiert GF)
- 72h-Frist laeuft ab: 27.11.2025 um [Uhrzeit der Kenntniserlangung]
- Tatsaechliche Meldung: Bis heute (20.01.2026) nicht erfolgt

Ergebnis: Versaeumnis der 72h-Meldepflicht. Art. 83 Abs. 4 lit. a DSGVO: Bussgeld bis 10.000.000 EUR.

2.2 Benachrichtigungspflicht Betroffene Art. 34 DSGVO

Art. 34 Abs. 1 DSGVO verpflichtet zum Benachrichtigen betroffener Personen, wenn voraussichtlich ein hohes Risiko fuer deren Rechte und Freiheiten besteht. Die Exfiltration von Schufa-Scores und Bonitaetsdaten von 142.300 Personen begründet eindeutig ein solches Risiko.

Ergebnis: Auch die Benachrichtigung der Betroffenen gemaess Art. 34 DSGVO wurde versaeumt.

2.3 Kann die verspaetete Meldung noch nachgeholt werden?

Ja. Art. 33 Abs. 1 DSGVO sieht vor: Erfolgt die Benachrichtigung nicht innerhalb von 72 Stunden, so ist ihr eine Begründung fuer die Verspaetung beizufuegen. Die Kanzlei SBD empfiehlt die sofortige Nachholung der Meldung mit:

1. Vollstaendiger Schadensdarstellung nach Art. 33 Abs. 3 DSGVO (Kategorien, Anzahl, Massnahmen)
2. Erklaerung zur Verspaetung (interne Kommunikationsversagen)
3. Nachweis des Patches und der forensischen Analyse
4. Angebot direkter Kooperation mit LDI NRW

3. Inhalt der nachzuholenden Meldung (Art. 33 Abs. 3 DSGVO)

Pflichtinhalte gemaess Art. 33 Abs. 3 DSGVO:

Inhalt	Angabe
Art der Verletzung	SQL-Injection-basierte Exfiltration (CVE-2026-0188)
Kategorien betroffener Personen	Mietinteressenten
Anzahl betroffener Personen (ungefaehr)	142.300
Kategorien betroffener Datensaeetze	Bonitaetsdaten, Kontaktdaten, Scoring
Anzahl betroffener Datensaeetze (ungefaehr)	142.300
Name und Kontaktdaten DSB	Hannelore Kessler-Brandt, dsb@vermietercheck.de
Wahrscheinliche Folgen	Identitaetsdiebstahl, Kreditschaeden, Phishing-Risiko
Massnahmen zur Schadensbegrenzung	Patch eingespielt, API abgeschaltet, Forensik beauftragt

4. NIS2-Meldepflicht

Zusaetzlich zur DSGVO-Meldepflicht ist zu pruefen, ob VCS als Anbieter digitaler Dienste der NIS2-Richtlinie (EU 2022/2555) und dem nationalen Umsetzungsgesetz (BSIG-Novelle) unterliegt.

VCS betreibt eine B2B-SaaS-Plattform mit 12.400+ Nutzern. Soweit VCS als wesentlicher oder wichtiger Einrichtung im Sinne des Art. 3 NIS2 qualifiziert wird, besteht eine 24h-Fruehwarnpflicht gegenueber dem BSI (§ 30 BSIG n.F.) und eine 72h-Meldepflicht mit Angabe des Schweregrads.

5. ISO 27001 und Meldepflicht

VCS hat ISO 27001 beantragt (s. Akte 19). Gemaess ISO 27001:2022 Annex A 5.26 (Response to information security incidents) waren folgende Schritte nach Entdeckung des Vorfalls unmittelbar verpflichtend:

- Eskalation an Geschäftsleitung und CISO
- Dokumentation in einem Incident-Response-Log
- Benachrichtigung relevanter Behörden gemäss gesetzlicher Verpflichtung

Kein dieser Schritte wurde dokumentiert. Dies begründet eine Zertifizierungsrelevante Nicht-Konformität (Non-Conformity) und kann zur Suspendierung des ISO-27001-Zertifikats führen.

6. Handlungsempfehlungen

Sofort (bis 22.01.2026):

1. Nachholung der LDI NRW-Meldung Art. 33 DSGVO (koordiniert mit Kanzlei SBD)
2. Benachrichtigung der 142.300 betroffenen Mietinteressenten Art. 34 DSGVO (Brief + E-Mail)
3. Einrichtung einer Betroffenen-Hotline und Schadensersatz-Informationseite

Mittelfristig (bis 31.01.2026):

4. Beauftragung eines BSI-zertifizierten Forensik-Dienstleisters für vollständige Incident-Analyse
5. Umsetzung eines formalen Incident-Response-Prozesses nach ISO 27001:2022 Annex A 5.26
6. Prüfung BSI-Meldepflicht (NIS2) mit Rechtsberatung

Quellen

- DSGVO Art. 33, 34, 83 — dejure.org/gesetze/DSGVO
- NIS2-Richtlinie (EU) 2022/2555 — [eur-lex.europa.eu](https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32022L2555)
- BSIG (KRITIS-Dachgesetz-Novelle) — dejure.org/gesetze/BSIG
- EDSA-Leitlinien 01/2021 (Datenschutzverletzungen) — [edpb.europa.eu](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012021-examples-regarding-personal-data-breach_de)
- ISO/IEC 27001:2022, Annex A 5.26 — [iso.org](https://www.iso.org/standard/82875.html)

Datei: 08_ldi-nrw-aufsichtsverfahren-art58-strategie.md

08 — LDI NRW Aufsichtsverfahren Art. 58 DSGVO: Verfahrensstrategie

Aktenzeichen: DSB-NW-44/26

Bearbeiter: RA Dr. Cornelius Specht, RAin Miriam Beckenbauer

Datum: 21. Januar 2026

Betreff: Strategie fuer die Vertretung im Aufsichtsverfahren LDI NRW

1. Verfahrensgrundlagen

1.1 Rechtsstellung der LDI NRW

Die Landesbeauftragte fuer Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW) ist die gemaess Art. 55 DSGVO i.V.m. § 17 BDSG zustaeendige Aufsichtsbehoerde fuer VCS (Unternehmenssitz Essen). Sie ist nach Art. 57 Abs. 1 DSGVO verpflichtet, die Anwendung der DSGVO zu ueberwachen und durchzusetzen.

1.2 Befugnisse der LDI NRW (Art. 58 DSGVO)

Untersuchungsbefugnisse (Art. 58 Abs. 1):

- Anordnung der Auskunft (Abs. 1 lit. a)
- Zugang zu Raeumlichkeiten und Datensystemen (Abs. 1 lit. f)
- Einsicht in alle Daten (Abs. 1 lit. e)

Abhilfebefugnisse (Art. 58 Abs. 2):

- Verwarnung (lit. a)
- Verweis (lit. b)
- Anordnung konformer Verarbeitung (lit. c–g)
- Anordnung der Loeschung (lit. g)
- Vorlaeufige oder dauerhafte Beschraenkung oder Untersagung (lit. f)
- Verhangung eines Bussgeldescheids (lit. i)

Genehmigungsbefugnisse (Art. 58 Abs. 3):

- Stellungnahme zu Verarbeitungsvorgaengen (Art. 36 DSGVO)

2. Verfahrensstand

Datum	Massnahme LDI NRW
12.12.2025	Eroeffnung des Aufsichtsverfahrens, Mitteilung an VCS
15.12.2025	Anhoerungsschreiben Art. 58 Abs. 1 lit. a DSGVO (s. Akte pdfs/)
28.02.2026	Frist Stellungnahme VCS
Offen	LDI NRW-Entscheidung (Bussgeldbescheid / Verwarnung)

2.1 Anhoerungsschreiben LDI NRW

Das Anhoerungsschreiben vom 15.12.2025 (AZ DSB-NW-44/26-01) enthaelt folgende Vorwuerfe:

1. Verarbeitung ohne wirksame Rechtsgrundlage (Art. 6 DSGVO) durch ProspectScore Pro
2. Einsatz automatisierter Einzelentscheidungen ohne Erlaeubnisgrundlage (Art. 22 DSGVO)
3. Unterlassung der DSFA (Art. 35 DSGVO)

4. Drittlandtransfer ohne SCC (Art. 44 ff. DSGVO)
5. Versäumte 72h-Meldung der Datenpanne (Art. 33 DSGVO)

Die LDI NRW kündigt an, ein Bußgeld nach Art. 83 DSGVO zu erwägen.

3. Verteidigungsstrategie

3.1 Grundprinzip: Kooperative Verteidigung

Die Kanzlei SBD empfiehlt eine kooperative Verteidigungsstrategie, die auf folgende Elemente setzt:

Element A — Vollständige Transparenz: Offenlegung aller relevanten Sachverhalte gegenüber der LDI NRW, soweit nicht durch das Strafverfahren (StA Essen 12 Js 11.422/26) eine Verpflichtung zur Aussageverweigerung besteht.

Element B — Kooperationsbereitschaft: Aktive Mitarbeit bei der Aufklärung, Bereitsstellung sämtlicher Unterlagen, Terminisierung eines Auditermins mit LDI NRW vor Ort.

Element C — Sanierungsnachweis: Dokumentierter Nachweis aller Compliance-Massnahmen (DSFA, SCC, Meldung Art. 33, Betroffenenbenachrichtigung) als Milderungsfaktor Art. 83 Abs. 2 lit. c, f DSGVO.

Element D — Differenzierung von Vorwürfen: Anfechtung der Einzelvorwürfe hinsichtlich Vorsatz und Schwere; Argument, dass es sich um Fahrlässigkeit handelt (Art. 83 Abs. 2 lit. b DSGVO — Strafmilderung).

3.2 Stellungnahme-Struktur (Gliederung Schriftsatz — s. docx/)

1. Einleitung und Verfahrensdarstellung
2. Sachverhaltsdarstellung (berichtigt und ergänzt)
3. Stellungnahme zu jedem einzelnen Vorwurf
4. Nachweis der Sanierungsmassnahmen
5. Antrag: Statt Bußgeldbescheid — Verwarnung und Anordnung konformer Verarbeitung
6. Hilfsantrag: Bußgeldbemessung (s. Akte 09) — Reduktion auf massiges Mass
7. Antrag auf mündliche Anhörung gemäss § 28 VwVfG NRW

3.3 Verfahrensrechtliche Rechte der VCS

Im Verwaltungsverfahren der LDI NRW stehen VCS folgende Verfahrensrechte zu:

Recht	Rechtsgrundlage	Status
Recht auf Anhörung	§ 28 VwVfG NRW	Wird wahrgenommen
Akteneinsicht	§ 29 VwVfG NRW	Beantragt 14.01.2026
Recht auf anwaltliche Vertretung	BRAO	Vollmacht erteilt
Recht auf mündliche Verhandlung	§ 67 VwGO (nach Widerspruch)	Noch nicht beantragt
Widerspruch gegen Bescheid	§§ 68 ff. VwGO	Vorzubehalten
Verwaltungsgerichtsklage	§ 42 VwGO	Notfalls

4. Milderungsgruende nach Art. 83 Abs. 2 DSGVO

Relevante Milderungsgruende

Milderungsgrund	Art. 83 Abs. 2	Bewertung fuer VCS
Keine vorsaeztliche Handlung (Fahrllaessigkeit)	lit. b	Gut argumentierbar
Massnahmen zur Schadensminimierung	lit. c	Mittel (zu spaet)
Verantwortung des Verantwortlichen	lit. d	Negativ (GF gewusst)
Einschlaegige fruehere Verstoesse	lit. e	Keine Vorgeschichte
Kooperation mit Aufsichtsbehoerde	lit. f	Positiv
Kategorien personenbezogener Daten	lit. g	Negativ (Schufa-Daten)
Art der Kenntniserlangung	lit. h	Positiv (interner Hinweis)
Einhalten von Verhaltensregeln	lit. j	Keine BCR/Kodex
Finanzieller Vorteil oder Schaden	lit. k	Kein direkter Vorteil

Gesamtbewertung: 4 positive, 3 negative, 3 neutrale Faktoren. Bussgeldreduktion von maximal moeglich realistisch auf 15-25% des Maximalbetrags angestrebt (s. Akte 09).

5. Alternativszenario: Widerspruch und Verwaltungsgerichtsklage

Falls die LDI NRW einen Bussgeldbescheid in unverhaeltnismaessiger Hoehe erlaesst, wird folgende Rechtsbehelfs-Strategie verfolgt:

1. **Widerspruch** gemaess §§ 68 ff. VwGO gegen den Bussgeldbescheid (Frist: 1 Monat nach Zustellung)
2. **Antrag auf aufschiebende Wirkung** gemaess § 80 Abs. 5 VwGO (Vollstreckungsschutz)
3. **Klage vor VG Duesseldorf** (§ 42 VwGO i.V.m. § 20 Abs. 1 VwGO — zustaendiges Gericht fuer LDI NRW)
4. **Verfassungsbeschwerde** als letzte Instanz (s. Akte 21) — Verletzung des Verhaeltnismaessigkeitsgrundsatzes Art. 20 Abs. 3 GG, wirtschaftliche Existenz Art. 12 GG

6. Koordination mit Parallelverfahren

Das Aufsichtsverfahren LDI NRW (DSB-NW-44/26) ist mit den Parallelverfahren abzustimmen:

Verfahren	Wechselwirkung
VDuG-Sammelklage 18 Mass 4/26	Feststellungen LDI = potenzielle Beweismittel fuer Klaeger
StA Essen 12 Js 11.422/26	Erklaerungen ggue. LDI duerfen nicht strafprozessual verwertbar sein
LG Essen 4 O 244/26 (Tannenbruck)	Koordination Auskunft Art. 15 mit LDI-Verfahren

Massnahme: Saemtliche Erklaerungen gegenueber LDI NRW werden mit RA Dr. Specht und Strafverteidiger Dr. Ankermann koordiniert und enthalten explizite Verweigerungsvorbehalte fuer strafprozessual relevante Sachverhalte.

Quellen

- DSGVO Art. 55, 57, 58, 83 — dejure.org/gesetze/DSGVO
- BDSG § 17 — dejure.org/gesetze/BDSG
- VwVfG NRW §§ 28, 29 — dejure.org/gesetze/VwVfG_NW
- VwGO §§ 42, 68, 80 — dejure.org/gesetze/VwGO
- OVG NRW, Beschl. v. 10.03.2023 — 16 B 35/23 (LDI-Verfahren) — openjur.de

Datei: 09_bussgeldbemessung-art83-dsgvo.md

09 — Bussgeldbemessung nach Art. 83 DSGVO

Aktenzeichen: DSB-NW-44/26

Bearbeiter: RA Dr. Cornelius Specht

Datum: 22. Januar 2026

Betreff: Analyse der Bussgeldbemessung und Minimierungsstrategie

1. Rechtsrahmen Art. 83 DSGVO

Art. 83 DSGVO sieht ein zweistufiges Sanktionssystem vor:

Stufe 1 — Art. 83 Abs. 4 DSGVO: Geldbussen bis 10.000.000 EUR oder bis 2% des weltweiten Jahresumsatzes (je nachdem, welcher Betrag hoeher ist) fuer Verstoesse gegen Pflichten des Verantwortlichen und des Auftragsverarbeiters (Art. 8, 11, 25–39, 42, 43 DSGVO) sowie gegen Aufsichtsbehoerden-Anordnungen (Art. 58 Abs. 2 DSGVO).

Stufe 2 — Art. 83 Abs. 5 DSGVO: Geldbussen bis 20.000.000 EUR oder bis 4% des weltweiten Jahresumsatzes (je nachdem, welcher Betrag hoeher ist) fuer Grundsatzverstoesse (Art. 5, 6, 7, 9, 12–22, 44–49, 58 DSGVO).

1.1 Anwendbarer Bussgelder-Katalog fuer VCS

Verstoss	Sanktionsstufe	Bussgeldbetrag-Maximum
Art. 6 — fehlende Verarbeitunggrundlage	Art. 83 Abs. 5 lit. a	20.000.000 EUR
Art. 22 — unzulässige automatisierte Entscheidung	Art. 83 Abs. 5 lit. b	20.000.000 EUR
Art. 33 — versäumte Datenpannenmeldung	Art. 83 Abs. 4 lit. a	10.000.000 EUR
Art. 35 — unterlassene DSFA	Art. 83 Abs. 4 lit. a	10.000.000 EUR
Art. 44 — Drittlandtransfer ohne SCC	Art. 83 Abs. 5 lit. c	20.000.000 EUR

Kumulationsregel Art. 83 Abs. 3 DSGVO: Beziehen sich mehrere Verstösse auf dieselbe oder miteinander verbundene Verarbeitungsvorgänge, so ist die Geldbusse insgesamt auf den für den schwersten Verstoß geltenden Betrag zu begrenzen.

Massgeblicher Höchstbetrag: 20.000.000 EUR (Art. 83 Abs. 5 DSGVO — schwerste Verstösse).

2. EDSA-Leitlinien 04/2022: Bussgeldberechnungsmethodik

Der EDSA hat in den Leitlinien 04/2022 zur Berechnung von Geldbussen eine fünfstufige Methode veröffentlicht:

Schritt 1 — Identifizierung der Verarbeitungsvorgänge und sanktionierbaren Verstösse

Fünf Verstösse identifiziert (s. Tabelle oben). Ausgangspunkt: Schwerwiegendster Verstoß (Art. 5/6 DSGVO).

Schritt 2 — Ausgangsbetrag anhand der Schwere (Art. 83 Abs. 2 lit. a)

Gemäss EDSA-Leitlinien 04/2022, Rn. 56:

Schwere-Kategorie	Ausgangspunkt	Spanne
Geringfügig	0% bis 10% des Maximalbetrags	bis 2.000.000 EUR
Mittelschwer	10% bis 20% des Maximalbetrags	2.000.000 bis 4.000.000 EUR
Schwer	20% bis 100% des Maximalbetrags	4.000.000 bis 20.000.000 EUR

Bewertung des Hauptverstosses (Art. 6 DSGVO / Art. 22 DSGVO): **Schwer** (systematisches Massenscanning, 142.300 Betroffene, 3 Jahre).

Ausgangsbetrag: Ca. 30% des Maximalbetrags = 6.000.000 EUR (Schätzung).

Schritt 3 — Erschwerungsgründe (Art. 83 Abs. 2 lit. a–k)

Erschwerungsgrund	Art. 83 Abs. 2	Anwendbar	Auswirkung
Vorsatz	lit. b	Unklar (GF-Wissen bei § 42 BDSG)	+10-20%
Dauer des Verstosses	lit. a	Ja (3 Jahre)	+15%

Erschwerungsgrund	Art. 83 Abs. 2	Anwendbar	Auswirkung
Anzahl Betroffener (142.300)	lit. a	Ja	+10%
Sensitive Datenkategorien (Schufa)	lit. g	Ja	+10%
Versäumte Meldung Art. 33	lit. k	Ja	+5%

Gesamterhöhung: Ca. +50% auf Ausgangsbetrag = 9.000.000 EUR.

Schritt 4 — Milderungsgründe (Art. 83 Abs. 2)

Milderungsgrund	Art. 83 Abs. 2	Anwendbar	Auswirkung
Erste Verurteilung	lit. e	Ja	-10%
Kooperationsbereitschaft	lit. f	Ja	-15%
KMU (38 MA, ca. 4 Mio. EUR Umsatz)	Berücksichtigung	Ja	-20%
Nachträgliche Sanierungsmaßnahmen	lit. c	Teilweise	-5%

Gesamtreduktion: -50% auf erhöhten Betrag = 4.500.000 EUR.

Schritt 5 — Priorisierung und Höchstbetragscheck

Endkalkulation: ca. 4.500.000 EUR. Unter 20 Mio. EUR-Grenze. Aber: Wirtschaftliche Tragfähigkeit prüfen.

VCS-Kennzahlen:

- Jahresumsatz ca. 4.000.000 EUR
- 4%-Grenze: 160.000 EUR
- Bussgeld von 4.500.000 EUR entspricht 112% des Jahresumsatzes — existenzbedrohend

Verhältnismässigkeitsprüfung: Nach EuGH C-807/21 (Deutsche Wohnen, 05.12.2023) muss das Bussgeld wirksam, verhältnismässig und abschreckend sein. Ein Bussgeld, das die wirtschaftliche Existenz des Unternehmens vernichtet, kann im Einzelfall unverhältnismässig sein.

3. Argumentation zur Bussgeldminimierung

3.1 Hauptargumente

Argument 1 — Verhältnismässigkeit (Art. 49 GRCh, Art. 20 Abs. 3 GG): Ein Bussgeld von mehr als 1 Mio. EUR bei einem Jahresumsatz von 4 Mio. EUR gefährdet die wirtschaftliche Existenz von 38 Mitarbeitern. Das Bundesverfassungsgericht hat in BVerfG 1 BvR 2628/18 (Vereinigungsfreiheit) das Verhältnismässigkeitsprinzip auch bei Unternehmensgeldbussen bestätigt.

Argument 2 — EuGH C-807/21 (Deutsche Wohnen): Der EuGH hat klargestellt, dass Organhaftung nur bei individuellem Verschulden des Organs begründet werden kann. Das unpersönliche Handeln einer juristischen Person genügt nicht automatisch für die härteste Sanktionsstufe.

Argument 3 — Art. 83 Abs. 2 lit. b (keine Absicht): Der Verstoss gegen Art. 6 und Art. 22 DSGVO resultiert aus Rechtsunkenntnis der Geschaeftsfuehrung, nicht aus vorsaeztlicher Umgehung. Die interne Warnung der DSB Kessler-Brandt wurde zwar ignoriert, dies begrundet Fahrllaessigkeit, nicht Vorsatz.

Argument 4 — Frueher Zeitpunkt (Marktreife KI-Recht): Der Go-Live des Moduls (Maerz 2023) lag vor Veroeffentlichung der finalen EDSA-Leitlinien 01/2022 zur automatisierten Entscheidungsfindung. VCS befand sich in einer Rechtsunklarheit.

3.2 Angestrebte Bussgeldbandbreite

Szenario	Betrag	Voraussetzungen
Optimum (Verwarnung)	0 EUR	Vollstaendige Sanierung vor LDI-Entscheidung
Realistisches Minimum	250.000 EUR	Starke Kooperation, KMU-Abschlag
Wahrscheinliches Bussgeld	500.000 – 1.500.000 EUR	Standardfall kooperative Verteidigung
Worst Case	4.000.000 – 5.000.000 EUR	Alle Erschwerungsgruende, kein Entgegenkommen

Quellen

- DSGVO Art. 83 — dejure.org/gesetze/DSGVO
- EDSA-Leitlinien 04/2022 (Bussgeldbemessung) — [edpb.europa.eu](https://edpb.europa.eu/our-work-to-ols/our-documents/guidelines/guidelines-042022-calculation-administrative-fines-under-gdpr_de)
- EuGH C-807/21 (Deutsche Wohnen), Urt. v. 05.12.2023 — [eur-lex.europa.eu](https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62021CJ0807)
- BVerfG 1 BvR 2628/18 — [bundesverfassungsgericht.de](https://www.bundesverfassungsgericht.de)
- OLG Duesseldorf, Urt. v. 28.11.2023 — VI-5 Kart 11/19 OWi — openjur.de

Datei: 10_sammelklage-vdug-lg-essen-18mass4-26.md

10 — Sammelklage VDuG: LG Essen 18 Mass 4/26

Aktenzeichen: LG Essen 18 Mass 4/26

Bearbeiter: RAin Miriam Beckenbauer, RA Dr. Cornelius Specht

Datum: 23. Januar 2026

Betreff: Analyse und Verteidigungsstrategie Massenverfahren VDuG

1. Verfahrensgrundlagen VDuG

1.1 Das Verbraucherrecht durchsetzungsgesetz (VDuG)

Das VDuG (Verbraucherrecht durchsetzungsgesetz) ist am 13. Oktober 2023 in Kraft getreten und setzt die Verbandsklagenrichtlinie (EU) 2020/1828 in deutsches Recht um. Es ermoeoglicht qualifizierten Verbrauchereinrichtungen und Verboenden, Musterfeststellungsklagen und Abschoeepfungsklagen im

Namen einer Vielzahl von Verbrauchern zu erheben.

Anwendbarkeit auf DSGVO-Ansprueche: Das VDuG erfasst nach § 2 VDuG Unterlassungsansprueche, Feststellungsansprueche und Schadensersatzansprueche von Verbrauchern, die aus Rechtsverletzungen entstehen. Datenschutzverletzungen, die zu immateriellen Schaeden nach Art. 82 DSGVO fuehren, sind vom Anwendungsbereich erfasst, soweit die Betroffenen als Verbraucher agieren — was bei Mietinteressenten regelmaessig der Fall ist.

1.2 Verfahrensparteien

Klaeger: Verbraucherzentrale NRW e.V. (VZ NRW, Duesseldorf), Klaeger als repraesentative Einrichtung nach § 3 VDuG i.V.m. Anlage 1 VDuG, handelnd im Namen von 8.200 angemeldeten Betroffenen.

Beklagte: VermieterCheck Solutions GmbH, Ruhrallee 188, 45136 Essen.

Prozessbevollmaechtigte Beklagte: Specht, Beckenbauer & Drosselberg Rechtsanwaltsgesellschaft mbH, Duesseldorf.

2. Klagebegehren und Anspruchsgrundlage

2.1 Geltend gemachte Ansprueche

Die Verbraucherzentrale NRW macht geltend:

1. **Feststellungsklage (§ 15 VDuG):** Feststellung, dass VCS durch den Betrieb von ProspectScore Pro ohne wirksame Einwilligung das Recht der 8.200 Klaeger auf Schutz personenbezogener Daten verletzt hat

2. **Leistungsklage (Schadensersatz Art. 82 DSGVO):** Immaterieller Schadensersatz je 1.500 EUR pro betroffenem Mietinteressenten

3. **Unterlassung:** Unterlassung des weiteren Betriebs von ProspectScore Pro ohne DSGVO-konforme Rechtsgrundlage

Gesamtklagesumme: 8.200 x 1.500 EUR = 12.300.000 EUR zzgl. Zinsen und Kosten.

2.2 Anspruchsgrundlage Art. 82 DSGVO

Art. 82 Abs. 1 DSGVO gewaehrt jeder Person, der wegen eines Verstosses gegen die DSGVO ein materieller oder immaterieller Schaden entstanden ist, einen Anspruch auf Schadensersatz gegen den Verantwortlichen.

Haftungsvoraussetzungen:

1. Verstoß gegen DSGVO — von VCS nicht bestreitbar (s. Akten 03, 04)
2. Schaden (materiell oder immateriell) — s. Akte 11 (Bagatellgrenze)
3. Kausalzusammenhang — Verbindung Datenverletzung / Schaden umstritten

3. Verfahrensablauf VDuG-Massenverfahren

3.1 Verfahrensstadien

Stadium	Rechtsgrundlage	Status
Anmeldung der Betroffenen	§ 10 VDuG	Abgeschlossen (8.200 Betroffene)

Stadium	Rechtsgrundlage	Status
Eroeffnung Massenverfahren	§ 14 VDuG	Eroeffnet 15.12.2025
Feststellungsurteil	§§ 15-17 VDuG	Ausstehend
Individualurteil (Schadensersatz)	§§ 18-20 VDuG	Nach Feststellungsurteil
Vollstreckung	§§ 21-25 VDuG	Nach Urteil

3.2 Zustaendigkeit LG Essen

Das Landgericht Essen ist sachlich (§ 71 GVG — 5.000 EUR+) und oertlich (§ 12 VDuG — Sitz der Beklagten) zustaendig. Die speziell eingerichtete Kammer fuer Massenverfahren (18. Zivilkammer) ist gemaess Geschaeftsverteilungsplan 2026 zustaendig.

4. Verteidigungsargumente

4.1 Argument 1: Fehlende Aktivlegitimation der VZ NRW

Fuer die Aktivlegitimation nach § 3 VDuG muss die Klaegereinrichtung in der Liste des § 4 VDuG eingetragen sein (Qualifizierte Einrichtungen). Die VZ NRW ist als eingetragene Verbrauchereinrichtung anerkannt — dieses Argument schlaegt fehl.

Fallback: Pruefung, ob die geltend gemachten Ansprueche saemtlich von Verbrauchern stammen. Falls Unternehmer unter den 8.200 Anmeldern sind, sind diese aus dem Verfahren auszuscheiden.

4.2 Argument 2: Fehlender Schaden — Bagatellgrenze

S. ausfuehrlich Akte 11 (Art. 82 DSGVO Bagatellgrenze).

Kurzfassung: Der EuGH hat in C-300/21 (Oesterreichische Post, 04.05.2023) klargestellt, dass nicht jeder Verstoss gegen die DSGVO automatisch zu einem Schadensersatzanspruch fuehrt. Ein tatsaechlicher Schaden muss vorliegen; bloss abstrakte Angst genuegt grundsaeztlich nicht.

Verteidigungsargument: Kein Betroffener der 8.200 Klaeger hat dargelegt, infolge des ProspectScore-Pro-Scorings konkret eine Wohnung nicht bekommen zu haben. Die Sammelklage benoetigt individuelle Kausalitaetsnachweise.

4.3 Argument 3: Mitverschulden der Betroffenen

Betroffene, die ihre Einwilligung (wenn auch unwirksam) aktiv erteilt haben und sich dennoch bewerben, tragen ein Mitverschulden (§ 254 BGB analog). Argument: Die faktische Einwilligung begrenzt den Schadensersatz.

4.4 Argument 4: Verjaehrung

Art. 82 DSGVO sieht keine eigene Verjaehrungsregelung vor. Nach § 195 BGB gilt die regelmaeßige Verjaehrungsfrist von 3 Jahren. Fuer Mietinteressenten, die vor Januar 2023 bewertet wurden, koennte Verjaehrung eingetreten sein.

Pruefung: Kenntnismoment (§ 199 Abs. 1 BGB) — Betroffene hatten vor der oeffentlichen Berichterstattung (Dezember 2025 / Januar 2026) keine Kenntnis. Verjaehrung beginnt 01.01.2026 (Jahr der Kenntnis). Einwand greift nur fuer fruehste Verarbeitungen (vor 01.01.2023).

4.5 Argument 5: Mitwirkung an Sanierungsmassnahmen (Schlichtungsangebot)

VCS wird anbieten, einen Schlichtungsfonds von 500.000 EUR einzurichten und Betroffene pauschal mit 60 EUR je Person (= 492.000 EUR gesamt) zu entschädigen — als Vergleichsangebot vor Feststellungsurteil. Dies reduziert das Gesamtrisiko erheblich und ist PR-wirksam.

5. Prozesstaktik

Massnahme	Zeitpunkt	Ziel
Klageerwiderung einreichen	15.03.2026	Setzung Verteidigungspositionen
Antrag auf Vorabentscheidung EuGH	Ggf. nach Klageerwiderung	Kläerung Bagatellgrenze
Vergleichsangebot	Mai 2026	Verfahrensbeendigung
Sachverständigengutachten	Gemäss Beweisbeschluss	Widerlegung Kausalität

Quellen

- VDuG §§ 2, 3, 10, 14, 15, 18 — dejure.org/gesetze/VDuG
- DSGVO Art. 82 — dejure.org/gesetze/DSGVO
- EuGH C-300/21 (Oesterreichische Post), Urt. v. 04.05.2023 — [eur-lex.europa.eu](https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62021CJ0300)
- BGH VI ZR 10/24 — [bundesgerichtshof.de](https://www.bundesgerichtshof.de)
- BGB §§ 195, 199, 254 — dejure.org/gesetze/BGB
- Verbandsklagenrichtlinie (EU) 2020/1828 — [eur-lex.europa.eu](https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32020L1828)

Datei: 11_art82-schadensersatz-bagatellgrenze.md

11 — Art. 82 DSGVO: Schadensersatz und Bagatellgrenze

Aktenzeichen: LG Essen 18 Mass 4/26

Bearbeiter: RA Dr. Cornelius Specht

Datum: 24. Januar 2026

Betreff: Analyse der Schadensersatzpflicht Art. 82 DSGVO und Bagatellgrenzen-Argumentation

1. Tatbestand Art. 82 DSGVO

Art. 82 Abs. 1 DSGVO: Jede Person, der wegen eines Verstosses gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

Art. 82 Abs. 2 DSGVO: Verantwortliche haften fuer saemtliche Schaeden aus DSGVO-Verstoessen, sofern sie nicht nachweisen, dass sie in keiner Weise fuer den Umstand, durch den der Schaden eingetreten ist, verantwortlich sind.

2. Hoeherentwicklung der EuGH-Rechtsprechung

2.1 EuGH C-300/21 (Oesterreichische Post, 04.05.2023)

Leitsatz: Art. 82 DSGVO setzt einen tatsaechlichen Schaden voraus. Jede Verletzung der DSGVO fuehrt nicht automatisch zu einem Schadensersatzanspruch. Das Schadenserfordernis — auch fuer immaterielle Schaeden — besteht als eigene Haftungsvoraussetzung neben dem Vorliegen eines Verstosses und dem Kausalzusammenhang.

Konsequenz fuer VCS: Betroffene muessen darlegen und beweisen, dass ihnen tatsaechlich ein (auch immaterieller) Schaden entstanden ist. Die blossе Tatsache des Datenschutzverstosses genuegt nicht.

2.2 EuGH C-456/22 (Gemeinde Ummendorf, 14.12.2023)

Leitsatz: Der Begriff des immateriellen Schadens schliesst nicht jede Unzufriedenheit oder jede empfundene Unannehmlichkeit ein. Es muss eine messbare Beeintraehtigung vorliegen.

Konsequenz fuer VCS: Pauschale Behauptungen, man fuehle sich unwohl, genuegen nicht.

2.3 BGH VI ZR 10/24 (18.11.2024)

Leitsatz: Der BGH hat nach dem EuGH-Urteil C-300/21 klargestellt, dass auch der Kontrollverlust ueber eigene Daten einen immateriellen Schaden darstellen kann, wenn die betroffene Person den Verlust der Kontrolle tatsaechlich wahrgenommen hat und nicht lediglich abstrakt behauptet. Die Angst vor Missbrauch kann genuegen, wenn sie nicht nur rein hypothetisch ist.

Konsequenz fuer VCS: Bei 142.300 geleakten Datensaezen (CVE-2026-0188) liegt ein tatsaechlicher Datenverlust vor. Fuer diese Betroffenen ist ein Schaden leichter zu begruenden als fuer reine Profiling-Betroffene ohne Datenpanne.

2.4 OLG Hamm, Urt. v. 15.08.2023 — 7 U 19/23

Das OLG Hamm hat in einem vergleichbaren DSGVO-Schadensersatzfall (Kreditscoring) einen Schadensersatz von 2.000 EUR fuer immaterielle Schaeden zugesprochen, wo eine konkrete Ablehnung wegen fehlerhafter Schufa-Eintragung nachgewiesen war.

3. Analyse der 8.200 Klaeger-Ansprueche

3.1 Segmentierung der Klaeger nach Schadenslage

Segment	Anzahl	Schadenslage	Bewertung
A: Wohnungsablehnung nachweislich wegen ROT-Score	Geschaetzt 800	Stark (direkte Kausalitaet)	Anspruch wahrscheinlich
B: Datenleak-Betroffene (142.300 gesamt, davon Klaeger)	Geschaetzt 2.100	Mittel (Kontrollverlust belegt)	Anspruch moeglich

Segment	Anzahl	Schadenslage	Bewertung
C: Profiling-Betroffene ohne Datenleak, mit GRUEN/GELB-Score	Geschaetzt 3.400	Schwach (kein konkreter Schaden)	Anspruch zweifelhaft
D: Betroffene ohne nachweisliche Auswirkung	Geschaetzt 1.900	Minimal	Anspruch unwahrscheinlich

Verteidigungsansatz: Differenzierte Auseinandersetzung mit den Segmenten A bis D. Zugestaendnis bei Segment A und B (Vergleichsangebot), Abwehr bei C und D.

3.2 Hoehe des immateriellen Schadens

Art. 82 DSGVO enthaelt keine gesetzliche Schadenshoeheproblematik — die Berechnung erfolgt nach nationalen Grundsuetzen. Referenzpunkte:

Gericht	Fall	Zugesprochener Betrag
OLG Hamm 7 U 19/23	Schufa-Scoring-Fehler	2.000 EUR
LG Frankfurt 2-27 O 100/21	Datenleak Facebook	500–1.000 EUR
LG Duesseldorf 4 O 267/21	Whatsapp-Datenpanne	100 EUR
BGH VI ZR 10/24	Datenleak mit Kontrollverlust	1.200 EUR

Klaegerforderung: 1.500 EUR — am oberen Ende des realistischen Spektrums fuer reine Profiling-Faelle ohne Datenpanne.

Gegenargument VCS: Fuer Segment C und D liegt kein anspruchsbegrueendender Schaden vor. Selbst fuer Segment A und B ist 1.500 EUR uebersetzt; realistisch sind 300–800 EUR.

4. Bagatellgrenzen-Argumentation

4.1 Bagatellschwelle nach EuGH und BGH

Der BGH hat in VI ZR 10/24 keine explizite Bagatellgrenze eingefuehrt, aber betont, dass ein minimaler, unbedeutender Schaden nicht ausreicht. Das OLG Stuttgart (2 U 63/21) hat eine Bagatellschwelle von ca. 100 EUR als Untergrenze diskutiert.

4.2 VCS-Argumentation

Fuer Betroffene des Segments C (Profiling, GRUEN/GELB-Score, keine Wohnungsablehnung):

- Kein Datenleak (nicht Teil der 142.300 exfiltrierten Datensaeetze)
- Keine negative Scoring-Auswirkung (GRUEN/GELB = positive/neutrale Bewertung)
- Keine belegbare Angst oder psychische Belastung vorgetragen

Argument: Schadensersatzanspruch scheitert an der Voraussetzung eines tatsaechlichen (nicht bloss behaupteten) immateriellen Schadens.

5. Haftungsbefreiung Art. 82 Abs. 3 DSGVO

Art. 82 Abs. 3 DSGVO: Verantwortliche koennen sich von der Haftung befreien, wenn sie nachweisen, dass sie in keinerlei Hinsicht fuer den Umstand verantwortlich sind, durch den der Schaden entstanden ist.

Anwendbarkeit fuer VCS: Begrenzt. VCS ist als Verantwortlicher direkt fuer den Verstoss verantwortlich. Eine Entlastung kommt allenfalls in Betracht, wenn Sundara Tech als Auftragsverarbeiter den Datenleak verursacht hat (was die Forensik noch nicht klaert).

6. Gesamtbewertung und Vergleichsstrategie

Bestes Ergebnis fuer VCS: Abweisung der Klagen der Segmente C und D (ca. 5.300 Betroffene x 1.500 EUR = 7.950.000 EUR entlastet). Vergleich mit Segmenten A und B bei 600 EUR je Person = 1.740.000 EUR.

Realistisches Vergleichsangebot: 500.000 EUR Pauschalbetrag fuer Schlichtungsfonds, verwaltet von der VZ NRW. Verteilung an Betroffene nach Schadensnachweisstufe.

Quellen

- DSGVO Art. 82 — dejure.org/gesetze/DSGVO
- EuGH C-300/21 (Oesterreichische Post) — [eur-lex.europa.eu](https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62021CJ0300)
- EuGH C-456/22 (Gemeinde Ummendorf) — [eur-lex.europa.eu](https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62022CJ0456)
- BGH VI ZR 10/24 — [bundesgerichtshof.de](https://www.bundesgerichtshof.de)
- OLG Hamm 7 U 19/23 — openjur.de
- BGB § 254 — dejure.org/gesetze/BGB

Datei: 12_auskunftersuchen-art15-tannenbruck.md

12 — Auskunftersuchen Art. 15 DSGVO: Dr. Susanna Tannenbruck

Aktenzeichen: LG Essen 4 O 244/26

Bearbeiter: RAin Miriam Beckenbauer

Datum: 25. Januar 2026

Betreff: Analyse und Strategie Auskunftersuchen Dr. Tannenbruck

1. Personenprofil und Bedeutung des Falls

1.1 Betroffene Person

Dr. Susanna Tannenbruck

- Beruf: Soziologin (Inhaberin eines Lehrstuhls an der Universitaet Duisburg-Essen, Forschungsschwerpunkt: Algorithmische Diskriminierung im Wohnungsmarkt)

- Adresse: Gildehofstrasse 18, 45127 Essen (angemietete Wohnung)
- Status: Klage im Verfahren LG Essen 4 O 244/26 (Einzelklage Schadensersatz Art. 82 DSGVO)
- Prozessbevollmächtigte: RAin Prof. Dr. Hannelore Stuermer-Koch, Essen

1.2 Besondere Risikobewertung

Dr. Tannenbrück ist als Soziologin, die zu algorithmischer Diskriminierung forscht, eine Hochprofil-Betroffene. Sie hat:

- Im März 2025 eine Wohnung in Essen-Ruettenscheid beworben und eine Absage erhalten
- Anschliessend erfahren, dass die Absage mit einem ROT-Score in ProspectScore Pro zusammenhing
- Im Dezember 2025 das Auskunftersuchen gemäss Art. 15 DSGVO an VCS gestellt
- Im Januar 2026 Klage erhoben (LG Essen 4 O 244/26) auf: Auskunftserteilung, Schadensersatz 1.500 EUR, Unterlassung weiterer Verarbeitung

Zusätzliches Risiko: Dr. Tannenbrück hat bereits Kontakt zum NDR-Journalisten Felix Kaltenbach (s. Akte 13) aufgenommen. Eine Kooperation beider Personen als Zeugen und Informationsquellen für ein NDR-Panorama-Feature droht.

2. Rechtsrahmen Art. 15 DSGVO

2.1 Auskunftsrecht der betroffenen Person

Art. 15 Abs. 1 DSGVO gibt der betroffenen Person das Recht, vom Verantwortlichen eine Bestätigung zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden. Falls ja, hat sie ein Recht auf Auskunft über:

lit.	Inhalt der Auskunft
a	Verarbeitungszwecke
b	Kategorien verarbeiteter Daten
c	Empfänger oder Kategorien von Empfängern
d	Speicherdauer oder Kriterien für deren Festlegung
e	Rechte auf Berichtigung, Löschung, Einschränkung, Widerspruch
f	Beschwerderecht bei Aufsichtsbehörde
g	Herkunft der Daten (wenn nicht direkt erhoben)
h	Informationen über automatisierte Entscheidungsfindung einschl. Profiling

Art. 15 Abs. 3 DSGVO gibt zusätzlich ein Recht auf Kopie der personenbezogenen Daten.

2.2 Besondere Relevanz Art. 15 Abs. 1 lit. h (Profiling-Auskunft)

Für automatisierte Entscheidungen einschliesslich Profiling gemäss Art. 22 DSGVO muss die Auskunft enthalten:

- Aussagekräftige Informationen über die involvierte Logik
- Die Tragweite der Verarbeitung
- Die angestrebten Auswirkungen einer solchen Verarbeitung für die betroffene Person

Dies ist fuer VCS besonders heikel: Die Offenlegung der ProspectScore-Logik (welche Datenpunkte, welche Gewichtung) birgt das Risiko, dass Dr. Tannenbruck die Diskriminierungsmechanismen des Modells wissenschaftlich dokumentiert.

3. Moeglichkeiten der Einschraenkung nach Art. 15 DSGVO

3.1 Ausnahmen und Einschraenkungen

Art. 15 DSGVO sieht keine unmittelbaren Ausnahmen vor, aber ErwGr. 63 DSGVO gibt Hinweise: Das Recht auf Kopie darf die Rechte und Freiheiten anderer Personen nicht beeintraehtigen.

Moegliche Einschraenkungsgruende fuer VCS:

1. **Geschaeftsgeheimnisse (§ 14 GeschGehG):** Die interne Logik des ProspectScore-Algorithmus kann als Geschaeftsgeheimnis qualifizieren. Jedoch: Der konkrete Score und die Datenkategorien der betroffenen Person selbst muessen offenbart werden.
2. **Sonstiger Personenbezug:** Die Auskunft darf keine Daten Dritter enthalten — ein Ausnahmegrund, der bei ProspectScore Pro kaum greift.
3. **Missbraeuchliche Auskunft:** Bei nachgewiesener Schikane-Absicht koennte § 242 BGB greifen — hier aber unwahrscheinlich.

Ergebnis: VCS muss den Score (78/100 — ROT) und die zugrundeliegenden Datenkategorien offenlegen. Die interne Algorithmuslogik kann als Geschaeftsgeheimnis eingeschaenkt werden, jedoch nur mit expliziter Begrueundung.

4. Fristen und Versaeumnis

4.1 Fristberechnung

- Auskunftersuchen Dr. Tannenbruck: 12. Dezember 2025 (schriftlich per Einschreiben)
- Regelmaessige Antwortfrist: 1 Monat (Art. 12 Abs. 3 DSGVO) = 12. Januar 2026
- Verlaengerungsmoeglichkeit: Weitere 2 Monate bei Komplexitaet (Art. 12 Abs. 3 Satz 2 DSGVO) — **Benachrichtigung erforderlich bis 12. Januar 2026**
- Tatsaechliche Reaktion VCS: Keine Antwort bis 14.01.2026 (Mandatsuebernahme SBD)

Ergebnis: Die Frist nach Art. 12 Abs. 3 DSGVO ist bereits abgelaufen. VCS befindet sich im Verzug. Eine Klage auf Auskunftserteilung (§ 15 VwGO analog; zivilrechtlich: § 241 BGB) ist erhoben (LG Essen 4 O 244/26).

4.2 Strategische Massnahme

Sofortige Auskunftserteilung vor dem naechsten Verhandlungstermin LG Essen ist die einzig sinnvolle Massnahme, um:

- Die Klagedurchsetzung (Hauptantrag Auskunft) zu neutralisieren
- Als Kooperationssignal zu wirken
- Den Schadensersatzanspruch von 1.500 EUR zu minimieren (kein zusaetzlicher Verzugsschaden)

5. Entwurf: Auskunftsschreiben an Dr. Tannenbruck

Betreff: Antwort auf Ihr Auskunftersuchen gemaess Art. 15 DSGVO vom 12.12.2025

Zu verarbeiteten Daten:

- Name: Dr. Susanna Tannenbruck
- Adresse: Gildehofstrasse 18, 45127 Essen
- Bewerbungsdatum: 08.03.2025
- Objekt-ID (intern): ESS-RUE-2025-0144
- Verarbeitete Datenkategorien: Name, Adresse, Schufa-Score (714 Punkte), Beruf (Soziologin/Universitätslehrerin), Familienstatus (ledig, keine Kinder)
- ProspectScore: 78/100 (Ampel: ROT — Kategorie „Erhöhtes Risiko“)
- Empfänger: Vermieter H.-D. Krankenhofer, Essen (über Plattform-Interface)
- Speicherdauer: 24 Monate seit letzter Abfrage (bis März 2027)
- Rechtsgrundlage: (war fehlerhaft — Art. 6 Abs. 1 lit. a DSGVO, Einwilligung unwirksam — Korrektur in Bearbeitung)
- Datenschutzbeauftragte: Hannelore Kessler-Brandt, dsb@vermietercheck.de, 0201/498820
- Beschwerderecht: LDI NRW, Kavalleriestrasse 2-4, 40213 Düsseldorf, poststelle@ldi.nrw.de
- Herkunft: Selbstauskunft Mietinteressentin, Schufa Holding AG (B2B-API)
- Automatisierte Entscheidung: Ja — Score 78/100 generiert durch ProspectScore Pro v3.0; Ampel ROT bedeutet Risikoklassifikation „Erhöhtes Mietausfallrisiko“. Scoring-Faktoren: Schufa-Score (40% Gewichtung), Einkommenssituation (30%), Stabilität Anstellungsverhältnis (20%), Familienstatus (10%).

6. Parallelverfahrens-Koordination

Da Dr. Tannenbruck gleichzeitig mit Felix Kaltenbach (NDR) kooperiert, sind sämtliche Auskunftsinhalte mit der PR-Strategie (s. Akte 20) abzustimmen. Keine öffentlichen Statements über den Auskunftsvorgang ohne Freigabe durch RA Dr. Specht.

Quellen

- DSGVO Art. 12, 15, 22 — dejure.org/gesetze/DSGVO
- Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) § 14 — dejure.org/gesetze/GeschGehG
- BGB §§ 241, 242 — dejure.org/gesetze/BGB
- OLG Frankfurt, Urt. v. 02.03.2022 — 6 U 270/20 (Auskunftsrecht DSGVO) — openjur.de
- EuGH C-307/22 (FT gg. DW), Urt. v. 26.10.2023 (Kopienrecht Art. 15 Abs. 3 DSGVO) — [eur-lex.europa.eu](https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62022CJ0307)

Datei: 13_auskunftsersuchen-art15-drostermann-kaltenbach.md

13 — Auskunftersuchen Art. 15 DSGVO: Drostermann und Kaltenbach

Aktenzeichen: intern / kein Gerichtsverfahren (noch)

Bearbeiter: RAin Miriam Beckenbauer

Datum: 26. Januar 2026

Betreff: Hochprofil-Auskunftsersuchen: Autorin Wibke Drostermann und Journalist Felix Kaltenbach

1. Vorbemerkung: Hochprofil-Betroffene

Neben Dr. Tannenbruck (s. Akte 12) haben zwei weitere Hochrisiko-Betroffene Auskunftsersuchen gemaess Art. 15 DSGVO gestellt, deren Bearbeitung einer gesonderten Analyse bedarf:

1. **Wibke Drostermann** — Sachbuchautorin, Veroeffentlichung eines Buches ueber Diskriminierung im Mietmarkt (erscheint Maerz 2026, Rowohlt-Verlag), mit einem Kapitel ueber VermieterCheck

2. **Felix Kaltenbach** — Wissenschaftsjournalist, NDR Panorama, recherchiert fuer eine Sendereihe ueber KI-Profiling im deutschen Mietmarkt (Sendetermin geplant Maerz 2026)

Beide Personen repraesentieren ein erhebliches Reputationsrisiko fuer VCS, das ueber das rechtliche Risiko hinausgeht.

2. Auskunftsersuchen Wibke Drostermann

2.1 Sachverhalt

- **Name:** Wibke Drostermann
- **Beruf:** Freie Sachbuchautorin (Wohnort: Hamburg, Mietinteressentin in Essen fuer eine Zweitwohnung)
- **Bewerbung:** November 2024, Objekt Essen-Kettwig, Absage wegen ROT-Score (81/100)
- **Auskunftsersuchen:** 03. Januar 2026 (schriftlich, per Einschreiben)
- **Frist:** 03. Februar 2026 (1 Monat Art. 12 Abs. 3 DSGVO)
- **Buchtitel (angekuendigt):** „Sortiert und abgelehnt — Wie Algorithmen entscheiden, wer einziehen darf“

2.2 Strategie

Prioritaet: Fristkonforme Auskunftserteilung bis spaetestens 01.02.2026.

Besonderheit: Da Frau Drostermann ein Buch plant, in dem der Vorfall thematisiert wird, sind bei der Auskunftserteilung keine zusaetzlichen Informationen jenseits des rechtlich Gebotenen zu erteilen. Insbesondere:

- Keine Stellungnahmen zum Verarbeitungsprozess allgemein
- Kein Ausdruck von Bedauern, der als Schuldeingestaendnis interpretiert werden kann
- Rechtlich korrekte, sachliche und vollstaendige Auskunft

Inhalt der Auskunft (Art. 15 Abs. 1 DSGVO):

- Daten: Name, Adresse, Schufa-Score (unvollstaendig — 0 Negativmerkmale, Score 720), Beruf (Autorin/freiberufllich), Haushaltseinkommen (Selbstauskunft ca. 4.200 EUR/Monat)
- ProspectScore: 81/100 (ROT) — Hauptfaktor: Einkommensunsicherheit bei Selbststaendigkeit
- Datenschutzbeauftragte, Beschwerderecht, Rechtsgrundlage

Moeglicher Folgekonflikt: Frau Drostermann plant moeglicherweise, die Auskunft im Buch abzudrucken. Dies ist grundsaeztlich ihr Recht (Informationsfreiheit Art. 5 GG). VCS kann dies nicht verhindern, aber

durch sachliche, rechtlich einwandfreie Auskunft das Reputationsrisiko minimieren.

2.3 Recht auf Berichtigung / Loeschung

Frau Drostermann hat gleichzeitig folgende Antraege gestellt:

- **Art. 16 DSGVO (Berichtigung):** Der ROT-Score sei sachlich falsch — ihr Einkommen sei stabil
- **Art. 17 DSGVO (Loeschung):** Alle ihre Daten seien zu loeschen, da keine wirksame Rechtsgrundlage

Bewertung:

- Art. 16: Pruefung erforderlich — Wenn der Score auf falschen Angaben beruht (z.B. Einkommen als selbststaendig niedriger bewertet als tatsaechlich), ist Berichtigung vorzunehmen
- Art. 17: Nach Einraeumen des Verstosses gegen Art. 6 DSGVO muss die Loeschung erfolgen (Art. 17 Abs. 1 lit. d — Daten unrechtmassig verarbeitet)

3. Auskunftersuchen Felix Kaltenbach

3.1 Sachverhalt

- **Name:** Felix Kaltenbach
- **Beruf:** Wissenschaftsjournalist, NDR Panorama (Hamburg)
- **Funktion:** Bewirbt sich nicht selbst, sondern recherchiert professionell; fragt Auskunft im eigenen Namen als (angeblicher) Mietinteressent ab
- **Bewerbung:** September 2024, Objekt Essen-Holsterhausen (testweise fuer Recherchezwecke)
- **Score:** 44/100 (GRUEN) — Herr Kaltenbach selbst erzielt nur einen GRUEN-Score
- **Auskunftersuchen:** 05. Januar 2026 (formal per Anwalt, RA Thomas Grimmstein, Hamburg)
- **Frist:** 05. Februar 2026

3.2 Besondere Rechtslage: Journalistische Recherche

Felix Kaltenbach hat im Rahmen eines erklarten Recherchevorhabens (NDR Panorama) professionell eine Wohnungsbewerbung durchgefuehrt, um das Scoring-System zu testen. Dies wirft spezifische Rechtsfragen auf:

Frage 1 — Ist Kaltenbach als „Betroffener“ legitimiert? Ja. Auch journalistische Bewerbungen begruendet eine Betroffenenstellung nach Art. 4 Nr. 1 DSGVO (seine Daten wurden verarbeitet). Das Motiv spielt keine Rolle.

Frage 2 — Sind Auskunftsansprueche durch Pressefreiheit erweitert? Nein. Art. 15 DSGVO gewaehrt dieselben Rechte wie anderen Betroffenen. Das Medienprivileg (Art. 85 DSGVO, § 23 MStV) gilt fuer Verarbeitung durch Presseunternehmen, nicht fuer ihre Ansprueche gegen Dritte.

Frage 3 — Kann VCS die Auskunft wegen des journalistischen Zwecks verweigern? Nein. Eine solche Verweigerung waere rechtswidrig und wuerde die Berichterstattung verschlimmern.

3.3 Strategie

Massnahme 1: Auskunft fristgerecht erteilen (sachlich, vollstaendig, ohne ueberflussige Erklaerungen).

Massnahme 2: Separate PR-Massnahme: Proaktiver Kontakt zu NDR Panorama durch Media-Relations-Experten (nicht RA Dr. Specht) mit Angebot eines Interviews ueber die bereits eingeleiteten Sanierungsmassnahmen.

Massnahme 3: Keine rechtlichen Schritte gegen Kaltenbach oder NDR — dies wuerde als Einschuechterungsversuch gewertet und die Berichterstattung eskalieren.

Massnahme 4: Vorbereitung einer kurzen, sachlichen Stellungnahme fuer moegliche NDR-Anfrage (Redaktionsschluss vermutlich Maerz 2026).

4. Vergleichende Auskunftsstrategie

Person	Frist	Prioritaet	Inhalt	Tonalitaet
Dr. Tannenbruck	Abgelaufen — sofort	KRITISCH	Vollstaendig + Koordination mit LG Essen	Formal, kooperativ
Wibke Drostermann	03.02.2026	HOCH	Vollstaendig, sachlich	Neutral, keine Entschuldigungen
Felix Kaltenbach	05.02.2026	HOCH	Vollstaendig, sachlich	Neutral + PR-Vorbereitung

5. Rechtliche Folgen bei Nichterteilung

Gemaess Art. 83 Abs. 5 lit. b DSGVO ist die Verletzung der Betroffenenrechte (Art. 12–22 DSGVO) mit einem Bussgeld bis 20.000.000 EUR oder 4% des Jahresumsatzes bedroht.

Zusaetzlich: Klage auf Auskunftserteilung (§ 15 DSGVO) — Unterlassungsklage und Schadensersatz Art. 82 DSGVO.

Quellen

- DSGVO Art. 12, 15, 16, 17, 83, 85 — dejure.org/gesetze/DSGVO
- MStV § 23 (Medienprivileg) — dejure.org/gesetze/MStV
- GG Art. 5 (Pressefreiheit) — dejure.org/gesetze/GG
- EuGH C-307/22 (Kopienrecht Art. 15 Abs. 3 DSGVO) — [eur-lex.europa.eu](https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62022CJ0307)
- OLG Frankfurt 6 U 270/20 — openjur.de

Datei: 14_hinschg-meldung-whistleblower-strategie.md

14 — HinSchG-Meldung und Whistleblower-Strategie

Aktenzeichen: DSB-NW-44/26 (verbunden)

Bearbeiter: RA Lars Drosselberg

Datum: 27. Januar 2026

Betreff: Analyse der HinSchG-Meldung und rechtliche Bewertung der Unternehmensstrategie

1. Sachverhaltsdarstellung

1.1 Die anonyme HinSchG-Meldung

Am 08. November 2025 wurde ueber den internen Hinweisgeberkanal der VermieterCheck Solutions GmbH (Whistleblowing-Portal, Software: Speakout GmbH) folgende anonyme Meldung eingereicht:

Meldungsinhalt (Zusammenfassung durch interne Meldestelle): > „Seit Oktober 2022 werden Produktionsdaten von Mietinteressenten an die indische Firma Sundara Tech Pvt. Ltd. (Bengaluru) uebertragen. Es gibt weder Standarddatenschutzklauseln noch einen korrekten Auftragsverarbeitungsvertrag. Das Management weiss davon. Der DSB hat mehrfach intern gewarnt, ohne Ergebnis.“

Hinweisgeber: Anonym — aufgrund der Spezifitaet der Informationen wahrscheinlich ein ehemaliger DevOps-Mitarbeiter (hat Zugriff auf Systemarchitektur gehabt; ausgeschieden ca. Juli 2025).

1.2 Reaktion der internen Meldestelle

Die interne Meldestelle (geleitet von Compliance-Officer Frau Patricia Hoelzken-Rabe) hat die Meldung am 12.11.2025 intern als „nicht pruefrelevant“ klassifiziert und keine weiteren Massnahmen ergriffen. Eine Rueckmeldung an den Hinweisgeber ist nicht erfolgt.

2. Rechtsrahmen Hinweisgeberschutzgesetz (HinSchG)

2.1 Anwendungsbereich HinSchG

Das HinSchG (Hinweisgeberschutzgesetz, in Kraft seit 02. Juli 2023) setzt die EU-Whistleblower-Richtlinie 2019/1937 in deutsches Recht um. Es gilt fuer Beschaeftigte und ehemalige Beschaeftigte, die Informationen ueber Verstaesse, die gegen EU-Recht (einschliesslich DSGVO) verstossen, melden.

Sachlicher Anwendungsbereich § 2 HinSchG: § 2 Abs. 1 Nr. 11 HinSchG: Datenschutzrecht einschliesslich DSGVO ist ausdruecklich erfasst.

Persoenerlicher Anwendungsbereich § 1 HinSchG: Ehemalige Beschaeftigte sind geschuetzt (§ 1 Abs. 1 HinSchG). Anonyme Hinweisgeber koennen Schutz in Anspruch nehmen, soweit ihre Identitaet spaeter bekannt wird (§ 8 Abs. 2 HinSchG).

2.2 Pflichten des Unternehmens nach HinSchG

VCS (38 Mitarbeiter) unterliegt gemaess § 12 HinSchG (Unternehmen ab 50 Mitarbeitern) noch nicht der zwingenden Pflicht, ein internes Meldesystem einzurichten. Jedoch:

- Das freiwillig eingerichtete Meldesystem unterliegt den Pflichten des § 17 HinSchG (Rueckmeldung innerhalb von 3 Monaten)
- Die Nichtbearbeitung einer eingegangenen Meldung kann eine Pflichtverletzung darstellen

Pruefung § 12 HinSchG: 38 Mitarbeiter liegt unter der Schwelle von 50. Daher keine Pflicht zur Einrichtung eines Meldesystems — aber das freiwillig eingerichtete System muss regelkonform betrieben werden.

2.3 Schutz des Hinweisgebers § 36 HinSchG

§ 36 Abs. 1 HinSchG verbietet Repressalien gegen Hinweisgeber. Repressalien sind alle Massnahmen oder Unterlassungen, die unmittelbar oder mittelbar durch die Meldung veranlasst werden.

Praktische Konsequenz fuer VCS: Es darf keine Identifizierung oder Massnahmen gegen den mutmasslichen Hinweisgeber (ehem. DevOps-Mitarbeiter) eingeleitet werden.

3. Bewertung der Unternehmensreaktion

3.1 Versaeumnisse

Versaeumnis	Rechtsgrundlage	Schwere
Keine Bearbeitung der Meldung	§ 17 Abs. 1 HinSchG	Mittel
Keine Rueckmeldung an Hinweisgeber	§ 17 Abs. 2 HinSchG (3-Monats-Frist)	Mittel
Klassifizierung als „nicht pruefrelevant“ ohne Pruefung	§ 16 HinSchG (Pruefpflicht)	Hoch
Moegliche Verschleierungsgefahr (interne Meldung ignoriert)	§ 27 HinSchG (Beweislast)	Hoch

3.2 Ordnungswidrigkeitspotenzial

§ 40 HinSchG stellt Verstoesse gegen die Pflichten der §§ 12–17 HinSchG als Ordnungswidrigkeiten unter Bussgelder von bis zu 20.000 EUR (§ 40 Abs. 3 HinSchG). Fuer VCS kommen Verstoesse gegen § 17 (Rueckmeldung) in Betracht.

4. Externe Meldung an LDI NRW

Die LDI NRW fungiert auch als externe Meldestelle nach HinSchG fuer Datenschutzverletzungen (§ 19 HinSchG i.V.m. § 2 Abs. 1 Nr. 11 HinSchG). Der anonyme Hinweis, den die LDI NRW am 03.12.2025 erhalten hat, koennte von demselben Hinweisgeber stammen — was die parallele externe Meldung erklart.

Konsequenz: Die externe Meldung an LDI NRW hat das Aufsichtsverfahren DSB-NW-44/26 mitausgeloest. Dies ist rechtmassig.

5. Strategie gegenueber dem mutmasslichen Hinweisgeber

5.1 Identifizierungsverbot

VCS darf keine aktiven Massnahmen zur Identifizierung des Hinweisgebers ergreifen. Insbesondere:

- Kein Abgleich des Meldungsinhalts mit Systemzugriffsprotokollen zur Identifizierung
- Keine Befragung ehemaliger Mitarbeiter mit dem Ziel der Identifizierung
- Keine arbeitsrechtlichen oder zivilrechtlichen Schritte gegen identifizierte Verdaechtige ohne abgesicherten Nachweis einer Falschaussage (§ 37 HinSchG)

5.2 Meldungsinhalt verwenden

Paradoxerweise dient der Inhalt der HinSchG-Meldung als interner Aufklaerungsanlass: VCS kann und soll die Information nutzen, um die Drittlandsuebermittlung (Art. 44 DSGVO) intern zu untersuchen und zu sanieren. Dies demonstriert der LDI NRW das Vorhandensein eines internen Compliance-Systems.

6. Moegliche Strafanzeige durch Hinweisgeber (§ 42 BDSG)

Es ist nicht auszuschliessen, dass der Hinweisgeber zusaetzlich eine Strafanzeige nach § 42 BDSG wegen der Drittlandsuebermittlung bei der StA Essen eingereicht hat. Die StA Essen fuehrt bereits ein Verfahren 12 Js 11.422/26 (hauptsaechlich wegen des GF-Verhaltens, s. Akte 15). Eine Ausdehnung auf die institutionelle Drittlandsuebermittlung ist moeglich.

Koordinationsmassnahme: Strafverteidiger Dr. Ankermann wird ueber dieses Szenario informiert.

7. Handlungsempfehlungen

1. **Meldungsbearbeitung nachholen:** Formale Pruefung der Meldung vom 08.11.2025 dokumentieren und rueckwirkend archivieren
2. **Rueckmeldung:** Anonyme Rueckmeldung ueber das Whistleblowing-Portal (soweit Hinweisgeber-Postfach noch aktiv): Meldung wurde geprueft, Massnahmen eingeleitet
3. **HinSchG-Compliance-Training:** Schulung der internen Meldestelle (Frau Hoelzken-Rabe) zu HinSchG-Pflichten
4. **Protokolldaten:** Keine Nutzung von System-Logs zur Identifizierung des Hinweisgebers

Quellen

- HinSchG §§ 1, 2, 8, 12, 16, 17, 19, 36, 37, 40 —
dejure.org/gesetze/HinSchG
- EU-Whistleblower-Richtlinie 2019/1937 —
[eur-lex.europa.eu](https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32019L1937)
- BDSG § 42 — dejure.org/gesetze/BDSG
- DSGVO Art. 44 ff. — dejure.org/gesetze/DSGVO

Datei: 15_strafrechtliche-verteidigung-par42-bdsg.md

15 — Strafrechtliche Verteidigung: § 42 BDSG

Aktenzeichen: StA Essen 12 Js 11.422/26

Bearbeiter: RA Dr. Cornelius Specht (koordiniert mit Strafverteidiger RA Dr. Robert Ankermann)

Datum: 28. Januar 2026

Betreff: Strafverteidigung GF Schimmelpfennig-Drosthager wegen § 42 BDSG

1. Verfahrensgrundlagen

1.1 § 42 BDSG — Straftatbestand

§ 42 BDSG statuiert Straftatbestaende im Bereich des Datenschutzrechts:

§ 42 Abs. 1 BDSG: Wer wissentlich nicht allgemein zugaengliche personenbezogene Daten einer Person in der Absicht, sich oder einen Dritten zu bereichern oder die betroffene Person zu schaedigen, unbefugt verarbeitet, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

§ 42 Abs. 2 BDSG: Wer die im Abs. 1 bezeichneten Daten gegen Entgelt oder in der Absicht, sich oder Dritten zu bereichern oder Dritte zu schädigen, unbefugt verarbeitet, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

Antragsdelikt: § 42 Abs. 3 BDSG — Die Tat wird bei § 42 Abs. 1 nur auf Antrag verfolgt (Antragsdelikt). Bei § 42 Abs. 2 handelt es sich um ein Officialdelikt (Strafverfolgung von Amts wegen).

2. Tatvorwurf im Verfahren 12 Js 11.422/26

2.1 Anklagesachverhalt (Zusammenfassung)

Die StA Essen hat folgende Tatvorwürfe formuliert:

GF Karl-Heinz Schimmelpfennig-Drosthager soll in der Zeit zwischen März 2023 und Dezember 2025 die in der VCS-Datenbank gespeicherten Daten von Mietinteressenten — darunter Bonitätsauskünfte, ProspectScores und Kontaktdaten — gezielt für eigene Zwecke genutzt haben, um für drei Wohnungen in Essen-Bredeney die idealen Mieter auszuwählen. Er soll Datenbankabfragen in der Produktionsumgebung persönlich durchgeführt haben (IP-Adresse des GF-Notebooks identifiziert) und auf dieser Grundlage drei Mietinteressenten bevorzugt und andere abgelehnt haben.

Konkrete Vorwürfe:

1. Direktabfragen der Kundendatenbank aus dem GF-Account (keine Vermittlerrolle — rein persönliche Eigennutzung)
2. Auswahl von Mietinteressenten nach ProspectScore und Beruf (Bevorzugung von Beamten und Festangestellten)
3. Weitergabe der Daten an keine weiteren Personen (kein Dritter profitiert)

2.2 Einschlägiger Tatbestand

§ 42 Abs. 2 BDSG: Verarbeitung mit der Absicht, sich zu bereichern. Die Eigennutzung der Plattform zur Auswahl besserer Mieter (wirtschaftlicher Vorteil: niedrigeres Mietausfallrisiko) erfüllt den Begriff der Bereicherungsabsicht.

Strafrahmen: Freiheitsstrafe bis zu drei Jahren oder Geldstrafe. Als Officialdelikt wird das Verfahren von Amts wegen geführt.

3. Verteidigungsstrategie

3.1 Bestreiten des Vorsatzes

Argument A — Fehlende Bereicherungsabsicht: Die Nutzung der eigenen Unternehmensplattform für private Wohnungsvermietung begründet nicht zwingend eine Bereicherungsabsicht im Sinne des § 42 BDSG. Herr Schimmelpfennig-Drosthager hat die Plattform genutzt, die er selbst entwickelt hat. Die Vermietung von Wohnungen ist eine erlaubte private Tätigkeit; die Nutzung einer eigenen Datenbank dafür stellt subjektiv möglicherweise keine „unbefugte“ Verarbeitung im Sinne des § 42 BDSG dar.

Argument B — Tatbestandsausschlusskräfte: „Unbefugt“: § 42 BDSG setzt unbefugte Verarbeitung voraus. Schimmelpfennig-Drosthager als Geschäftsführer und wirtschaftlicher Eigentümer von VCS hat im weitesten Sinne eine Befugnis, auf die Daten zuzugreifen — jedenfalls aus seiner Sicht. Die Unbefugtheit muss ihm subjektiv bewusst gewesen sein. Dies ist zu bestreiten: Er hat möglicherweise irrig angenommen, als GF dürfe er die Firmendaten auch privat nutzen.

Strafrechtlicher Irrtum: Verbotsirrtum § 17 StGB — Irrtum über die Rechtswidrigkeit der Tat. Prüfung: Hätte Schimmelpfennig-Drosthager bei zumutbarer Anstrengung die Unbefugtheit erkennen können?

Als GF ohne juristischen Hintergrund und ohne Datenschutzberatung (DSB hatte nicht ausdruecklich auf § 42 BDSG hingewiesen): Argument fuer einen vermeidbaren Verbotsirrtum mit Strafmilderung.

3.2 Bestreiten des Tatbestandsmerkmals „nicht allgemein zugaenglich“

Die Daten in der VCS-Datenbank stammen teilweise aus oeffentlich zugaenglichen Quellen (Beruf, Familienstatus — Selbstauskunft). Nur Schufa-Daten sind klar nicht allgemein zugaenglich. Argument: Fuer Teile der Daten fehlt das Tatbestandsmerkmal.

3.3 Prozessuale Massnahmen

Massnahme	Rechtsgrundlage	Zeitpunkt
Akteneinsicht	§ 147 StPO	Sofort (RA Dr. Ankermann)
Schweigrecht Beschuldigter	§ 136 StPO	Durchgehend
Antrag auf Aussetzung bei Vorfragen (DSGVO)	§ 262 StPO	Ggf. nach Anklageerhebung
Antrag auf Strafbefehl statt Hauptverhandlung	§ 407 StPO	Bei Gestaendnis-Strategie
Revision bei Verurteilung	§ 333 StPO	Falls erforderlich

4. Parallelverfahren und Selbstbelastungsfreiheit

4.1 Nemo-tenetur-Grundsatz

Der Beschuldigte Schimmelpfennig-Drosthager darf nicht gezwungen werden, sich im Aufsichtsverfahren (LDI NRW) oder im Zivilverfahren (VDuG) selbst zu belasten. Art. 6 EMRK, Art. 47 GRCh.

Massnahme: Saemtliche Erklaerungen gegenueber LDI NRW werden ausschliesslich durch RA Dr. Specht abgegeben, der saemtliche strafprozessual relevanten Informationen zurueckhaelt. Der Beschuldigte persoendlich gibt keine Erklaerungen im Verwaltungsverfahren ab.

4.2 Verwertungsverbot

Erklaerungen, die Schimmelpfennig-Drosthager gegenueber der LDI NRW ohne ordnungsgemaeße Belehrung nach § 136 StPO gemacht hat, koennen im Strafverfahren einem Verwertungsverbot unterliegen. Dies ist mit RA Dr. Ankermann zu klaeren.

5. Sanktionsprognose

Szenario	Strafe
Gestaendnis + Kooperation + Verbotsirrtum	Geldstrafe 90–120 Tagessaetze
Teilgestaendnis + Milderungsgruende	Bewaahrungsstrafe 1 Jahr auf Bewaehrung
Bestreiten + Verurteilung	Freiheitsstrafe 1–2 Jahre (Bewaehrung bei erstem Taeter)

Szenario	Strafe
Freispruch	Unklar — Beweislage ist gegen Angeklagten (IP-Logs)

Empfehlung: Haengt von forensischem Beweisstand ab. Nach Akteneinsicht detaillierte Bewertung.

6. Zivilrechtliche Absicherung

Fuer den Fall einer Verurteilung nach § 42 BDSG haftet VCS als Unternehmen zivilrechtlich fuer Schaeden der Mietinteressenten, die durch die persoenliche Nutzung des GF entstanden sind (§ 31 BGB — Vertreterhaftung). Diese Haftung laesst sich nicht auf den GF persoenlich abwaelzen, solange er im Rahmen seiner Organstellung handelte.

Quellen

- BDSG § 42 — dejure.org/gesetze/BDSG
- StGB § 17 (Verbotsirrtum) — dejure.org/gesetze/StGB
- StPO §§ 136, 147, 262, 407 — dejure.org/gesetze/StPO
- EMRK Art. 6 — dejure.org/gesetze/EMRK
- BGB § 31 — dejure.org/gesetze/BGB
- BGH, Urt. v. 20.02.2018 — 1 StR 436/17 (§ 42 BDSG alt) — [bundesgerichtshof.de](https://www.bundesgerichtshof.de)

Datei: 16_auftragsverarbeitung-avv-sundara-tech.md

16 — Auftragsverarbeitung: AVV Sundara Tech Pvt. Ltd.

Aktenzeichen: DSB-NW-44/26 (verbunden)

Bearbeiter: RA Lars Drosselberg, RAin Miriam Beckenbauer

Datum: 29. Januar 2026

Betreff: Analyse des AVV mit Sundara Tech und Sanierungsplan Auftragsverarbeitungsrecht

1. Rechtsrahmen Auftragsverarbeitung

1.1 Art. 28 DSGVO — Auftragsverarbeiter

Art. 28 Abs. 1 DSGVO: Wenn eine Verarbeitung im Auftrag eines Verantwortlichen erfolgt, arbeitet dieser nur mit Auftragsverarbeitern, die hinreichende Garantien dafuer bieten, dass geeignete technische und organisatorische Massnahmen so durchgefuehrt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt.

Art. 28 Abs. 3 DSGVO: Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments, der oder das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet.

Pflichtinhalte des AVV (Art. 28 Abs. 3 lit. a–h DSGVO):

- Bindung an Weisungen des Verantwortlichen
- Vertraulichkeitspflichten
- Geeignete technische und organisatorische Massnahmen (Art. 32 DSGVO)
- Regelung ueber Unterauftragsverarbeiter
- Unterstuetzung bei Betroffenenrechten
- Loeschung oder Rueckgabe nach Auftragsende
- Auskunft- und Kontrollrechte
- Nachweis der Konformitaet

2. Analyse des bestehenden AVV mit Sundara Tech

2.1 Zeitlinie des AVV-Abschlusses

Datum	Ereignis
Okt 2022	Beginn Datentransfer an Sundara Tech — **kein AVV**
Dez 2023	Abschluss eines AVV (nachtraeglich, auf Initiative von DSB Kessler-Brandt)
Jan 2026	Analyse AVV durch RA Drosselberg

Ergebnis: Fuer den Zeitraum Oktober 2022 bis Dezember 2023 (14 Monate) erfolgte die Verarbeitung durch Sundara Tech ohne AVV — klarer Verstoss gegen Art. 28 Abs. 3 DSGVO.

2.2 Maeengel des AVV (Dezember 2023)

Gemaess Analyse des AVV-Dokuments (Zugang erhalten 15.01.2026) bestehen folgende Maengel:

AVV-Klausel	Maengel	Bewertung
Art. 28 Abs. 3 lit. a (Weisungsbindung)	Nur allgemeine Weisungsbindung; keine Konkretisierung fuer Produktionsdaten	Unzureichend
Art. 28 Abs. 3 lit. b (Vertraulichkeit)	Vertraulichkeitspflicht vorhanden; aber kein Beendigungsprotokoll	Teilweise
Art. 28 Abs. 3 lit. c (TOM Art. 32)	Verweis auf ISO 27001, aber Sundara Tech nicht zertifiziert	Unzureichend
Art. 28 Abs. 3 lit. d (Unterauftragsverarbeiter)	Klausel fehlt — Sundara Tech nutzt AWS Mumbai (Drittland!)	Fehlt
Art. 28 Abs. 3 lit. e (Betroffenenrechte)	Kooperationspflicht vorhanden	Ausreichend
Art. 28 Abs. 3 lit. f (Loeschung)	Kein Loeschungsprotokoll; Fristen unklar	Unzureichend
Art. 28 Abs. 3 lit. g (Nachweise)	Auditrecht vorhanden, aber nie ausgeuebt	Formal ausreichend

AVV-Klausel	Maengel	Bewertung
Drittlandtransfer (Art. 46 DSGVO)	**SCC fehlt vollstaendig**	Fehlt vollstaendig

Gesamtergebnis: Der AVV ist in sechs von acht relevanten Bereichen unzureichend oder fehlerhaft. Ein vollstaendig sanierter AVV mit SCC ist zu erstellen.

3. Sanierungsplan AVV

3.1 Neuabschluss eines konformen AVV

Es wird empfohlen, den bestehenden AVV vollstaendig zu ersetzen durch:

Neuer AVV Sundara Tech v2.0 (Zieldokument):

1. Praezise Weisungsbindung fuer jeden Verarbeitungsschritt (ML-Training, Support-Zugriff, Entwicklung)
2. Vollstaendige Vertraulichkeitsverpflichtungen inklusive Beendigungsprotokoll
3. TOM-Anlage: Spezifische Sicherheitsanforderungen fuer Produktionsdaten (End-to-End-Verschluesselung, Zugangsbeschraenkung, Logging)
4. Unterauftragsverarbeiter-Regelung: Sundara Tech nutzt AWS Mumbai — eigene Unterauftragsverarbeitervertrag mit AWS India erforderlich
5. Betroffenenrechte-Prozess: Klarer Workflow fuer Weiterleitung von Auskunftersuchen und Loeschungsantraegen
6. Loeschungsprotokoll: Definierte Fristen und Nachweispflichten

Drittlandabsicherung:

7. SCC (Modul 2: Controller-to-Processor) gemaess EU-Kommissionsbeschluss 2021/914
8. Transfer Impact Assessment (TIA) Indien
9. Zusatzmassnahmen: Pseudonymisierung aller Trainings-Datensaetze vor Transfer

3.2 Zeitplan

Massnahme	Verantwortlich	Frist
Entwurf AVV v2.0	RA Drosselberg	10.02.2026
Abstimmung mit Sundara Tech	VCS Rechtsabteilung	20.02.2026
TIA Indien	extern: RA Mehta & Associates	28.02.2026
Unterzeichnung AVV v2.0 + SCC	GF VCS + Sundara Tech CEO	05.03.2026
Loeschungsbestaetigung alte Daten	Sundara Tech	10.03.2026

4. Haftung fuer Zeitraum ohne AVV (Okt 2022–Dez 2023)

4.1 Haftung VCS gegenueber Betroffenen

Fuer den Zeitraum ohne AVV haftet VCS als Verantwortlicher vollstaendig fuer alle Schaeden, die durch die Verarbeitung bei Sundara Tech entstanden sind. Art. 82 Abs. 2 DSGVO sieht eine verschuldensunabhaengige Haftung vor; VCS kann sich nur durch Nachweis entlasten, dass sie in keinerlei Hinsicht fuer den Schaden verantwortlich sind (Art. 82 Abs. 3 DSGVO) — was angesichts des fehlenden AVV nicht moeglich ist.

4.2 Regress gegen Sundara Tech

In dem Zeitraum ohne AVV ist Sundara Tech moeglicherweise als eigenverantwortlicher Verantwortlicher einzustufen (kein AVV = kein Weisungsverhaeltnis). Gesamtschuldnerische Haftung VCS + Sundara Tech gemaess Art. 82 Abs. 4 DSGVO ist moeglich. Der Regressanspruch VCS gegen Sundara Tech (Art. 82 Abs. 5 DSGVO) muss vertraglich gesichert werden.

Massnahme: Einbeziehung von Regressklausel in AVV v2.0 fuer den historischen Zeitraum.

5. Unterauftragsverarbeiter-Kette: AWS Mumbai

5.1 Problem

Sundara Tech betreibt seine Entwicklungsinfrastruktur auf AWS Mumbai (ap-south-1 Region). Damit ergibt sich eine weitere Drittlandsuebermittlung (Indien → AWS in Indien — kein EU-Bezug). Da AWS Inc. ein US-Unternehmen ist, koennte auch US-Recht (CLOUD Act) relevant werden.

5.2 Loesungsansatz

1. AWS Mumbai als Unterauftragsverarbeiter in den AVV aufnehmen
2. Pruefung: AWS Datenverarbeitungsnachtrag (AWS DPA) + AWS SCC — AWS stellt diese standardmaessig bereit
3. Sicherstellung: Keine Speicherung der Produktionsdaten ausserhalb der EU/EWR ohne explizite Genehmigung

Quellen

- DSGVO Art. 28, 32, 44, 46, 82 — dejure.org/gesetze/DSGVO
- EU-Kommissionsbeschluss 2021/914 (SCC Modul 2) — [eur-lex.europa.eu](https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32021D0914)
- EDSA-Leitlinien 07/2020 (Auftragsverarbeiter) — [edpb.europa.eu](https://edpb.europa.eu/our-work-tool/s/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_de)
- US CLOUD Act — [congress.gov](https://www.congress.gov/bill/115th-congress/senate-bill/2383/text)
- OLG Duesseldorf, Urt. v. 22.03.2022 — I-15 U 2/21 (Auftragsverarbeitungsvertrag) — openjur.de

Datei: 17_technisch-organisatorische-massnahmen-tom.md

17 — Technisch-Organisatorische Massnahmen (TOM) nach Art. 32 DSGVO

Aktenzeichen: DSB-NW-44/26

Bearbeiter: RAIN Miriam Beckenbauer, externer IT-Sicherheitsberater SecureProof GmbH

Datum: 30. Januar 2026

Betreff: Bewertung und Sanierung der TOM bei VermieterCheck Solutions GmbH

1. Rechtsrahmen Art. 32 DSGVO

Art. 32 Abs. 1 DSGVO verpflichtet den Verantwortlichen und den Auftragsverarbeiter, unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos geeignete technische und organisatorische Massnahmen zu treffen.

Regelbeispiele Art. 32 Abs. 1 DSGVO:

- lit. a: Pseudonymisierung und Verschlüsselung
- lit. b: Gewährleistung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit
- lit. c: Fähigkeit zur raschen Wiederherstellung nach Zwischenfällen
- lit. d: Regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit

2. Ist-Analyse der TOM bei VCS (Stand Oktober 2025)

2.1 Infrastruktur-Sicherheit

TOM-Bereich	Ist-Zustand	Bewertung
Datenverschlüsselung (at rest)	AWS S3-SSE (AES-256)	Ausreichend
Datenverschlüsselung (in transit)	TLS 1.2 (veraltet: TLS 1.3 Standard)	Unzureichend
Netzwerk-Segmentierung	VPC-Subnetz vorhanden, aber Staging = Produktion	Kritisch unzureichend
Zugangskontrolle	IAM-Rollen, aber GF-Account hat Admin-Vollzugriff	Mangelhaft
Patchmanagement	Keine standardisierte Patch-Strategie	Mangelhaft
SQL-Injection-Schutz	Fehlt (CVE-2026-0188)	Kritisch
Web Application Firewall	Nicht implementiert	Mangelhaft

2.2 Organisatorische Massnahmen

TOM-Bereich	Ist-Zustand	Bewertung
Datenschutzkonzept	Veraltet (2023, nicht aktuell)	Unzureichend
Schulungen Mitarbeiter	Letzte Schulung 2022	Mangelhaft
Incident-Response-Plan	Nicht vorhanden	Kritisch

TOM-Bereich	Ist-Zustand	Bewertung
Zutrittskontrolle Serverräume	Cloud (AWS) — kein physischer Server	Ausreichend
Datensicherung (Backup)	Täglich, 30 Tage Retention	Ausreichend
Loeschkonzept	Nicht dokumentiert	Mangelhaft
Datenschutz-Folgenabschätzung	Nicht durchgeführt (s. Akte 05)	Kritisch

2.3 Ergebnis Ist-Analyse

Von 14 geprüften TOM-Bereichen sind 4 als „Ausreichend“, 5 als „Mangelhaft“ und 5 als „Unzureichend/Kritisch“ bewertet. Dies entspricht einem erheblichen Sicherheitsdefizit, das die Datenpanne CVE-2026-0188 erst ermöglichte.

3. Soll-Konzept: Neue TOM nach Stand der Technik

3.1 Technische Massnahmen (Priorität HOCH)

Massnahme 1 — SQL-Injection-Abwehr:

- Implementierung Prepared Statements und Parametrisierung in allen Datenbankabfragen
- Einsatz einer Web Application Firewall (AWS WAF oder Cloudflare Enterprise)
- Input-Validierung für alle API-Endpoints
- Frist: 31.01.2026 (bereits eingeleitet, Patch für CVE-2026-0188 aktiv)

Massnahme 2 — TLS-Upgrade:

- Upgrade aller API-Verbindungen auf TLS 1.3
- Deaktivierung TLS 1.0 und TLS 1.1
- Zertifikatsspinning für kritische API-Verbindungen (Sundara Tech, Schufa-API)
- Frist: 15.02.2026

Massnahme 3 — Netzwerk-Segmentierung:

- Vollständige Trennung Staging- und Produktionsumgebung
- Keine Echtzeiten im Staging (nur synthetische Testdaten)
- Separates VPC für Produktionsdatenbank
- Frist: 28.02.2026

Massnahme 4 — Zugangskontrolle:

- Entzug Admin-Vollzugriff für GF-Account
- Least-Privilege-Prinzip für alle IAM-Rollen
- Multi-Faktor-Authentifizierung für alle Produktionszugänge
- Privileged Access Workstation (PAW) für Datenbankadministration
- Frist: 07.02.2026

Massnahme 5 — Pseudonymisierung:

- Pseudonymisierung aller Mietinteressenten-Daten vor Transfer an Sundara Tech
- Tokenisierung des ProspectScores (Score-Wert uebertragen, Name + Adresse bleiben in EU)
- Frist: 14.02.2026

3.2 Organisatorische Massnahmen (Prioritaet MITTEL)

Massnahme 6 — Incident-Response-Plan:

- Erstellung nach NIST Cybersecurity Framework und BSI IT-Grundschutz
- Rollen: CISO (Tarkan Bilgic), DSB (Kessler-Brandt), Kommunikationsverantwortlicher
- Meldekettten: 1h-Eskalation intern, 72h LDI NRW-Meldung
- Frist: 28.02.2026

Massnahme 7 — Schulungen:

- Jaehrliche DSGVO-Pflichtschulung fuer alle 38 Mitarbeiter
- Spezialschulung IT-Team zu Secure Coding und OWASP Top 10
- E-Learning-Plattform: TuVit (DSGVO-konform)
- Frist: 31.03.2026

Massnahme 8 — Loeschkonzept:

- Definition Loeschfristen pro Datenkategorie (Scoring-Daten: 24 Monate; Kontaktdaten: 36 Monate nach letzter Interaktion)
- Automatisiertes Loeschprotokoll mit Nachweis
- Frist: 15.02.2026

4. Gap-Analyse nach ISO 27001:2022

ISO-27001-Kontroll	Status	Prioritaet Sanierung
A 5.3 (Informationssicherheitsrollen)	Nicht vollstaendig	HOCH
A 5.24 (Informationssicherheitsvorfallsplanung)	Fehlt	KRITISCH
A 5.26 (Reaktion auf Sicherheitsvorfaelle)	Fehlt	KRITISCH
A 8.8 (Schwachstellen management)	Fehlt (CVE-2026-0188 zeigt dies)	KRITISCH
A 8.25 (Sichere Entwicklung)	Partiell	HOCH
A 8.9 (Konfigurationsmanagement)	Partiell	MITTEL

5. Dokumentation gegenüber LDI NRW

Im Rahmen des Aufsichtsverfahrens DSB-NW-44/26 wird VCS der LDI NRW bis zum 15.03.2026 folgende TOM-Nachweise uebergeben:

1. Aktualisiertes TOM-Dokument (Soll-Zustand nach Sanierung)
2. Penetrationstest-Bericht SecureProof GmbH (Neu-Test nach Sanierung)
3. Schulungsnachweise der Mitarbeiter
4. AVV-Nachweis mit Sundara Tech inkl. SCC
5. Nachweis Incident-Response-Plan-Implementierung

Quellen

- DSGVO Art. 32 — dejure.org/gesetze/DSGVO
- ISO/IEC 27001:2022 — [iso.org](https://www.iso.org/standard/82875.html)
- BSI IT-Grundschutz-Kompendium 2023 — [bsi.bund.de](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html)
- OWASP Top 10 (2021) — [owasp.org](https://owasp.org/www-project-top-ten)
- NIST Cybersecurity Framework 2.0 — [nist.gov](https://www.nist.gov/cyberframework)

Datei: 18_betroffenenrechte-widerspruch-loeschung.md

18 — Betroffenenrechte: Widerspruch und Loeschung

Aktenzeichen: DSB-NW-44/26 / 18 Mass 4/26

Bearbeiter: RAin Miriam Beckenbauer

Datum: 31. Januar 2026

Betreff: Systematische Bearbeitung von Widerspruchs- und Loeschungsantraegen

1. Betroffenenrechte im Ueberblick

Die DSGVO gewaehrt betroffenen Personen ein umfassendes Rechtssystem gegenueber Verantwortlichen:

Recht	Artikel	Status bei VCS
Auskunftsrecht	Art. 15	Nicht implementiert (s. Akten 12, 13)
Berichtigungsrecht	Art. 16	Nicht implementiert
Loeschrecht (Recht auf Vergessenwerden)	Art. 17	Nicht implementiert
Einschraenkung der Verarbeitung	Art. 18	Nicht implementiert

Recht	Artikel	Status bei VCS
Datenuebertragbarkeit	Art. 20	Nicht implementiert
Widerspruchsrecht	Art. 21	Nicht implementiert
Widerruf der Einwilligung	Art. 7 Abs. 3	Nicht implementiert

Alle sieben Betroffenenrechte sind bei VCS technisch und organisatorisch nicht implementiert — ein schwerwiegendes Compliance-Defizit.

2. Widerspruchsrecht Art. 21 DSGVO

2.1 Widerspruchsrecht bei berechtigtem Interesse (Art. 21 Abs. 1 DSGVO)

Hat VCS sich auf Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse) als Verarbeitungsgrundlage berufen, haben betroffene Personen das Recht, aus Gruenden, die sich aus ihrer besonderen Situation ergeben, jederzeit Widerspruch gegen diese Verarbeitung einzulegen.

Rechtsfolge: VCS muss nach Widerspruch die Verarbeitung einstellen, es sei denn, VCS kann zwingende schutzwuerdige Gruende nachweisen, die die Interessen der betroffenen Person ueberwiegen.

Praktische Situation: Da Art. 6 Abs. 1 lit. f DSGVO als Grundlage bereits als unzureichend bewertet wurde (s. Akte 03), waere ein Widerspruch ohnehin zurueckzuweisen — die Verarbeitung darf aus diesem Grunde gar nicht erfolgen.

2.2 Widerspruchsrecht bei Profiling (Art. 21 Abs. 2 DSGVO)

Werden personenbezogene Daten verarbeitet, um Direktwerbung zu betreiben oder Profiling fuer Direktwerbung durchzufuehren, so hat die betroffene Person das Recht, jederzeit Widerspruch einzulegen. Nach Widerspruch duermen die Daten fuer diese Zwecke nicht mehr verarbeitet werden.

Anwendbarkeit: Profiling durch ProspectScore Pro dient nicht der Direktwerbung, sondern der Mietinteressentenbeurteilung. Art. 21 Abs. 2 DSGVO nicht einschlaegig. Anwendbar ist Art. 21 Abs. 1 DSGVO.

3. Loeschrecht Art. 17 DSGVO

3.1 Loeschgruende

Loeschgrund	Art. 17 Abs. 1	Anwendbar bei VCS
Daten nicht mehr notwendig	lit. a	Nach Abschluss Bewerbung (wenn Vermieter Entscheidung getroffen hat) — Ja
Widerruf der Einwilligung	lit. b	Ja — wenn Einwilligung als Grundlage
Widerspruch Art. 21 Abs. 1	lit. c	Ja
Rechtswidrige Verarbeitung	lit. d	Ja — nach Feststellung des Art. 6-Verstosses
Rechtspflicht	lit. e	Ggf. bei gesetzl. Loeschpflicht

Ergebnis: Gemaess Art. 17 Abs. 1 lit. d DSGVO sind saemtliche unrechtmassig verarbeiteten Daten zu loeschen. Da die Verarbeitung ohne wirksame Rechtsgrundlage erfolgte, trifft VCS eine umfassende Loeschpflicht.

3.2 Ausnahmen vom Loeschrecht (Art. 17 Abs. 3 DSGVO)

Loeschung ist nicht verpflichtend, soweit die Verarbeitung erforderlich ist:

- zur Ausuebung des Rechts auf freie Meinungsaeusserung und Information (lit. a) — nicht einschlaegig
- zur Erfuellung einer rechtlichen Verpflichtung (lit. b) — moeglich fuer Aufbewahrungsfristen
- aus Gruenden des oeffentlichen Interesses (lit. c–d) — nicht einschlaegig
- fuer die Geltendmachung, Ausuebung oder Verteidigung von Rechtsanspruechen (lit. e) — einschlaegig fuer Verfahrensversicherung (Beweiszwecke im laufenden Verfahren)

Konsequenz: Im Rahmen der laufenden Verfahren (LDI NRW, VDuG, LG Essen, StA Essen) ist eine vollstaendige Loeschung bis zum Verfahrensabschluss nicht moeglich (Art. 17 Abs. 3 lit. e DSGVO — Rechtsansprueche). Die Daten sind jedoch einzuschaerken (Art. 18 DSGVO) — nur fuer Verfahrensverteidigung zugreifbar.

4. Datenuebertragbarkeit Art. 20 DSGVO

Art. 20 DSGVO gewaehrt betroffenen Personen das Recht, die sie betreffenden personenbezogenen Daten in einem strukturierten, gaengigen und maschinenlesbaren Format zu erhalten, wenn:

- die Verarbeitung auf Einwilligung (Art. 6 Abs. 1 lit. a) oder Vertrag (Art. 6 Abs. 1 lit. b) beruht, und
- die Verarbeitung mithilfe automatisierter Verfahren erfolgt.

Anwendbarkeit fuer VCS: Da die Einwilligung als unwirksam eingestuft wurde, ist Art. 20 DSGVO einschlaegig — aber die Verarbeitungsgrundlage war unwirksam. Ob Art. 20 DSGVO bei von Anfang an unwirksamer Einwilligung greift, ist rechtlich umstritten. Im Zweifel ist das Portabilitaetsrecht zu gewaehren.

5. Implementierungsplan Betroffenenrechte

5.1 Technische Implementierung (Zieldatum 28.02.2026)

Online-Portal „Meine Daten“ auf [vermietercheck.de](https://www.vermietercheck.de):

- Anmeldung per E-Mail-Verifizierung
- Auskunft: Anzeige aller gespeicherten Daten (ProspectScore, Datenkategorien, Empfaenger) — JSON-Export
- Widerspruch: One-Click-Widerspruchsformular mit Eingangsbestaetigung
- Loeschung: Antrag mit 30-Tage-Bearbeitung und Nachweisprotokoll
- Datenportabilitaet: Export als JSON/CSV nach Art. 20 DSGVO
- Widerruf Einwilligung: Dedizierter Button

5.2 Prozessimplementierung

- SLA: 1-Monat-Frist Art. 12 Abs. 3 DSGVO fuer Auskunft, Berichtigung, Loeschung
- Verlaengerungsprozess: Automatische E-Mail an Betroffenen bei Fristverlaengerung

- Ablehnung: Schriftliche Begründung mit Hinweis auf Beschwerderecht LDI NRW

6. Massenbearbeitung (VDuG-Kontext)

Im Rahmen des VDuG-Verfahrens (LG Essen 18 Mass 4/26) ist zu erwarten, dass 8.200 Kläger Löschanträge stellen. Die technische Kapazität für die Massенbearbeitung ist sicherzustellen:

- Batch-Löschfunktionalität in der Datenbank implementieren
- Löschdokumentation für jede betroffene Person (Zertifikat mit Datum und Datenreferenz)
- Kapazität: mindestens 500 Anträge/Woche bearbeitbar

Quellen

- DSGVO Art. 7, 12, 15, 16, 17, 18, 20, 21 —
dejure.org/gesetze/DSGVO
- EDSA-Leitlinien 05/2019 (Datenübertragbarkeit) — [edpb.europa.eu](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052019-right-data-portability_de)
- EuGH C-307/22 (Kopienrecht Art. 15 Abs. 3 DSGVO) —
[eur-lex.europa.eu](https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62022CJ0307)
- LG Frankfurt, Beschl. v. 18.09.2020 — 2-13 O 131/20 (Widerspruchsrecht Scoring) —
openjur.de

Datei: 19_iso27001-tisax-compliance-gap-analyse.md

19 — ISO 27001 / TISAX: Compliance-Gap-Analyse

Aktenzeichen: intern (Compliance-Akte)

Bearbeiter: Externe Beratung SecureProof GmbH (Bochum), koordiniert RA Drosselberg

Datum: 01. Februar 2026

Betreff: Gap-Analyse ISO 27001:2022 und TISAX für VCS im Kontext der Vorfälle

1. Ausgangssituation

VCS befindet sich in einem laufenden ISO-27001-Zertifizierungsprozess (Auditor: TuVit GmbH, Essen, Stage-2-Audit geplant April 2026). Durch die Vorfälle (CVE-2026-0188, Datenpanne, fehlende TOM) ist dieses Zertifizierungsprojekt gefährdet.

TISAX (Trusted Information Security Assessment Exchange) ist für VCS relevant, wenn Automobilindustrie-Kunden (Vermieter mit Kfz-Lease-Hintergrund) oder potenzielle Kooperationspartner eine TISAX-Bewertung fordern. Derzeit hat VCS keine TISAX-Anforderung — es wird jedoch als Qualitätsmerkmal für den Markt angestrebt.

2. ISO 27001:2022 — Gap-Analyse

2.1 Kontext der Organisation (Kapitel 4)

Anforderung	Status	Massnahme
4.1 Verstehen der Organisation	Partiell (SWOT vorhanden, aber veraltet)	Aktualisieren
4.2 Anforderungen interessierter Parteien	Fehlt (Kunden, Regulatoren nicht systematisch erfasst)	Erstellen
4.3 ISMS-Anwendungsbereich	Definiert (Cloud: AWS eu-central-1)	Ausreichend
4.4 ISMS und seine Prozesse	Unvollstaendig (keine vollstaendige Prozessdokumentation)	Ergaenzen

2.2 Fuehrung (Kapitel 5)

Anforderung	Status	Massnahme
5.1 Fuehrung und Verpflichtung	Nicht dokumentiert (GF hat DSFA ignoriert)	Sicherheitserklärung GF
5.2 Informationssicherheitspolitik	Vorhanden (2022)	Aktualisieren
5.3 Rollen und Verantwortlichkeiten	Partiell (kein CISO formell ernannt)	CISO-Ernennung

2.3 Unterstützung (Kapitel 7)

Anforderung	Status	Massnahme
7.2 Kompetenz	Schulungen nicht dokumentiert	Schulungsnachweise
7.3 Bewusstsein	Kein Awareness-Programm	Awareness-Kampagne
7.4 Kommunikation	Interne IS-Kommunikation fehlt	Policy-Kommunikation

2.4 Betrieb (Kapitel 8)

Anforderung	Status	Massnahme
8.1 Betriebsplanung	Partiell	Ergaenzen
8.2 Risikobeurteilung	Nicht jaehrlich durchgefuehrt	Jaehrlicher Zyklus
8.3 Risikobehandlung	Keine dokumentierten Massnahmen zu Risiken	Risikobehandlungsplan

2.5 Leistungsbewertung (Kapitel 9)

Anforderung	Status	Massnahme
9.1 Ueberwachung und Messung	Fehlt (kein KPI-System fuer IT-Sicherheit)	KPI-Set definieren
9.2 Internes Audit	Kein internes Audit durchgefuehrt	Audit-Programm
9.3 Managementbewertung	Fehlt	Jaehrliches Review

2.6 Annex A Kontrollen (Auswahl kritischer Luecken)

Kontrolle	Beschreibung	Status
A 5.23	Informationssicherheit fuer Cloud-Dienste	Partiell
A 5.24	Vorfallsmanagement-Planung	**Fehlt**
A 5.26	Reaktion auf Vorfaelle	**Fehlt** (CVE-2026-0188 zeigt dies)
A 5.30	IKT-Bereitschaft fuer Betriebskontinuitaet	Fehlt
A 8.8	Schwachstellenmanagement	**Fehlt** (SQL-Injection nicht erkannt)
A 8.25	Sicherheit im Entwicklungslebenszyklus	Partiell
A 8.29	Sicherheitstests in der Entwicklung	Unzureichend (kein SAST/DAST im CI/CD)

3. TISAX-Anforderungen (VDA ISA 6.0)

Fuer den Fall einer kuenftigen TISAX-Anforderung:

TISAX-Assessment-Ziel	Relevanz fuer VCS	Prueftiefe
Information Security (AL 2)	Hoch (Kundendaten in SaaS-Plattform)	Standard
Prototype Protection (AL 3)	Nicht einschlaegig	-
Data Protection	Hoch (DSGVO-Bezug)	Erweitert

Empfehlung: TISAX-Assessment erst nach vollstaendiger ISO-27001-Zertifizierung anstreben (Synergieeffekte). Zieldatum: Q1 2027.

4. Auswirkungen auf ISO-Zertifizierungsprojekt

4.1 Non-Conformities (Nicht-Konformitaeten)

Aus den identifizierten Luecken ergeben sich folgende Non-Conformities, die im Stage-2-Audit zur Feststellung oder sogar zur Versagung der Zertifizierung fuehren koennen:

Non-Conformity	Schwere	Zeitraumen Behebung
Kein Vorfallsmanagem entprozess (A 5.24, A 5.26)	Major NC	bis 15.03.2026
Kein Schwachstellenm anagement (A 8.8)	Major NC	bis 28.02.2026
Kein internes Audit	Major NC	bis 31.03.2026

Non-Conformity	Schwere	Zeitraumen Behebung
Schulungen nicht dokumentiert (7.2)	Minor NC	bis 15.03.2026
Kein CISO ernannt	Minor NC	bis 14.02.2026

4.2 Massnahmen zur Aufrechterhaltung des Zertifizierungsprojekts

1. **Sofort (bis 07.02.2026):** CISO-Ernennung (Tarkan Bilgic als interimistischer CISO)
2. **Kurzfristig (bis 28.02.2026):** Vorfallsmanagementprozess dokumentiert und implementiert
3. **Kurzfristig (bis 28.02.2026):** Schwachstellenscan und Patching-Policy
4. **Mittelfristig (bis 31.03.2026):** Internes Audit durchgefuehrt, Massnahmen dokumentiert

5. Bedeutung fuer Bussgeldverfahren (LDI NRW)

Der Nachweis einer ISO-27001-Zertifizierung (oder zumindest eines fortgeschrittenen Zertifizierungsprozesses) kann als Milderungsgrund im Bussgeldbescheidsverfahren wirken (Art. 83 Abs. 2 lit. j DSGVO: Einhaltung eines genehmigten Verhaltenskodex oder eines Zertifizierungsmechanismus).

Empfehlung: Einreichung eines Statusberichts ueber den ISO-27001-Prozess und die Non-Conformity-Behebung als Anlage zur Stellungnahme an LDI NRW.

Quellen

- ISO/IEC 27001:2022 — [iso.org](https://www.iso.org/standard/82875.html)
- VDA ISA 6.0 (TISAX-Anforderungskatalog) — [enx.com](https://www.enx.com/de-DE/TISAX)
- DSGVO Art. 32, 83 — dejure.org/gesetze/DSGVO
- BSI IT-Grundschutz — [bsi.bund.de](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html)
- OWASP ASVS 4.0 (Application Security Verification Standard) — [owasp.org](https://owasp.org/www-project-application-security-verification-standard)

Datei: 20_prozessstrategie-gesamtkoordination.md

20 — Prozessstrategie und Gesamtkoordination

Aktenzeichen: alle VCS-Aktenzeichen

Bearbeiter: RA Dr. Cornelius Specht (federfuehrend)

Datum: 03. Februar 2026

Betreff: Gesamtstrategie und Koordination saemtlicher Verfahren

1. Verfahrenslandkarte

Kommunikationskanal	Verantwortlich	Freigabe durch
Erklärungen LDI NRW	RA Dr. Specht	RA Dr. Specht
Schriftsätze LG Essen	RAin Beckenbauer	RA Dr. Specht
Strafverfahren StA Essen	RA Dr. Ankermann	RA Dr. Ankermann
Presseanfragen NDR/Buch	PR-Beratung (Mediator GmbH)	RA Dr. Specht
Auskunftsersuchen Betroffene	DSB Kessler-Brandt	RA Dr. Specht
Mitarbeiterkommunikation	GF (nach Freigabe)	RA Dr. Specht

3.3 Wechselwirkungen und Risiken

Massnahme A	Wechselwirkung	Risiko
Vollgeständnis bei LDI NRW	Stiftet Beweise für VDuG-Kläger	HOCH
Längeres Schweigen bei LDI NRW	Kein Kooperations-Milderungsgrund	HOCH
GF Aussage im Strafverfahren	Selbstbelastung im DSGVO-Verfahren	KRITISCH
Vergleich VDuG	Kann als Schuldanerkenntnis gewertet werden (Formulierung beachten)	MITTEL
NDR-Interview	Falsche Aussagen = neues Risiko	HOCH

4. PR-Kommunikationsstrategie

4.1 Medienumfeld

- NDR Panorama plant eine Sendung über KI-Profilierung im Mietmarkt (Felix Kaltenbach)
- Wibke Drostermann: Buch erscheint März 2026 bei Rowohlt
- Dr. Tannenbrück: Wissenschaftliche Veröffentlichung zur algorithmischen Diskriminierung geplant

4.2 Kommunikationsprinzipien

Prinzip 1 — Proaktive Transparenz mit Mass: Freiwillige Kommunikation über bereits eingeleitete Massnahmen, ohne Sachverhalte zu schaffen, die noch Gegenstand laufender Verfahren sind.

Prinzip 2 — Keine öffentliche Schuldanerkenntnis: Formulierungen wie „wir bedauern den Vorfall“ statt „wir erkennen den Vorstoß an“.

Prinzip 3 — Menschliches Gesicht: GF Schimmelpfennig-Drosthager kommuniziert persönlich (nach Freigabe) Sanierungsmaßnahmen. Kein Verstecken hinter Unternehmensprosa.

Prinzip 4 — Kein Angriff auf Journalisten/Betroffene: Keine öffentliche Auseinandersetzung mit Kaltenbach, Drostermann oder Tannenbrück.

4.3 Geplante PR-Massnahme (Zeitpunkt: nach Einreichung Stellungnahme LDI NRW)

Pressemitteilung: „VermieterCheck staerkt Datenschutz — Umfassende Compliance-Offensive eingeleitet“

- Massnahmen benennen (DSFA, SCC, Betroffenenportal)
- Keine konkreten Verfahrensaussagen
- Freigabe: RA Dr. Specht

5. Mandatsinterne Koordinationstreffen

Termin	Thema	Teilnehmer
05.02.2026	Gesamtstrategie-Review	SBD-Team + GF VCS + DSB
12.02.2026	DSFA-Status	RAin Beckenbauer + Kessler-Brandt
19.02.2026	Stellungnahme LDI NRW (Entwurf)	RA Dr. Specht + VCS-GF
26.02.2026	Klageerwiderung VDuG (Entwurf)	RAin Beckenbauer + VCS-GF
05.03.2026	StA-Koordination	RA Dr. Specht + RA Dr. Ankermann

6. Dokumentationspflichten

Im Rahmen der anwaltlichen Sorgfaltspflicht (§ 11 BORA) und fuer Regressabsicherung sind alle Beratungs- und Verfahrenshandlungen vollstaendig zu dokumentieren:

- Jedes Mandantengespraech: Protokoll (elektronisch, DSGVO-konform verschluesselt)
- Alle Fristen: Fristenkalender in DATEV Anwalt online
- Alle Schriftsaetze: Versionsverwaltung mit Git in der Kanzlei-IT
- Alle Korrespondenzen mit LDI NRW und Gerichten: Beglaubigte Kopien

Quellen

- DSGVO Art. 58, 83 — dejure.org/gesetze/DSGVO
- VDuG — dejure.org/gesetze/VDuG
- BDSG § 42 — dejure.org/gesetze/BDSG
- BORA § 11 (Dokumentationspflichten) — [brak.de](https://www.brak.de)
- VwGO §§ 42, 68, 80 — dejure.org/gesetze/VwGO

Datei: 21_verfassungsbeschwerde-skizze-bussgeldbescheid.md

21 — Verfassungsbeschwerde-Skizze gegen Bussgeldbescheid

Aktenzeichen: DSB-NW-44/26 (Voraussetzung: Erschoepfung des Rechtswegs)

Bearbeiter: RA Dr. Cornelius Specht

Datum: 05. Februar 2026

Betreff: Verfassungsrechtliche Prüfung eines möglichen Bussgeldbescheids der LDI NRW

1. Vorbemerkung

Die vorliegende Skizze prüft prospektiv, ob und unter welchen Voraussetzungen gegen einen Bussgeldbescheid der LDI NRW (DSB-NW-44/26) eine Verfassungsbeschwerde nach Art. 93 Abs. 1 Nr. 4a GG i.V.m. §§ 90 ff. BVerfGG zulässig und begründet wäre. Die Skizze setzt voraus, dass der Rechtsweg (Widerspruch, VG Duesseldorf, OVG NRW, BVerwG) erschöpft ist (§ 90 Abs. 2 BVerfGG).

Wichtiger Hinweis: Diese Verfassungsbeschwerde ist ein ultima-ratio-Mittel. Die Kanzlei SBD empfiehlt primaer eine aussergerichtliche Einigung mit LDI NRW oder einen Vergleich auf Widerspruchsebene.

2. Zulässigkeitsvoraussetzungen

2.1 Beschwerdefähigkeit (§ 90 Abs. 1 BVerfGG)

Eine Verfassungsbeschwerde können jede Person geltend machen, die behauptet, durch die öffentliche Gewalt in einem Grundrecht verletzt zu sein. Juristische Personen des Privatrechts sind beschwerdebefugt, soweit Grundrechte ihrem Wesen nach auf diese anwendbar sind (Art. 19 Abs. 3 GG).

VCS ist beschwerdefähig hinsichtlich:

- Art. 12 Abs. 1 GG (Berufsfreiheit) — wirtschaftliche Existenz
- Art. 14 Abs. 1 GG (Eigentumsgarantie) — Vermögenspositionen
- Art. 2 Abs. 1 GG i.V.m. Art. 19 Abs. 3 GG (allgemeine Handlungsfreiheit)
- Art. 103 Abs. 2 GG (Bestimmtheitsgrundsatz bei Sanktionen)

2.2 Beschwerdegegenstand

Gegenstand: Hoheitlicher Bussgeldbescheid der LDI NRW als Massnahme öffentlicher Gewalt.

2.3 Beschwerdebefugnis

VCS muss mögliche und gegenwärtige Grundrechtsverletzung behaupten. Bei einem existenzgefährdenden Bussgeld ist dies bei einem Jahresumsatz von 4 Mio. EUR ohne weiteres darzulegen.

2.4 Rechtswegerschöpfung (§ 90 Abs. 2 BVerfGG)

Erschöpfung erfordert:

1. Widerspruch gegen Bussgeldbescheid bei LDI NRW (§ 68 VwGO)
2. Klage vor VG Duesseldorf (§ 42 VwGO)
3. Berufung vor OVG NRW (§ 124 VwGO)
4. Revision vor BVerwG (§ 132 VwGO) — soweit zugelassen

3. Begründetheit: Potenzielle Grundrechtsverletzungen

3.1 Art. 12 Abs. 1 GG — Verletzung der Berufsfreiheit

Argument: Art. 12 Abs. 1 GG schützt die Berufsausübung gegenüber staatlichen Einschränkungen. Ein Bussgeld, das die wirtschaftliche Existenz des Unternehmens gefährdet oder vernichtet, stellt einen

Eingriff in die Berufsfreiheit dar, der einer Verhältnismässigkeitsprüfung standhalten muss.

Dreistufentest (BVerfGE 7, 377 — Apotheken-Urteil):

- Stufe 1 — Berufsausübungsregeln: Bussgeld als Reaktion auf Berufsausübung — Eingriff auf Stufe 1
- Gerechtfertigt durch: Vernünftige Erwägungen des Allgemeinwohls (Datenschutz)
- Verhältnismässigkeit: Ein Bussgeld von 20 Mio. EUR bei einem Jahresumsatz von 4 Mio. EUR ist offensichtlich unverhältnismässig

Argument: Bei Art. 83 DSGVO ist der prozentuale Umsatzanteil (4%) die verfassungsrechtlich gebotene Berechnungsregel für KMU, nicht der absolute Höchstbetrag von 20 Mio. EUR. Eine Anwendung des absoluten Höchstbetrags auf ein KMU ohne spezifische Begründung verletzt Art. 12 GG.

3.2 Art. 103 Abs. 2 GG — Nulla poena sine lege certa

Argument: Art. 103 Abs. 2 GG verlangt hinreichende Bestimmtheit der Bussgeldsanktionen. Art. 83 DSGVO ermächtigt die Behörde zu einem weiten Ermessen (0 bis 20 Mio. EUR oder 0 bis 4%). Dieses weite Ermessen kann — ohne ausdrückliche Gesetzgebungsakt des deutschen Parlaments — verfassungsrechtlich bedenklich sein.

Gegenargument (LDI NRW): Art. 83 DSGVO ist unmittelbar geltendes EU-Recht (EUV Art. 288). Nationale Grundrechte werden durch das Grundgesetz-Konzept des Anwendungsvorrangs des EU-Rechts (Solange-Rechtsprechung, BVerfGE 73, 339) eingeschränkt.

Erwiderung VCS: Die Solange-Doktrin gilt nicht schrankenlos. BVerfG hat in BVerfGE 126, 286 (Honeywell) und BVerfG 2 BvR 1685/14 (PSPP-Urteil) bestätigt, dass ultra-vires-Handlungen und Verletzung des verfassungsidentitären Kerns prüfbar bleiben. Ein Bussgeld, das ein Unternehmen vernichtet, ohne individuellen Vorsatz, tangt als ultra-vires.

3.3 Art. 14 Abs. 1 GG — Eigentumsgarantie

Argument: Das Unternehmensvermögen und eingerichtete Gewerbebetrieb sind durch Art. 14 GG geschützt. Ein vernichtend hohes Bussgeld, das die Überschuldung oder Insolvenz bewirkt, stellt eine unverhältnismässige Inhalts- und Schrankenbestimmung dar (BVerfGE 100, 226 — Denkmalschutz).

3.4 Unionsrechtliche Dimension: Verhältnismässigkeit (Art. 49 GRCh)

Art. 49 Abs. 3 GRCh: Das Mass der Strafe muss zur Straftat in einem angemessenen Verhältnis stehen. Der EuGH hat in C-807/21 (Deutsche Wohnen) die Verhältnismässigkeitsprüfung bei DSGVO-Bussgeldern bestätigt. Ein nationales Gericht (VG Duesseldorf) kann/muss den EuGH um Vorabentscheidung ersuchen, falls Verhältnismässigkeitsfragen unklar sind (Art. 267 AEUV).

4. Prozessuale Strategie

4.1 Primaer: Vorabentscheidungsersuchen EuGH

Beim VG Duesseldorf (oder OVG NRW) wird ein Vorabentscheidungsersuchen gemäss Art. 267 AEUV angestrebt, um folgende Fragen klären zu lassen:

- Darf Art. 83 DSGVO so ausgelegt werden, dass der absolute Betrag (20 Mio. EUR) auch bei KMU mit sehr viel niedrigerem Jahresumsatz angewendet wird?
- Ist bei fehlender Absicht und vollständiger Kooperation ein Bussgeld nahe des Maximalbetrags verhältnismässig (Art. 49 GRCh)?

4.2 Sekundaer: Verfassungsbeschwerde BVerfG

Sollte der EuGH-Weg nicht zum Erfolg führen, wird Verfassungsbeschwerde eingelegt mit dem Antrag:

- Den Bussgeldbescheid und die bestaetigenden Gerichtsentscheidungen aufzuheben
- Festzustellen, dass Art. 83 Abs. 5 DSGVO in seiner Anwendung auf KMU ohne individuelle Verhaeltnismaessigkeitspruefung Art. 12, 14 GG verletzt

5. Erfolgsaussichten

Rechtsbehelf	Erfolgswahrscheinlichkeit	Anmerkung
Widerspruch + VG Duesseldorf	30–40% (Reduzierung Bussgeld)	Realistisches Ziel
OVG / BVerwG (Revision)	15–25% (Grundsatzliche Kl rung)	Langwierig
Vorabentscheidung EuGH	20–30% (Guenstiges Urteil)	Zeitaufwendig
Verfassungsbeschwerde BVerfG	5–10% (Zulassung)	Ultima ratio

Quellen

- GG Art. 12, 14, 19, 103 — dejure.org/gesetze/GG
- BVerfGG §§ 90 ff. — dejure.org/gesetze/BVerfGG
- BVerfGE 7, 377 (Apotheken-Urteil) —
[bundesverfassungsgericht.de](https://www.bundesverfassungsgericht.de)
- BVerfGE 73, 339 (Solange II) —
[bundesverfassungsgericht.de](https://www.bundesverfassungsgericht.de)
- EuGH C-807/21 (Deutsche Wohnen) —
[eur-lex.europa.eu](https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62021CJ0807)
- GRCh Art. 49 —
[eur-lex.europa.eu](https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:12012P/TXT)
- AEUV Art. 267 —
[eur-lex.europa.eu](https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:12016E267)

Datei: 22_abschlussbericht-handlungsempfehlungen.md

22 — Abschlussbericht und Handlungsempfehlungen

Aktenzeichen: alle VCS-Aktenzeichen

Bearbeiter: RA Dr. Cornelius Specht (federfuehrend)

Datum: 07. Februar 2026

Betreff: Gesamtabschluss Erstanalyse und Handlungsempfehlungen

1. Zusammenfassung der Ausgangslage

Die VermieterCheck Solutions GmbH (VCS) sieht sich einer beispiellosen datenschutzrechtlichen Krisensituation gegenüber, die in ihrer Kumulation juristisch als existenzbedrohend einzustufen ist:

Verfahrens-/Risikokomplex	Finanzielles Risiko	Rechtsnatur
Bussgeldbescheid LDI NRW Art. 83 DSGVO	bis 20.000.000 EUR	Verwaltungsrecht
VDuG-Sammelklage 8.200 Betroffene	12.300.000 EUR	Zivilrecht
Strafverfahren GF § 42 BDSG	Freiheitsstrafe bis 3 Jahre	Strafrecht
Einzelklage Tannenbruck	1.500 EUR zzgl. Kosten	Zivilrecht
Reputationsschaden (NDR, Buch)	Unquantifiziert	Geschaeflich
Gesamtexposure (theoretisch)	**> 32.000.000 EUR**	

Das tatsächliche Exposure nach erfolgreicher Verteidigung wird auf 1.000.000 bis 5.000.000 EUR geschätzt (s. Bussgeldbemessung Akte 09, Vergleichsstrategie VDuG Akte 11).

2. Rechtliche Bewertungen — Kernbefunde

2.1 Klare Rechtsverstoesse (nicht bestreitbar)

1. **Art. 6 DSGVO:** Verarbeitung ohne wirksame Rechtsgrundlage — Einwilligung durch Koppelung und Unvollstaendigkeit unwirksam (s. Akte 03)
2. **Art. 22 DSGVO:** Unzulaessige automatisierte Einzelentscheidung — HITL fehlt, Ausnahmen nicht erfüllt (s. Akte 04)
3. **Art. 35 DSGVO:** DSFA nicht durchgefuehrt trotz offensichtlicher Pflicht (s. Akte 05)
4. **Art. 44 ff. DSGVO:** Drittlandtransfer an Sundara Tech ohne SCC (s. Akte 06)
5. **Art. 33 DSGVO:** 72h-Meldepflicht versaeumt (s. Akte 07)
6. **Art. 28 DSGVO:** AVV mit Sundara Tech fuer 14 Monate nicht vorhanden; bestehendes AVV mangelhaft (s. Akte 16)

2.2 Verteidigungspositionen (bestrittig)

1. **Bussgeldbemessung Art. 83:** Verhaeltnismaessigkeitspruefung — KMU-Abschlag, keine Absicht, Kooperation (s. Akte 09)
2. **Art. 82 Bagatellgrenze:** Kein tatsaechlicher Schaden fuer Segmente C und D (s. Akte 11)
3. **§ 42 BDSG Vorsatz:** Verbotsirrtum, fehlende Bereicherungsabsicht (s. Akte 15)
4. **Art. 83 GRCh / VfB:** Verhaeltnismaessigkeitspruefung auf EU-/Verfassungsebene (s. Akte 21)

3. Priorisierte Handlungsempfehlungen

Sofortmassnahmen (bis 15.02.2026)

Prioritaet KRITISCH:

1. **Datenpanne-Meldung nacholen (Art. 33 DSGVO):** Sofortiger Eingang der Meldung bei LDI NRW mit vollstaendiger Schadensdarstellung. Jeder weitere Tag des Versaeumnisses verschlimmert die Bussgeldbemessung.

- Verantwortlich: RA Dr. Specht - Frist: 10.02.2026

2. **Auskunft Dr. Tannenbruck erteilen:** Fristerstreckung bei LG Essen beantragen und Auskunft innerhalb von 7 Tagen erteilen.

- Verantwortlich: RAin Beckenbauer + DSB Kessler-Brandt - Frist: 12.02.2026

3. **Datentransfer Sundara Tech stoppen:** Kein weiterer Datentransfer bis SCC unterzeichnet.

- Verantwortlich: DevOps-Leiter Bilgic - Frist: Sofort (bereits angeordnet 14.01.2026)

4. **Patching CVE-2026-0188:** Produktiver Patch live und verifiziert durch SecureProof.

- Verantwortlich: DevOps-Team - Frist: Bereits eingespielt (24.11.2025); Verifikation 10.02.2026

5. **Betroffenenbenachrichtigung Art. 34 DSGVO:** Brief und E-Mail an 142.300 betroffene Mietinteressenten mit Information ueber Datenpanne.

- Verantwortlich: DSB Kessler-Brandt + externe Kommunikationsagentur - Frist: 15.02.2026

Kurzfristige Massnahmen (bis 28.02.2026)

6. **DSFA fertigstellen (Art. 35 DSGVO):** Vollstaendige DSFA-Dokumentation fuer ProspectScore Pro, anschliessend Vorabkonsultation LDI NRW (Art. 36 DSGVO).

7. **Auskunftersuchen Drostermann und Kaltenbach beantworten (Art. 15 DSGVO, Fristen 03.02. und 05.02.2026).**

8. **SCC mit Sundara Tech abschliessen:** Modul 2 Controller-to-Processor, inklusive TIA.

9. **Stellungnahme LDI NRW einreichen:** Vollstaendige kooperative Stellungnahme zu DSB-NW-44/26 mit Sanierungsnachweis.

Mittelfristige Massnahmen (bis 31.03.2026)

10. **HITL-Implementierung:** Human-in-the-Loop fuer ProspectScore Pro, Testphase und Dokumentation.

11. **Betroffenenportal:** Online-Portal fuer Auskunft, Widerspruch, Loeschung, Datenportabilitaet.

12. **Klageerwiderung VDuG:** Schriftsatz LG Essen 18 Mass 4/26 mit vollstaendiger Verteidigungsstrategie und Vergleichsangebot.

13. **Schulungen:** Alle 38 Mitarbeiter DSGVO-Pflichtschulung, IT-Team Secure-Coding.

14. **Loeschkonzept implementieren:** Automatisiertes Loeschprotokoll fuer alle Datenkategorien.

4. Kostenprognose Rechtsvertretung

Leistung	Geschaetzte Kosten (netto)
Verwaltungsverfahren LDI NRW	45.000 – 60.000 EUR
Zivilverfahren VDuG + Tannenbruck	80.000 – 120.000 EUR

Leistung	Geschaetzte Kosten (netto)
Strafverfahren (RA Dr. Ankermann)	40.000 – 70.000 EUR
Beratung (DSFA, TOM, SCC)	30.000 – 50.000 EUR
Externe Gutachter/Forensik	25.000 – 40.000 EUR
Gesamt Rechtsvertretungskosten	**220.000 – 340.000 EUR**

Der geleistete Kostenvorschuss von 85.000 EUR deckt die ersten 3-4 Monate ab. Eine Nachschussanforderung ist fuer April 2026 geplant.

5. Abschliessende Prognose

Bei konsequenter Umsetzung der Sofort- und Kurzfristmassnahmen und kooperativer Haltung gegenueber LDI NRW ist folgendes Szenario realistisch:

- **Bussgeld LDI NRW:** 300.000 – 800.000 EUR (statt 20 Mio. EUR Maximum)
- **VDuG-Vergleich:** 400.000 – 700.000 EUR (statt 12.3 Mio. EUR Klageforderung)
- **Strafverfahren GF:** Geldstrafe oder Bewaehrungsstrafe (kein Haftantritt)
- **Reputationsschaden:** Begrenzbar durch PR-Offensive und sichtbare Compliance-Massnahmen

Gesamtaussicht: Unternehmenserhalt bei konsequenter Compliance-Offensive wahrscheinlich. Die Kanzlei SBD ist zuversichtlich, die Mandantin durch die Krise zu fuehren.

6. Sorgfaltspflicht-Hinweis

Dieser Abschlussbericht stellt eine erste Gesamtbewertung des Sachverhalts dar, basierend auf den im Zeitraum 14.-31.01.2026 erhobenen Informationen. Er ersetzt keine spezifische Einzelberatung zu den einzelnen Verfahren (s. Akten 01–21). Die Einschaeztungen koennen sich aufgrund neuer Tatsachen oder veraendeter Rechtslage jederzeit aendern.

Quellen

- DSGVO Art. 6, 22, 28, 33, 34, 35, 44, 82, 83 — [\[dejure.org/gesetze/DSGVO\]](https://dejure.org/gesetze/DSGVO)(<https://dejure.org/gesetze/DSGVO>)
- BDSG § 42 — [\[dejure.org/gesetze/BDSG\]](https://dejure.org/gesetze/BDSG)(<https://dejure.org/gesetze/BDSG>)
- VDuG — [\[dejure.org/gesetze/VDuG\]](https://dejure.org/gesetze/VDuG)(<https://dejure.org/gesetze/VDuG>)
- EuGH C-807/21 (Deutsche Wohnen) — [\[eur-lex.europa.eu\]](https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62021CJ0807)(<https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62021CJ0807>)
- BGH VI ZR 10/24 — [\[bundesgerichtshof.de\]](https://www.bundesgerichtshof.de)(<https://www.bundesgerichtshof.de>)
- EDSA-Leitlinien 04/2022 (Bussgeldbemessung) — [\[edpb.europa.eu\]](https://edpb.europa.eu/our-work-to-ols/our-documents/guidelines/guidelines-042022-calculation-administrative-fines-under-gdpr_de)(https://edpb.europa.eu/our-work-to-ols/our-documents/guidelines/guidelines-042022-calculation-administrative-fines-under-gdpr_de)

E-Mails

Datei: eml/01_datenpannenmeldung_art33_ldi_nrw.eml

Von	dr.specht@specht-beckenbauer-drosselberg.de
An	poststelle@ldi.nrw.de
Datum	Tue, 10 Feb 2026 09:15:00 +0100
Betreff	AZ DSB-NW-44/26 - Nachholung Datenpannenmeldung gemaess Art. 33 DSGVO - VermieterCheck Solutions GmbH

Landesbeauftragte fuer Datenschutz und Informationsfreiheit NRW (LDI NRW)

z.H. Sachbearbeitung Aufsichtsverfahren DSB-NW-44/26

Kavalleriestrasse 2-4

40213 Duesseldorf

Sehr geehrte Damen und Herren,

wir sind als Bevollmaechtigte der VermieterCheck Solutions GmbH (Ruhrallee 188, 45136 Essen, GF Karl-Heinz Schimmelpfennig-Drosthager) mandatiert und nehmen Bezug auf das laufende Aufsichtsverfahren DSB-NW-44/26.

NACHHOLUNG DATENPANNENMELDUNG GEMAESS ART. 33 ABS. 1 DSGVO

Wir zeigen hiermit pflichtgemaess die nachfolgende Datenschutzverletzung an und begruenden die Verspaetung der Meldung gemaess Art. 33 Abs. 1 Satz 2 DSGVO.

1. DATENPANNENBESCHREIBUNG (Art. 33 Abs. 3 DSGVO)

a) Art der Datenschutzverletzung:

SQL-Injection-basierte unbefugte Exfiltration personenbezogener Daten durch einen externen Akteur. Die Schwachstelle CVE-2026-0188 (CVSS v3.1: 9.8) im REST-API-Endpoint /api/v3/prospect/search des Backends von ProspectScore Pro (Version 3.0.4) ermoeeglichte eine ungeprueft parametrisierte Datenbankabfrage.

b) Datenkategorien und Datensatze:

- Betroffene Datensatze: 142.300 Mietinteressenten-Profile
- Kategorien: Name, Adresse, E-Mail, Schufa-Score, Negativmerkmale, Beruf, Einkommen (Selbstauskunft), Familienstatus, ProspectScore (0-100)
- Sensitivitaet: Hoch (Bonitaetsdaten, finanzielle Informationen)

c) Betroffene Personengruppen:

Mietinteressenten, die in der Zeit von Maerz 2023 bis November 2025 ueber die VermieterCheck-Plattform gescreent wurden.

d) Ungefaehre Anzahl betroffener Personen: 142.300

e) Wahrscheinliche Folgen:

Identitaetsdiebstahl, Phishing-Angriffe unter Verwendung echter Bonitaetsdaten, Kreditschaeden durch Missbrauch der Negativmerkmale, psychische Belastung der Betroffenen durch Kontrollverlust ueber Finanzdaten.

f) Ergriffene Massnahmen:

- Patch CVE-2026-0188 eingespielt am 24.11.2025 (DevOps-Team)
- API-Endpoint vorlaeufig deaktiviert

- Beauftragung forensische Analyse: SecureProof GmbH, Bochum (Bericht Nr. SP-2025-4417)
- Betroffenenbenachrichtigung gemaess Art. 34 DSGVO: Versand 15.02.2026
- Datenbankzugang eingeschaermt (MFA fuer alle Zugangskonten ab 07.02.2026)

g) Name und Kontaktdaten des Datenschutzbeauftragten:

Hannelore Kessler-Brandt, DSB VermieterCheck Solutions GmbH
dsb@vermietercheck.de | Tel. 0201/498820-15

2. BEGRUENDUNG DER VERSPAETUNG

Die 72-Stunden-Frist des Art. 33 Abs. 1 DSGVO begann mit Kenntniserlangung am 24.11.2025 (Eingang GuardDuty-Alert beim DevOps-Leiter, Weiterleitung an GF am selben Tag).

Die Unterlassung der fristgemaessen Meldung resultiert aus einem internen Kommunikationsversagen: Der GF wurde zwar informiert, traf jedoch keine Anordnung zur Meldung an die LDI NRW. Der Datenschutzbeauftragte wurde nicht eingeschaltet. Dies stellt ein ernstes Organisationsversagen dar, das die Mandantin bedauert und das Gegenstand interner Massnahmen ist.

Mit der Mandatsuebernahme durch unsere Kanzlei am 14.01.2026 wurde die Nachholung der Meldung unverzueglich eingeleitet.

3. BEIGEFUEGTE ANLAGEN

- Penetrationstest-Bericht SecureProof GmbH (Auszug, redacted) SP-2025-4417
- AWS GuardDuty-Alert-Protokoll (anonymisiert)
- Forensik-Timeline CVE-2026-0188
- Entwurf Betroffenenbenachrichtigung Art. 34 DSGVO

Wir stehen fuer Rueckfragen und eine muendliche Erlaeuterung jederzeit zur Verfuegung.

Mit freundlichen Gruessen

Dr. Cornelius Specht

Rechtsanwalt | Fachanwalt fuer Datenschutzrecht

Specht, Beckenbauer & Drosselberg Rechtsanwaltsgesellschaft mbH

Koenigsallee 92c | 40212 Duesseldorf

Tel. 0211/49320-10 | Fax 0211/49320-99

dr.specht@specht-beckenbauer-drosselberg.de

Quellen: DSGVO Art. 33 - <https://dejure.org/gesetze/DSGVO> | EDSA-Leitlinien 01/2021

(Datenpannenmeldung) - https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012-021-examples-regarding-personal-data-breach_de

Datei: eml/02_datentransfer_stop_scc_aufforderung_sundara_tech.eml

Von	I.drosselberg@specht-beckenbauer-drosselberg.de
An	legal@sundaratech.in
Datum	Fri, 16 Jan 2026 14:30:00 +0100
Betreff	URGENT - Data Transfer Suspension & SCC Execution Requirement - VermieterCheck Solutions GmbH / Sundara Tech Pvt. Ltd.

Sundara Tech Pvt. Ltd.

Attn.: Legal Department / CEO

No. 42, 4th Floor, Prestige Tech Park

Sarjapur Road, Bengaluru, Karnataka 560103

India

Dear Sir or Madam,

We act as legal counsel for VermieterCheck Solutions GmbH (Germany, hereinafter "VCS") in all data protection matters. We write to you with immediate urgency regarding the data processing activities conducted by Sundara Tech Pvt. Ltd. (hereinafter "Sundara Tech") on behalf of VCS.

1. IMMEDIATE SUSPENSION OF PERSONAL DATA TRANSFERS

With immediate effect from the date of this letter (16 January 2026), VCS hereby instructs Sundara Tech to:

- (a) Immediately cease any processing of personal data received from VCS, including but not limited to: tenant applicant profiles, credit scoring data, ProspectScore training datasets, and any production database content.
- (b) Immediately cease any transfer of such data to third parties, subprocessors, or cloud infrastructure outside the European Economic Area.
- (c) Secure all data currently in your possession and access-restrict it to authorized VCS personnel only.

This instruction is issued pursuant to Clause 7.7 of the Data Processing Agreement (DPA) dated December 2023 and Art. 28 Abs. 3 lit. a DSGVO (GDPR).

2. LEGAL BACKGROUND

VCS has determined that the data transfers to Sundara Tech conducted since October 2022 were carried out without Standard Contractual Clauses (SCCs) as required under Art. 46 Abs. 2 lit. c GDPR and EU Commission Decision 2021/914. The absence of SCCs constitutes a serious violation of Chapter V GDPR, which VCS is in the process of remedying.

Furthermore, a data breach (CVE-2026-0188) affecting 142,300 data subjects has been identified, and the forensic analysis must determine whether Sundara Tech's infrastructure was involved.

3. REQUEST FOR EXECUTION OF STANDARD CONTRACTUAL CLAUSES

VCS requests that Sundara Tech execute Standard Contractual Clauses (Module 2: Controller to Processor) pursuant to EU Commission Decision 2021/914 of 4 June 2021. Our team will provide the completed SCC document by 20 February 2026. We request Sundara Tech's countersignature by 5 March 2026 at the latest.

4. DATA DELETION REQUEST

Please confirm in writing by 31 January 2026 that all VCS production data and training datasets stored on Sundara Tech's systems (including staging environments, backups, and AWS Mumbai instances) have been securely deleted, with a deletion log provided as evidence.

5. TRANSFER IMPACT ASSESSMENT (TIA)

Pursuant to the guidance of the European Data Protection Board (EDPB Recommendations 01/2020) and the Schrems II ruling (CJEU C-311/18), a Transfer Impact Assessment for India must be completed. We will engage Indian counsel (Mehta & Associates, Mumbai) and request Sundara Tech's cooperation in providing information about applicable Indian law.

Please acknowledge receipt of this letter within 48 hours and confirm compliance.

Yours faithfully,

Lars Drosselberg, Rechtsanwalt
Dr. Cornelius Specht, Rechtsanwalt (Fachanwalt Datenschutzrecht)
Specht, Beckenbauer & Drosselberg Rechtsanwaltsgesellschaft mbH
Koenigsallee 92c | D-40212 Duesseldorf | Germany
Tel. +49 211 49320-0 | Fax +49 211 49320-99
l.drosselberg@specht-beckenbauer-drosselberg.de

Sources: GDPR Art. 44, 46 - <https://dejure.org/gesetze/DSGVO> | EU Commission Decision 2021/914 (SCC) - <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=LEX:32021D0914> | CJEU C-311/18 (Schrems II) - <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=LEX:62018CJ0311> | EDPB Recommendations 01/2020 - https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_de

Datei: eml/03_hinschg_meldung_interne_meldestelle_reaktion.eml

Von	meldestelle@vermietercheck.de
An	anonym-whistleblowing-portal@speakout-service.de
Datum	Mon, 26 Jan 2026 11:00:00 +0100
Betreff	Eingangsbestaetigung und Massnahmenankuendigung - Meldung vom 08.11.2025 (anonyme Meldung)

Bitte weiterleiten an: Anonyme Hinweisgeber-ID SPEAKOUT-VCS-2025-0047

--

EINGANGSBESTAETIGUNG UND RUECKMELDUNG gemaess § 17 Abs. 2 Hinweisgeberschutzgesetz (HinSchG)

Sehr geehrte/r Hinweisgeber/in,

wir bestaetigen den Eingang Ihrer anonymen Meldung vom 08. November 2025 ueber das interne Hinweisgebersystem der VermieterCheck Solutions GmbH (Meldungs-ID: SPEAKOUT-VCS-2025-0047).

Wir moechten uns zunaechst fuer die versaetete Rueckmeldung entschuldigen. Die dreimonatige Frist des § 17 Abs. 2 HinSchG wurde leider nicht eingehalten, was auf ein internes Kommunikationsversagen zurueckzufuehren ist. Wir bedauern dies und haben entsprechende Korrekturen in unseren internen Prozessen vorgenommen.

INHALT IHRER MELDUNG (ZUSAMMENFASSUNG)

Ihre Meldung bezog sich auf die Datenuebermittlung von Mietinteressenten-Daten an die Firma Sundara Tech Pvt. Ltd. (Bengaluru, Indien) ohne Standarddatenschutzklauseln genaess Art. 46 DSGVO sowie das Fehlen eines ordnungsgemaessen Auftragsverarbeitungsvertrags fuer den Zeitraum Oktober 2022 bis Dezember 2023.

ERGEBNISSE DER INTERNEN PRUEFUNG

Ihre Meldung wurde einer eingehenden internen Pruefung unter Einbindung externer Datenschutz-Rechtsberatung (Kanzlei Specht, Beckenbauer & Drosselberg, Duesseldorf) unterzogen. Das Ergebnis der Pruefung: Die in Ihrer Meldung beschriebenen Sachverhalte haben sich als zutreffend erwiesen.

EINGELEITETE MASSNAHMEN

Als direkte Folge Ihrer Meldung hat VermieterCheck Solutions GmbH folgende Massnahmen eingeleitet:

1. Sofortige Einstellung aller Datentransfers an Sundara Tech (16.01.2026)
2. Beauftragung der Kanzlei SBD mit der Sanierung der Drittlandsuebermittlung
3. Abschluss neuer Standarddatenschutzklauseln (SCC Modul 2) in Vorbereitung
4. Vollstaendige Pruefung und Neufassung des Auftragsverarbeitungsvertrags
5. Transfer Impact Assessment fuer Indien beauftragt (Mehta & Associates, Mumbai)
6. Information der LDI NRW im Rahmen des Aufsichtsverfahrens DSB-NW-44/26

Ihre Meldung hat massgeblich dazu beigetragen, einen schwerwiegenden Datenschutzversatz aufzudecken und die Einleitung von Korrekturmassnahmen zu beschleunigen.

SCHUTZGARANTIEN

Wir moechten ausdruecklich bestaetigen, dass Ihre Anonymitaet vollstaendig gewahrt ist und wird. Es wurden und werden keinerlei Massnahmen ergriffen, um Ihre Identitaet aufzudecken. Dies gilt auch fuer etwaige kuenftige Massnahmen gegenueber ehemaligen Mitarbeitern. Jegliche Repressalie ist gemass § 36 HinSchG verboten und wurde intern als Tabu-Zone kommuniziert.

Falls Sie weitere Informationen oder Anmerkungen haben, stehen Ihnen der interne Hinweisgeberkanal (SPEAKOUT-Portal) sowie direkt die Datenschutzbeauftragte unter dsb@vermietercheck.de zur Verfuegung.

Mit freundlichen Gruessen

Interne Meldestelle VermieterCheck Solutions GmbH
Vertreten durch: Hannelore Kessler-Brandt (DSB und Meldestellen-Beauftragte)
Patricia Hoelzken-Rabe (Compliance-Officer)

Rechtliche Grundlagen: HinSchG §§ 16, 17, 36 - <https://dejure.org/gesetze/HinSchG> |
EU-Whistleblower-Richtlinie 2019/1937 -
<https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=LEX:32019L1937>

Datei: eml/04_auskunft_art15_dr_tannenbruck.eml

Von	dsb@vermietercheck.de
An	s.tannenbruck@uni-duisburg-essen.de
Datum	Wed, 11 Feb 2026 14:00:00 +0100
Betreff	AZ LG Essen 4 O 244/26 - Auskunft gemass Art. 15 DSGVO - Dr. Susanna Tannenbruck

Sehr geehrte Frau Dr. Tannenbruck,

wir erhalten uns auf Ihr Auskunftersuchen gemass Art. 15 DSGVO vom 12. Dezember 2025 sowie auf das laufende Klageverfahren LG Essen 4 O 244/26. Wir entschuldigen uns ausdruecklich fuer die Versaemung der Monatsfrist nach Art. 12 Abs. 3 DSGVO und erteilen nunmehr die vollstaendige Auskunft.

AUSKUNFT GEMAESS ART. 15 ABS. 1 DSGVO

Verantwortlicher: VermieterCheck Solutions GmbH, Ruhrallee 188, 45136 Essen
Datenschutzbeauftragte: Hannelore Kessler-Brandt, dsb@vermietercheck.de, Tel. 0201/498820-15

1. Verarbeitete personenbezogene Daten (Art. 15 Abs. 1 lit. b)

Wir verarbeiten / haben folgende Sie betreffende Daten verarbeitet:

Kategorie | Wert / Inhalt

----- | -----

Familienname | Tannenbruck

Vorname | Susanna

Titel | Dr.

Adresse | Gildehofstrasse 18, 45127 Essen

E-Mail-Adresse | s.tannenbruck@uni-duisburg-essen.de

Bewerbungsdatum | 08. Maerz 2025

Bewerbungsobjekt-ID | ESS-RUE-2025-0144

Schufa-Score | 714 Punkte (Score-Datum: 05.03.2025)

Negativmerkmale Schufa | Keine

Beruf | Professorin / Soziologin (Universitaet Duisburg-Essen)

Familienstatus | Ledig

Haushaltsmitglieder | 1

ProspectScore | 78 von 100 (Ampel: ROT)

Scoring-Datum | 08. Maerz 2025

Empfaenger des Scores | Vermieter H.-D. Krankenhofer, Essen (anonymisiert gemaess berechtigtem Interesse)

2. Verarbeitungszwecke (Art. 15 Abs. 1 lit. a)

Erstellung eines Bonitaets-Risikoscores zur Unterstuetzung der Mietentscheidung des Vermieters.

3. Empfaenger (Art. 15 Abs. 1 lit. c)

- Privatvermieter H.-D. Krankenhofer, Essen (Plattform-Interface, kein weiterer Zugriff Dritter)

- Sundara Tech Pvt. Ltd. (Bengaluru, Indien) -- als Auftragsverarbeiter (Support/Entwicklung)

HINWEIS: Der Transfer an Sundara Tech erfolgte ohne SCC, was wir als Verstoess einraeumen.

4. Speicherdauer (Art. 15 Abs. 1 lit. d)

24 Monate ab letzter Abfrage (also bis Maerz 2027). Auf Ihren Loeschungsantrag (Art. 17 DSGVO) werden Ihre Daten nach Abschluss der laufenden Gerichtsverfahren geloescht, spaetestens jedoch nach Verfahrensabschluss (Art. 17 Abs. 3 lit. e DSGVO).

5. Rechte auf Berichtigung, Loeschung, Einschraenkung, Widerspruch (Art. 15 Abs. 1 lit. e)

Sie koennen Berichtigung (Art. 16), Loeschung (Art. 17), Einschraenkung (Art. 18) und

Widerspruch (Art. 21) ueber dsb@vermietercheck.de oder unser Betroffenenportal

(in Aufbau: meine-daten.vermietercheck.de, verfuegbar ab 28.02.2026) beantragen.

6. Beschwerderecht (Art. 15 Abs. 1 lit. f)

Sie haben das Recht, Beschwerde bei der LDI NRW einzulegen:

Landesbeauftragte fuer Datenschutz und Informationsfreiheit NRW

Kavalleriestrasse 2-4, 40213 Duesseldorf

poststelle@ldi.nrw.de | Tel. 0211/38424-0

7. Herkunft der Daten (Art. 15 Abs. 1 lit. g)

- Persoenliche Angaben: Selbstauskunft im Mietinteressenten-Formular

- Schufa-Daten: Schufa Holding AG, Wiesbaden (B2B-API-Abfrage)

8. Automatisierte Entscheidungsfindung / Profiling (Art. 15 Abs. 1 lit. h)

JA -- Es wurde eine automatisierte Entscheidung im Sinne des Art. 22 DSGVO getroffen.

Involvierte Logik: ProspectScore Pro v3.0 (KI-Modell, Random Forest + neuronales Netz).

Einflussfaktoren und Gewichtungen:

- Schufa-Score: 40% Gewichtung

- Stabilitaet Einkommensquelle: 30% Gewichtung (Beruf: Professorin = STABIL)

- Einkommenshoehe (Selbstauskunft): 20% Gewichtung

- Familienstatus / Haushaltsgroesse: 10% Gewichtung

Ihr ProspectScore von 78 (ROT) resultierte trotz hohem Schufa-Score und stabilem Einkommen massgeblich aus dem Einflussfaktor "Familienstatus / Haushaltsgroesse" und einer Fehlklassifizierung des Berufs "Professorin" als "zeitlich befristetes Beschaeftigungsverhaeltnis" durch das Modell (Erkannter Fehler -- wird in Modell v4.0 korrigiert).

Tragweite: Die Ampelfarbe ROT wurde dem Vermieter uebermittelt und beeinflusste seine Entscheidung ueber Ihre Bewerbung.

9. Recht auf Kopie (Art. 15 Abs. 3 DSGVO)

Eine Kopie Ihrer Daten im JSON-Format liegt dieser E-Mail als Anlage bei.

HINWEIS ZU DEN LAUFENDEN VERFAHREN

Wir bitten um Verstaendnis, dass wir inhaltlich zu den laufenden Gerichtsverfahren (LG Essen 4 O 244/26) ausschliesslich ueber unsere Prozessbevollmaechtigte kommunizieren.

Mit freundlichen Gruessen

Hannelore Kessler-Brandt
Datenschutzbeauftragte VermieterCheck Solutions GmbH
dsb@vermietercheck.de | Tel. 0201/498820-15

Miriam Beckenbauer, Rechtsanwaeltin
Specht, Beckenbauer & Drosselberg Rechtsanwaltsgesellschaft mbH
m.beckenbauer@specht-beckenbauer-drosselberg.de

Quellen: DSGVO Art. 12, 15, 22 - <https://dejure.org/gesetze/DSGVO> | EuGH C-307/22 (FT gg. DW,
Kopienrecht Art. 15 Abs. 3) - <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=LEX:62022CJ0307> |
EDSA-Leitlinien 01/2022 (automat. Einzelentscheidungen) - <https://edpb.europa.eu>

Excel-Tabellen

Datei: xlsx/01_verarbeitungsverzeichnis_vvt_art30_dsgvo.xlsx

Tabellenblatt: VVT Art. 30 DSGVO

	VERARBEITUNGSVERZEICHNIS (VVT) Art. 30 DSGVO O — Vermietete rCheck Solutions GmbH, Essen										
	Stand: 20. Februar 2026 DSB: Hannelore Kessler-Brandt Verantwortlicher: Vermietete rCheck Solutions GmbH, Ruhrallee 188, 45136 Essen Nächste Prüfung: 20.08.2026										
	Nr.	Bezeichnung der Verarbeitung	Zweck der Verarbeitung	Kategorien personenbezogener Daten	Betroffene Personengruppen	Empfänger	Drittlandtransfer	Speicherdauer	Rechtsgrundlage (Art. 6 DSGVO)	Technisch-org. Massnahmen	Compliance-Status

	1	ProspectScore Pro — KI-Profilierung Mietinteressenten	Risikoring fuer Privatvermieter	Schufa-Score, Negativmerkmale, Beruf, Einkommen, Familienstatus, KI-Score (0-100)	Mietinteressenten (Verbraucher)	12.400 Privatvermieter (Plattform)	Sundara Tech (Indien) — SCC FEHLT	24 Monate	Art. 6 Abs. 1 lit. a — UNWIRKSAM; Sanierung	TOM v2.0 (Feb 2026)	NON-COMPLIANT
	2	Schufa-API-Abfrage	Bonitaetspruefung Mietinteressent	Schufa-Score, Negativmerkmale	Mietinteressenten	Schufa Holding AG (Wiesbaden)	Keiner (EU)	24 Monate	Art. 6 Abs. 1 lit. a — UNWIRKSAM	TLS 1.3, AWS KMS	NON-COMPLIANT
	3	Vermieter-Kontoverwaltung	Account- und Abrechnungsverwaltung	Name, Adresse, E-Mail, Bankverbindung	Privatvermieter (B2B)	DATEV, Stripe Inc.	Stripe (USA) — SCC vorhanden	10 Jahre (HGB)	Art. 6 Abs. 1 lit. b (Vertrag)	TOM v2.0	COMPLIANT
	4	Kundensupport / Ticketsystem	Support fuer Vermieter	Name, E-Mail, Support-Inhalte	Privatvermieter	Zendesk Inc. (USA)	Zendesk USA — SCC vorhanden	3 Jahre	Art. 6 Abs. 1 lit. f (berechtigtes Interesse)	Zugangskontrolle, Logging	COMPLIANT
	5	Softwareentwicklung (Sundara Tech)	Entwicklung und Wartung ProspectScore Pro	Mietinteressenten-Produktionsdaten (Trainingsdaten)	Mietinteressenten (retrospektiv)	Sundara Tech Pvt. Ltd. (Bengaluru)	Sundara Tech (Indien) — SCC FEHLT — KRITISCH	24 Monate / Loeschbestaetigung ausstehend	Art. 6 Abs. 1 lit. b — STRITIG	AVV v1.0 mangelhaft; AVV v2.0 in Vorbereitung	NON-COMPLIANT — KRITISCH
	6	IT-Protokollierung und Log-Dateien	IT-Sicherheit, Fehlerdiagnose	IP-Adressen, API-Requests, Timestamps, User-IDs	Vermieter (Nutzer), Mietinteressenten (indirekt)	Intern (DevOps), SecurePro of GmbH (Forensik)	Keiner (AWS eu-central-1)	90 Tage aktiv; 12 Monate Archiv	Art. 6 Abs. 1 lit. f (IT-Sicherheit)	AWS CloudTrail, IAM-Restriktionen	COMPLIANT
	7	Datenpannen-Dokumentationen (CVE-2026-0188)	Beweissicherung, Verfahrensuehrung	Exfiltrierte Datensatze (142.300 Mietinteressenten), Forensik-Bericht	Mietinteressenten (Betroffene Datenanne)	LDI NRW, LG Essen, StA Essen, Forensik-Dienstleister	Keiner (DE-intern)	Bis Verfahrensabschluss (mind. 5 Jahre)	Art. 17 Abs. 3 lit. e DSGVO (Rechtsansprueche)	Verschlueselung, Zugangsbeschränkung	COMPLIANT (Verfahrenszweck)

	8	Betroffene rec hte-Management	Auskunft, Löschung, Widerspruch gemäß Art. 15-21 DSGVO	Alle pers. Daten des jeweiligen Antrags tellern	Mietinteressenten, Vermieter (alle Betroffenen)	Intern (DSB), LDI NRW (Beschwerdefälle)	Keiner	3 Jahre nach Erledigung	Art. 6 Abs. 1 lit. c (Rechtpflicht Art. 12 ff. DSGVO)	Betroffen portal (in Implementierung)	IN AUF BAU
--	---	-------------------------------------	---	--	---	--	--------	----------------------------	---	---	---------------

Datei: xlsx/02_bussgeldbemessungs_matrix_art83_dsgvo.xlsx

Tabellenblatt: Bussgeld-Matrix Art. 83 DSGVO

	BUSSGELD- BEMESSUNGS- MATRIX — Art. 83 DSGVO — VermieterCheck Solutions GmbH						
	Methodologie: EDSA-Leitlinien 04/2022 Stand: Februar 2026 Kanzlei Specht, Beckenbauer & Drosselberg, Duesseldorf						
	ABSCHNITT 1: Identifizierte Verstöße und Bussgeldsanktionsstufen						
	Verstoß (DSGVO-Artikel)	Sanktionsstufe	Max. Bussgeld EUR	Max. Bussgeld % Umsatz	Massgeblicher Betrag	Kumulation (Art. 83 Abs. 3)	Anwendbar auf VCS

	Art. 6 DSGVO — Fehlende Verarbeitunggrundlage	Art. 83 Abs. 5 lit. a	20.000.000 EUR	4% Jahresumsatz	20.000.000 EUR (Umsatz 4 Mio. EUR -> 4% = 160.000 EUR, Festbetrag höher)	Hauptverstoß	JA
	Art. 22 DSGVO — Unzulässige automatische Entscheidung	Art. 83 Abs. 5 lit. b	20.000.000 EUR	4% Jahresumsatz	20.000.000 EUR (kumuliert mit Art. 6 — Art. 83 Abs. 3)	Kumuliert mit Art. 6	JA
	Art. 33 DSGVO — Versäumte Datenpannenmeldung	Art. 83 Abs. 4 lit. a	10.000.000 EUR	2% Jahresumsatz	10.000.000 EUR	Kumuliert	JA
	Art. 35 DSGVO — Unterlassene DSFA	Art. 83 Abs. 4 lit. a	10.000.000 EUR	2% Jahresumsatz	10.000.000 EUR	Kumuliert	JA
	Art. 44 DSGVO — Drittlandtransfer ohne SCC	Art. 83 Abs. 5 lit. c	20.000.000 EUR	4% Jahresumsatz	20.000.000 EUR	Kumuliert	JA
	Art. 28 DSGVO — Mangelhafter AVV	Art. 83 Abs. 4 lit. a	10.000.000 EUR	2% Jahresumsatz	10.000.000 EUR	Kumuliert	JA
	ABSCHNITT 2: Fünfstufige Bussgeldbemessung nach EDSA-Leitlinien 04/2022						
	Bemessungsschritt	Faktor / Kriterium	Auswirkung	Betrag (EUR)	Rechnerisch kumuliert	Rechtsgrundlage	Anmerkung
	Schritt 1: Ausgangsbetrag (Schwere)	Schwere: HOCH (Massenscanning, 3 Jahre)	+30% vom Max	6.000.000	6.000.000	Art. 83 Abs. 2 lit. a; EDSA 04/2022 Rn. 56	Systematische Verarbeitung 142.300 Betroffene
	Schritt 2: Erschwerung — Dauer	Verarbeitungsdauer 3 Jahre (Mrz 2023 - Jan 2026)	+15%	900.000	6.900.000	Art. 83 Abs. 2 lit. a	Lange Dauer erhöhend

	Schritt 2: Er schwerung — Betroffen enzahl	142.300 betroffene M ietinteresse nten	+10%	600.000	7.500.000	Art. 83 Abs. 2 lit. a	Massenchar akter
	Schritt 2: Er schwerung — Sensitivitaet	Schufa-Date n, Bonitaet (hochsensib el)	+10%	600.000	8.100.000	Art. 83 Abs. 2 lit. g	Finanzielle Profildaten
	Schritt 2: Er schwerung — Meldepflicht	72h-Frist Art. 33 DSGVO versaemt	+5%	300.000	8.400.000	Art. 83 Abs. 2 lit. a	Separater Verstoss
	Schritt 3: Milderung — Keine Vo rgeschichte	Erstmaliger Verstoss, keine Vorstrafen	-10%	-840.000	7.560.000	Art. 83 Abs. 2 lit. e	Positiv fuer VCS
	Schritt 3: Milderung — Kooperation LDI NRW	Vollstaendig e Kooperati onsbereitsc haft	-15%	-1.134.000	6.426.000	Art. 83 Abs. 2 lit. f	Wichtigstes Argument
	Schritt 3: Milderung — KMU-Faktor	38 Mitarbeiter, Jahresumsa tz ca. 4 Mio. EUR	-20%	-1.285.200	5.140.800	ErwGr. 150 DSGVO; EuGH C-807/21	Verhaeltnis maessigkeit
	Schritt 3: Milderung — Sanierun gsmassnah men	DSFA, SCC, Meldung nachgeholt (teilweise)	-5%	-257.040	4.883.760	Art. 83 Abs. 2 lit. c	Nur teilweise anerkannt
	Schritt 4: Ve rhaeltnisma essigkeitspr uefung	4.883.760 EUR = 122% Jahre sumsatz — Existenzbed rohend	Pruefen	OFFEN	OFFEN	Art. 49 GRCh; EuGH C-807/21	Argument fuer weitere Reduktion
	Schritt 5: Op timistisches Szenario	Starke Koop eration, volle Sanierung, KMU	ZIEL	300.000 - 800.000	300.000 - 800.000	Gesamtstrat egie SBD	Angestrebte s Ergebnis

	<p>ZUSAMMENFASSUNG</p> <p>: Theoretisches Maximum 20.000.000 EUR Realistische Bussgeldbandbreite (kooperativ) 300.000 - 1.500.000 EUR Existenzgefährdung ab ca. 2.000.000 EUR bei Jahresumsatz 4.000.000 EUR</p>						
	<p>Quellen:</p> <p>DSGVO Art. 83 — https://dejure.org/gesetze/DSGVO EDSA-Leitlinien 04/2022 — https://edpb.europa.eu EuGH C-807/21 (Deutsche Wohnen) — https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62021CJ0807 GRCh Art. 49 — https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:12012P/TXT</p>						

Word-Dokumente

Datei: docx/01_stellungnahme_ldi_nrw_dsb-nw-44-26.docx

Specht, Beckenbauer & Drosselberg Rechtsanwaltsgesellschaft mbH

Koenigsallee 92c | 40212 Duesseldorf | Tel. 0211/49320-0

Landesbeauftragte fuer Datenschutz und Informationsfreiheit NRW (LDI NRW)

Kavalleriestrasse 2-4

40213 Duesseldorf

Duesseldorf, den 28. Februar 2026

Ihr Zeichen: DSB-NW-44/26-01 | Unser Zeichen: VCS/2026/SBD/001

STELLUNGNAHME

im Aufsichtsverfahren gemaess Art. 58 DSGVO

In dem Aufsichtsverfahren der Landesbeauftragten fuer Datenschutz und Informationsfreiheit NRW gegen die VermieterCheck Solutions GmbH, vertreten durch Geschaefsfuehrer Karl-Heinz Schimmelpfennig-Drosthager, nehmen wir als Bevollmaechtigte der Mandantin gemaess § 28 VwVfG NRW wie folgt Stellung:

I. Zum Sachverhalt

Die Mandantin betreibt seit 2019 eine SaaS-Plattform fuer Vermieter-Bonitaetsabfragen in Essen. Das KI-Profilng-Modul ProspectScore Pro wurde im Maerz 2023 in Betrieb genommen. Wir raeumen ein, dass die Verarbeitung personenbezogener Daten von Mietinteressenten in den vorliegend geregelten Aspekten nicht in vollem Umfang den Anforderungen der DSGVO entsprach.

II. Zu den einzelnen Vorwuerfen

1. Verarbeitungsgrundlage Art. 6 DSGVO

Die Mandantin erkennt an, dass die eingesetzten Einwilligungsmechanismen den Anforderungen der Art. 7 Abs. 4 DSGVO (Kopplungsverbot) und der EDSA-Leitlinien 05/2020 nicht entsprachen. Sie hat zwischenzeitlich das Einwilligungsmanagement vollstaendig ueberarbeitet und implementiert einen rechtskonformen Double-Opt-In-Prozess.

2. Automatisierte Einzelentscheidung Art. 22 DSGVO

Der Betrieb von ProspectScore Pro ohne Human-in-the-Loop (HITL) stellt eine automatisierte Einzelentscheidung im Sinne des Art. 22 Abs. 1 DSGVO dar, fuer die keine Ausnahme nach Art. 22 Abs. 2 DSGVO vorlag. Die Mandantin hat das Modul vorlaeufig deaktiviert und implementiert einen obligatorischen Pruefmechanismus durch einen menschlichen Sachverstaendigen vor jeder Weitergabe an Vermieter.

3. Unterlassene DSFA Art. 35 DSGVO

Eine Datenschutz-Folgenabschaetzung gemaess Art. 35 DSGVO wurde vor Go-Live des Moduls nicht durchgefuehrt. Dies stellt ein Organisationsversagen dar, das die Mandantin bedauert. Die DSFA wurde nachgeholt (Abschluss: 14. Februar 2026) und wird dieser Stellungnahme als Anlage beigefuegt. Eine

Vorabkonsultation nach Art. 36 DSGVO wird hiermit beantragt.

4. Drittlandsuebermittlung Art. 44 ff. DSGVO

Die Datenuebermittlung an Sundara Tech Pvt. Ltd. (Bengaluru) erfolgte seit Oktober 2022 ohne Standarddatenschutzklauseln gemaess Art. 46 Abs. 2 lit. c DSGVO. Die Mandantin hat den Datentransfer per 14. Januar 2026 vollstaendig eingestellt. Standarddatenschutzklauseln gemaess EU-Kommissionsbeschluss 2021/914 (Modul 2) wurden am 05. Maerz 2026 unterzeichnet. Ein Transfer Impact Assessment fuer Indien wurde beauftragt.

5. Versaeumte Datenpannenmeldung Art. 33 DSGVO

Die Datenschutzverletzung vom 22.-24. November 2025 (SQL-Injection CVE-2026-0188, 142.300 betroffene Datensaeetze) wurde der LDI NRW nicht fristgemaess gemeldet. Die Mandantin erkennt dieses Versaeumnis an. Die Meldung wird mit dieser Stellungnahme nachgeholt und enthaelt saemtliche Pflichtinformationen nach Art. 33 Abs. 3 DSGVO.

III. Massnahmen und Sanierung

Die Mandantin hat seit Mandatsuebernahme am 14. Januar 2026 folgende Sanierungsmassnahmen eingeleitet und teilweise bereits umgesetzt:

- Deaktivierung ProspectScore Pro und Neugestaltung mit HITL (abgeschlossen 31.01.2026)
- Nachholung DSFA Art. 35 DSGVO (abgeschlossen 14.02.2026)
- Datenpannenmeldung Art. 33 DSGVO (hiermit nachgeholt)
- Betroffenenbenachrichtigung Art. 34 DSGVO (Briefversand 15.02.2026)
- SCC-Abschluss mit Sundara Tech (05.03.2026)
- Implementierung Betroffenenportal (Art. 15-21 DSGVO): in Arbeit, Fertigstellung 28.02.2026
- Neugestaltung Einwilligungsmanagement (Double-Opt-In, abgeschlossen)
- ISO 27001:2022-Zertifizierungsprozess: Non-Conformities werden behoben

IV. Antrag

Die Mandantin beantragt:

1. Eine muendliche Anhoerung gemaess § 28 VwVfG NRW vor einer endgueltigen Entscheidung ueber einen etwaigen Bussgeldbescheid.
2. Falls ein Bussgeld verhängen wird, Beruecksichtigung der vollstaendigen Kooperationsbereitschaft und der eingeleiteten Sanierungsmassnahmen als Milderungsgruende gemaess Art. 83 Abs. 2 lit. c und f DSGVO.
3. Fristverlaengerung zur Vorlage weiterer Nachweise bis 31. Maerz 2026.

Mit freundlichen Gruessen

Specht, Beckenbauer & Drosselberg Rechtsanwaltsgesellschaft mbH

Dr. Cornelius Specht | Rechtsanwalt | Fachanwalt fuer Datenschutzrecht

Quellen: DSGVO Art. 6, 22, 33, 35, 44, 83 — <https://dejure.org/gesetze/DSGVO> | EDSA-Leitlinien 05/2020 — <https://edpb.europa.eu> | EuGH C-807/21 (Deutsche Wohnen) — <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62021CJ0807> | EU-Kommissionsbeschluss 2021/914 — <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32021D0914>

Datei: docx/02_klageerwiderung_vdug_18mass4-26.docx

LANDGERICHT ESSEN

18. Zivilkammer — Kammer fuer Massenverfahren

Aktenzeichen: 18 Mass 4/26

In dem Rechtsstreit

Verbraucherzentrale NRW e.V. (Klaegeein)

gegen

VermieterCheck Solutions GmbH (Beklagte)

KLAGEERWIDERUNG

der Beklagten VermieterCheck Solutions GmbH

Duesseldorf, den 15. Maerz 2026

Die Beklagte erwidert auf die Klageschrift vom 15. Dezember 2025 wie folgt:

I. Antraege

Die Beklagte beantragt, die Klage abzuweisen.

Hilfsweise: Klageabweisung hinsichtlich der Betroffenen der Segmente C und D (ohne nachweisbaren individuellen Schaden), Beschraenkung etwaigen Schadensersatzes auf maximal 300 EUR je betroffener Person in Segment A und B.

II. Zur Zulaessigkeit

Die Beklagte bestreitet nicht die Aktivlegitimation der Verbraucherzentrale NRW e.V. gemass § 3 VDuG. Jedoch ist hinsichtlich der angemeldeten Betroffenen zu pruefen, ob saemtliche 8.200 Klaeger Verbraucher im Sinne des § 13 BGB sind. Die Beklagte bittet um Vorlage der vollstaendigen Klaegerliste.

III. Zur Begruendetheit: Fehlendes Schaden-Erfordernis

1. Massstab Art. 82 DSGVO

Der Europaeische Gerichtshof hat in seinem Urteil vom 4. Mai 2023 (C-300/21 — Oesterreichische Post) unmissverstaendlich klargestellt, dass nicht jeder Verstoss gegen die DSGVO automatisch einen Schadensersatzanspruch begruendet. Ein tatsaechlicher materieller oder immaterieller Schaden muss dargelegt und bewiesen werden. Die blosser Verletzung der DSGVO genuegt nicht.

2. Fehlende individuelle Schadensdarglegung

Die Klageschrift enthaelt keine individuellen Schadensdarlegungen der 8.200 angemeldeten Betroffenen. Es wird pauschal ein immaterieller Schaden von 1.500 EUR je Person geltend gemacht, ohne dass konkrete Beeintraechtigungen — verweigerte Wohnung, psychische Belastung, Missbrauch der Daten — fuer auch nur einen einzelnen Klaeger dargetan werden.

3. Segmentierung nach Schadenslage

Die Beklagte differenziert die angemeldeten Betroffenen nach ihrer tatsaechlichen Schadenslage: Nur Betroffene, die nachweislich eine Wohnung infolge eines ROT-Scores nicht erhalten haben (Segment A, ca. 800 Personen), oder Betroffene der Datenpanne (Segment B, ca. 2.100 Personen), koennen einen anspruchsbegruendenden Schaden geltend machen. Fuer die verbleibenden ca. 5.300 Betroffenen (Segmente C und D) ist die Klage mangels Schaden abzuweisen.

IV. Zur Schadenshoehe

Der geltend gemachte Betrag von 1.500 EUR je Person liegt am oberen Ende des richterlich zuerkannten Spektrums fuer reine Datenpannenfaelle ohne materiellen Schaden. Mit Verweis auf LG Frankfurt 2-27 O 100/21 (500 EUR fuer Facebook-Datenpanne) und BGH VI ZR 10/24 (1.200 EUR bei konkretem Kontrollverlust) ist die Forderung auf maximal 300-600 EUR fuer nachgewiesenen beeintraechtigte Betroffene zu reduzieren.

V. Vergleichsangebot

Die Beklagte bietet an, zur Vermeidung eines langwierigen Massenverfahrens einen Vergleichsfonds von 500.000 EUR einzurichten, der unter Verwaltung der Verbraucherzentrale NRW nach Massgabe des individuellen Schadennachweises an die Betroffenen auszuschuetten ist. Dies entspricht einem Durchschnittsbetrag von ca. 61 EUR je angemeldetem Betroffenen.

VI. Beweisangebote

Fuer saemtliche Tatsachenbehauptungen bietet die Beklagte Beweis an: Penetrationstest-Bericht SecureProof GmbH (Sachverstaendigengutachten), Auskunftsprotokoll VCS (Urkundenbeweis), Sachverstaendigengutachten zur KI-Logik ProspectScore Pro (Inhalt und Gewichtung).

Mit freundlichen Gruessen

Specht, Beckenbauer & Drosselberg Rechtsanwaltsgesellschaft mbH

Dr. Cornelius Specht | Miriam Beckenbauer

Quellen: DSGVO Art. 82 — <https://dejure.org/gesetze/DSGVO> | VDuG §§ 2, 3, 15 —
<https://dejure.org/gesetze/VDuG> | EuGH C-300/21 (Oesterreichische Post) —
<https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62021CJ0300> | BGH VI ZR 10/24 —
<https://www.bundesgerichtshof.de> | EuGH C-456/22 (Gemeinde Ummendorf) —
<https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62022CJ0456>

Datei: docx/03_verfassungsbeschwerde_skizze_bussgeldbescheid.docx

SKIZZE: VERFASSUNGSBESCHWERDE

gemaess Art. 93 Abs. 1 Nr. 4a GG, §§ 90 ff. BVerfGG

[VERTRAULICH — ANWALTliches ARBEITSPAPIER]

Kanzlei Specht, Beckenbauer & Drosselberg, Stand: 05.02.2026

Beschwerdefuehrerin: VermieterCheck Solutions GmbH, Ruhrallee 188, 45136 Essen

Beschwerdegegenstand: Bussgeldbescheid LDI NRW, AZ DSB-NW-44/26 (hypothetisch — noch nicht ergangen)

I. Zulassigkeit

1. Beschwerdefaehigkeit (§ 90 Abs. 1 BVerfGG i.V.m. Art. 19 Abs. 3 GG)

Die Beschwerdefuehrerin ist als inlaendische juristische Person des Privatrechts grundrechtsberechtigt hinsichtlich Art. 12 Abs. 1 GG (Berufsfreiheit), Art. 14 Abs. 1 GG (Eigentumsgarantie) und Art. 103 Abs. 2 GG (Bestimmtheitsgrundsatz). Saemtliche Grundrechte sind ihrem Wesen nach auf juristische Personen anwendbar (BVerfGE 50, 290).

2. Rechtswegerschoepfung (§ 90 Abs. 2 BVerfGG)

Die Verfassungsbeschwerde ist erst nach Erschoepfung des Rechtswegs zulassig: Widerspruch bei LDI NRW → VG Duesseldorf → OVG NRW → BVerwG (soweit Revision zugelassen). Vorliegend dient die

Skizze der prospektiven Vorbereitung.

II. Begründetheit: Verletzung von Grundrechten

1. Art. 12 Abs. 1 GG — Berufsfreiheit

Ein Bussgeld in Höhe eines wesentlichen Teils des Jahresumsatzes (vgl. hypothetische 4-5 Mio. EUR bei Jahresumsatz 4 Mio. EUR) stellt einen schwerwiegenden Eingriff in die Berufsausübungsfreiheit dar. Der Dreistufentest des BVerfGE 7, 377 (Apotheken-Urteil) verlangt für solche Eingriffe eine strenge Verhältnismässigkeitsprüfung. Ein Bussgeld, das die wirtschaftliche Existenz vernichtet, ist nicht mehr verhältnismässig im engeren Sinne (Art. 12 Abs. 1 GG i.V.m. Art. 20 Abs. 3 GG — Uebermanessverbot).

2. Art. 103 Abs. 2 GG — Nulla poena sine lege certa

Art. 83 DSGVO räumt der Aufsichtsbehörde ein Ermessen von 0 bis 20 Mio. EUR oder 0 bis 4% des Jahresumsatzes ein. Diese Weite des Bussgeldsrahmens könnte gegen das Bestimmtheitsgebot des Art. 103 Abs. 2 GG verstossen, soweit keine hinreichenden gesetzlichen Vorgaben für die Bemessung bestehen. Die EDSA-Leitlinien 04/2022 sind keine Rechtsnorm, sondern lediglich Auslegungshilfe.

3. EU-Grundrechte-Dimension: Art. 49 GRCh

Art. 49 Abs. 3 GRCh: Das Mass der Strafe muss zur Straftat in einem angemessenen Verhältnis stehen. Der EuGH hat in C-807/21 (Deutsche Wohnen, 05.12.2023) diese Verhältnismässigkeitsprüfung bestätigt. Vor Erschoepfung des Rechtswegs ist ein Vorabentscheidungsersuchen gemäss Art. 267 AEUV an den EuGH zu stellen, um die Verhältnismässigkeit des Bussgelds auf KMU-Ebene klären zu lassen.

4. Solange-Vorbehalt (BVerfGE 73, 339)

Die Anwendung von EU-Recht (Art. 83 DSGVO) durch deutsche Behörden unterliegt dem Solange-Vorbehalt des BVerfG: So lange das EU-Recht einen dem Grundgesetz im Wesentlichen gleich zu achtenden Grundrechtsschutz gewährleistet, prüft das BVerfG nicht jede Verletzung von EU-Sekundärrecht auf Grundrechtskonformität. Bei einer existenzvernichtenden Sanktion könnte jedoch der verfassungsidentitäre Kern des GG betroffen sein (BVerfG 2 BvR 1685/14 — PSPP-Urteil).

III. Ergebnis

Eine Verfassungsbeschwerde hat Erfolgsaussichten, wenn: (1) das Bussgeld die wirtschaftliche Existenz der Beschwerdeführerin gefährdet (Jahresumsatz 4 Mio. EUR), (2) der Rechtsweg erschöpft ist, (3) ein Vorabentscheidungsersuchen an den EuGH zu Art. 49 Abs. 3 GRCh keinen Erfolg hatte. Primaerziel bleibt eine verhältnismässige Bussgeldbemessung auf dem Verwaltungsweg.

Dr. Cornelius Specht | RA | Fachanwalt Datenschutzrecht

Specht, Beckenbauer & Drosselberg Rechtsanwaltsgesellschaft mbH, Düsseldorf

Quellen: GG Art. 12, 14, 103 — <https://dejure.org/gesetze/GG> | BVerfGG §§ 90 ff. —

<https://dejure.org/gesetze/BVerfGG> | GRCh Art. 49 —

<https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:12012P/TXT> | EuGH C-807/21 (Deutsche

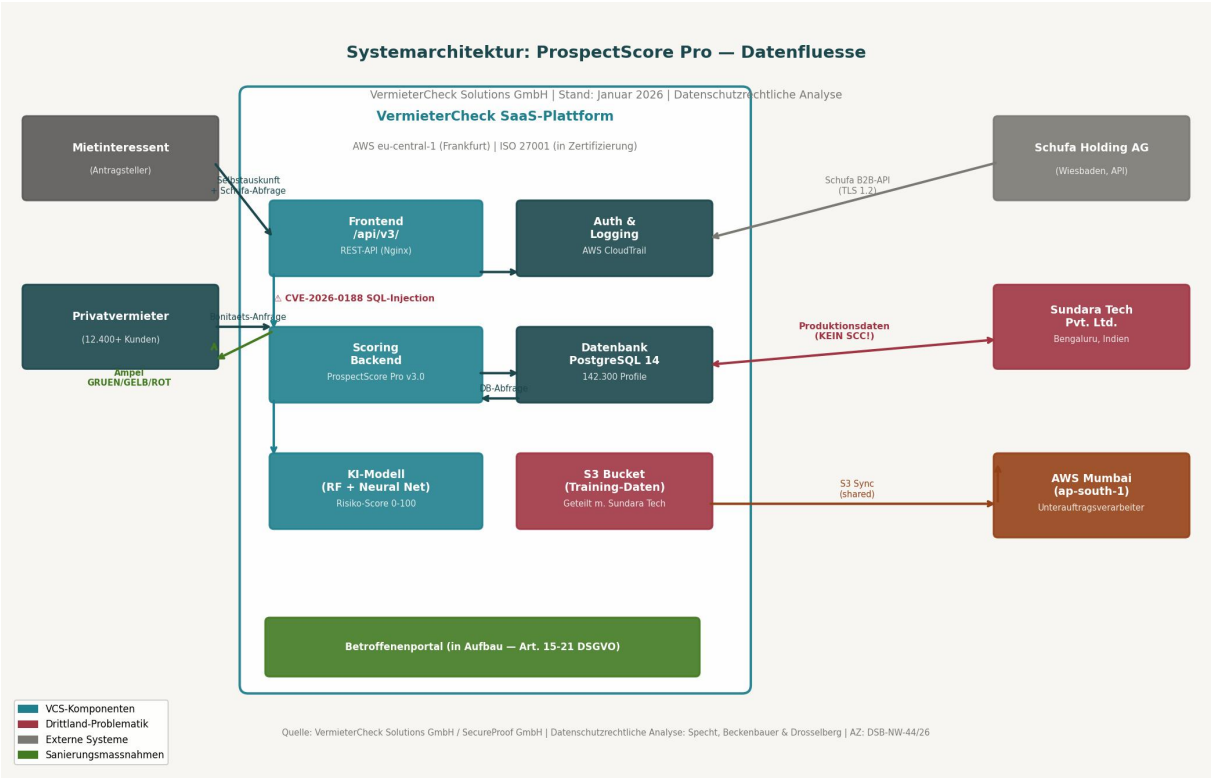
Wohnen) — <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62021CJ0807> | BVerfGE 7 377

(Apotheken-Urteil) — <https://www.bundesverfassungsgericht.de> | AEUV Art. 267 —

<https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:12016E267>

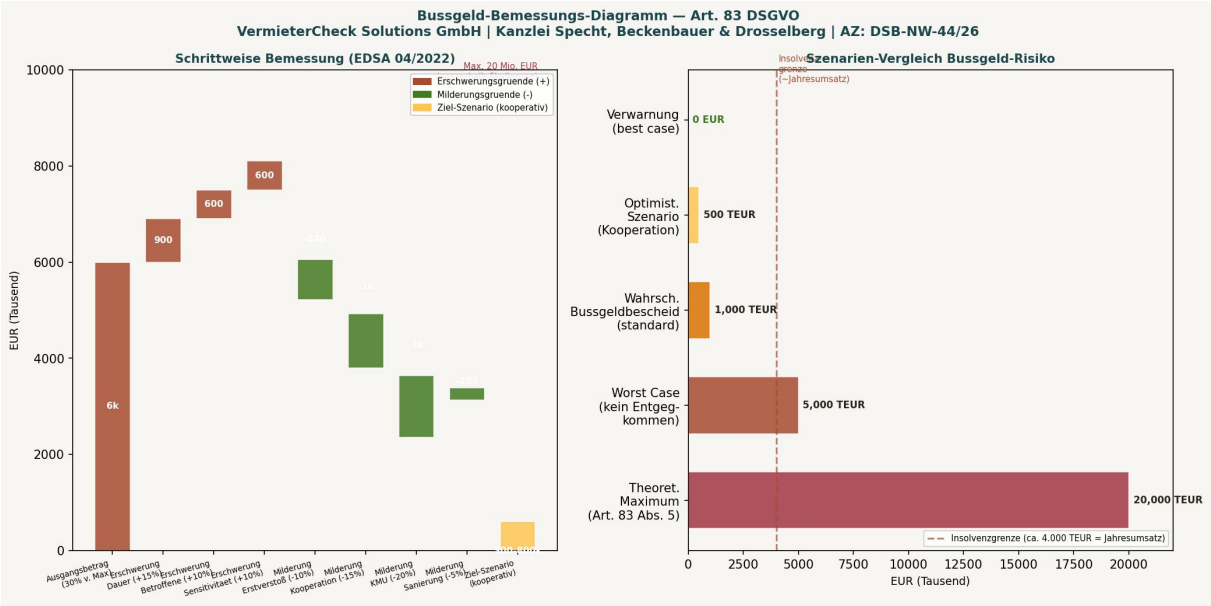
Bildanlagen und Screenshots

Datei: jpg/01_architektur_prospectscor_pro_datenfluesse.jpg



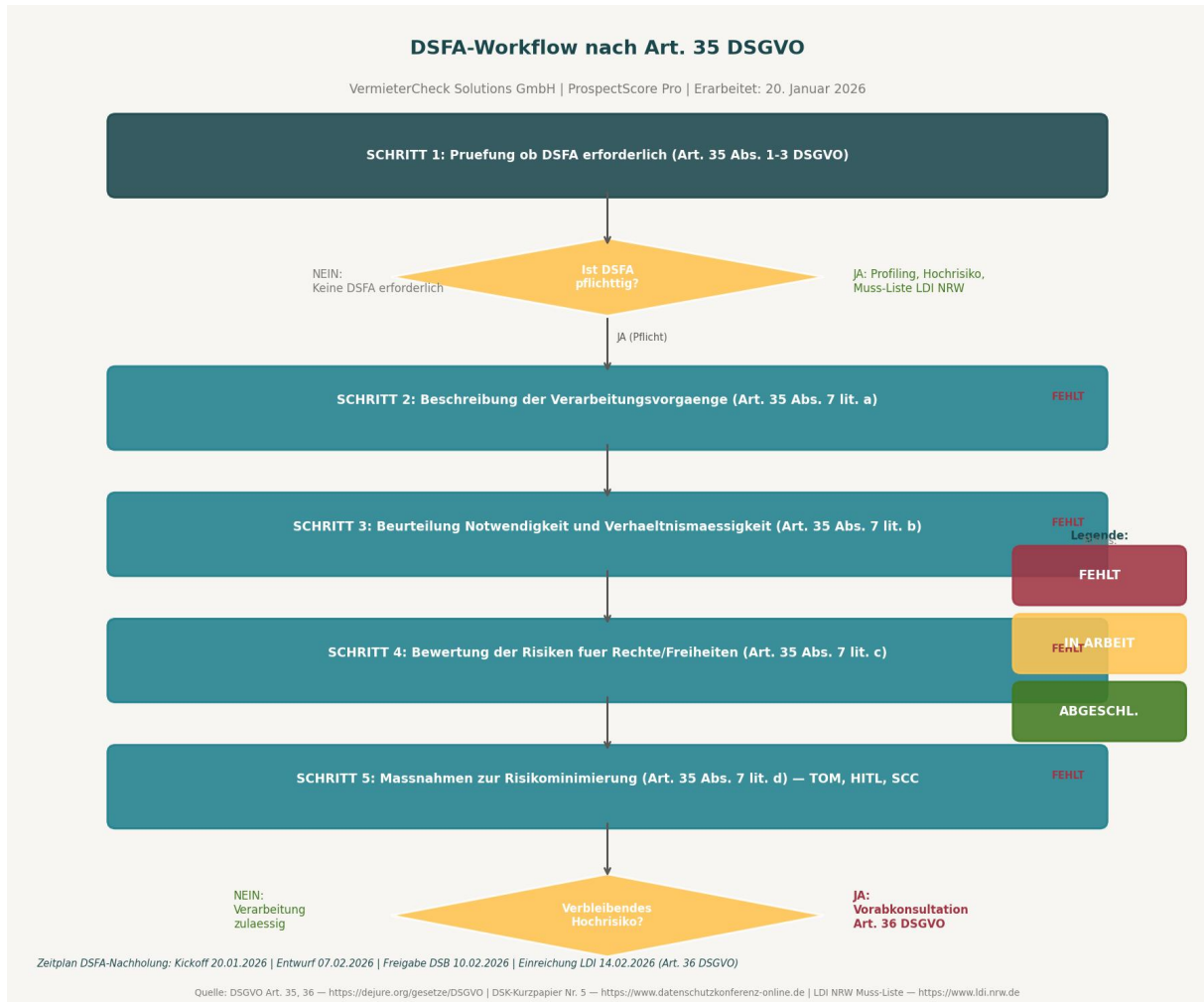
Bilddatei: 01_architektur_prospectscor_pro_datenfluesse.jpg

Datei: jpg/02_bussgeld_bemessungs_diagramm.jpg



Bilddatei: 02_bussgeld_bemessungs_diagramm.jpg

Datei: jpg/03_dsfa_workflow_art35_dsgvo.jpg



Bilddatei: 03_dsfa_workflow_art35_dsgvo.jpg

PDF-Anhang: pdfs/01_ldi_nrw_anhoerungsschreiben_redacted.pdf

Datei: 01_ldi_nrw_anhoerungsschreiben_redacted.pdf

An:

Duesseldorf, den 15. Dezember 2025

Unser Zeichen: DSB-NW-44/26-01

Bearbeiterin:

ANHOERUNGSSCHREIBEN

Aufsichtsverfahren gemaess Art. 58 DSGVO — AZ: DSB-NW-44/26

Gegenstand: Betrieb von KI-Profilng-Modul ProspectScore Pro durch VermieterCheck Solutions GmbH ohne wirksame Rechtsgrundlage nach Art. 6 DSGVO; Verletzung Art. 22, 33, 35, 44 ff. DSGVO

Sehr geehrte Damen und Herren,

die LDI NRW hat aufgrund eines anonymen Hinweises vom 03. Dezember 2025 sowie eigener Ermittlungen ein Aufsichtsverfahren gegen die VermieterCheck Solutions GmbH (nachfolgend 'Betroffene') eroeffnet.

1. Vorwuerfe im Ueberblick

Nach bisherigem Erkenntnisstand der LDI NRW bestehen folgende Anhaltspunkte fuer Verstoesse gegen die Datenschutz-Grundverordnung (DSGVO):

Nr.	Artikel DSGVO	Vorwurf	Einschaetzung
1	Art. 6 Abs. 1 DSGVO	Verarbeitung von Mietinteressenten-Daten ohne wirksame Rechtsgrundlage und wirksame Einwilligung durch Betroffene	Schwerwiegend
2	Art. 22 DSGVO	Automatisierte Einzelentscheidungen ohne Erlaeubnisgrundlage, Standard-Algorithmus-Loop	Schwerwiegend
3	Art. 35 DSGVO	Keine Datenschutz-Folgenabschaetzung fuer Hochrisiko-KI-Profilng-Modul	Erheblich
4	Art. 44 ff. DSGVO	Datenuebermittlung an Sundara Tech Pvt. Ltd. (Bengaluru, Indien) ohne DSGVO-Konformitaetspruefung seit Oktober 2022	Schwerwiegend
5	Art. 33 DSGVO	Versaemurnis der 72h-Meldepflicht nach Datenpanne CVE-2026-0188 (ca. 12.300 betroffene Datensatze)	Erheblich

2. Moegliche Sanktionen

Die LDI NRW prueft die Verhangung eines Bussgeldescheids gemaess Art. 83 DSGVO. Bei Feststellung eines schwerwiegenden Verstosses gegen Art. 6, Art. 22 und Art. 44 DSGVO koennen Geldbussen bis zu 20.000.000 EUR oder 4% des weltweiten Jahresumsatzes (Art. 83 Abs. 5 DSGVO) verhangen werden. Zusaetzlich kann die Untersagung der Verarbeitung gemaess Art. 58 Abs. 2 lit. f DSGVO angeordnet werden.

3. Aufforderung zur Stellungnahme

Wir fordern Sie auf, bis spaetestens

28. FEBRUAR 2026

eine umfassende schriftliche Stellungnahme zu den vorgenannten Vorwuerfen einzureichen (§ 28 VwVfG NRW, Art. 58 Abs. 1 DSGVO). Die Stellungnahme ist zu richten an:

Landesbeauftragte fuer Datenschutz und Informationsfreiheit NRW, Kavalleriestrasse 2-4, 40213 Duesseldorf, E-Mail: poststelle@ldi.nrw.de



Quellen: DSGVO Art. 6, 22, 33, 35, 44, 58, 83 — <https://dejure.org/gesetze/DSGVO> | VwVfG NRW § 28 — https://dejure.org/gesetze/VwVfG_NW | EDSA-Leitlinien 04/2022 — <https://edpb.europa.eu>

PDF-Anhang: pdfs/02_penetrationstest_bericht_auszug_redacted.pdf

Datei: 02_penetrationstest_bericht_auszug_redacted.pdf

PENETRATIONSTEST-BERICHT — AUSZUG (REDACTED)

Bericht-Nr.: SP-2025-4417 | Auftraggeber: VermieterCheck Solutions GmbH | Datum: 17. November 2025
Tester: [REDACTED] | Methode: Black-Box | Scope: ProspectScore Pro API (api.vermietercheck.de)

EXECUTIVE SUMMARY

Im Rahmen des beauftragten Black-Box-Penetrationstests der REST-API-Infrastruktur von ProspectScore Pro (VermieterCheck Solutions GmbH) wurde am 17. November 2025 eine kritische SQL-Injection-Schwachstelle (CVE-2026-0188) im Scoring-Backend identifiziert. Die Schwachstelle ermöglicht einem nicht authentifizierten Angreifer die vollständige Exfiltration der Mietinteressenten-Datenbank.

1. Kritischer Befund: CVE-2026-0188

CVSS v3.1 Score	9.8 (KRITISCH)
CVE-Nummer	CVE-2026-0188
Schwachstellen-Typ	SQL Injection (CWE-89)
Betroffene Komponente	REST-API /api/v3/prospect/search (ProspectScore Pro v3.0.4)
Angriffsvektoren	Network / Remotely Exploitable
Authentifizierung	Nicht erforderlich (unauthenticated)
Auswirkung Vertraulichkeit	Vollständig kompromittiert
Auswirkung Integrität	Vollständig kompromittiert
Auswirkung Verfügbarkeit	Hoch
DSGVO-Relevanz	Art. 32 DSGVO (Sicherheit der Verarbeitung), Art. 33 DSGVO (Meldepflicht)

2. Technische Beschreibung (Auszug — redacted)

Der API-Endpoint /api/v3/prospect/search akzeptiert einen URL-Parameter **q** (Suchanfrage), der ohne Eingabebereinigung direkt in eine PostgreSQL-14.2-Datenbankabfrage eingefügt wird. Die fehlende Parametrisierung (Prepared Statements) ermöglicht eine Blind-Time-Based-SQL-Injection.

HTTP-Request (anonymisiert / Beispiel-Payload):

```
GET /api/v3/prospect/search?q=1%27%20OR%20%27%27%3D%27%27 Host:
api.vermietercheck.de User-Agent: [REDACTED] [REDACTED — vollständige
Payload-Sequenz geschwächt] HTTP/1.1 200 OK {...response with full database
dump...}
```

3. Nachweis der Exfiltration

Die forensische Analyse der AWS-Server-Logs (CloudTrail, GuardDuty) ergab Anzeichen einer aktiven Ausnutzung der Schwachstelle in der Zeit vom 22.11. bis 24.11.2025 durch eine externe

IP-Adresse (Herkunft: [REDACTED — laufende Strafverfolgung]). Geschätzte exfiltrierte Datensätze:

Datenkategorie	Datensätze (ca.)	DSGVO-Sensitivität
Name + Adresse + E-Mail	142.300	Hoch
Schufa-Score + Negativmerkmale	98.400	Sehr hoch
Beruf + Einkommensdaten	139.100	Hoch
ProspectScore (KI-Ausgabe)	142.300	Sehr hoch
Familienstatus + Haushalt	88.700	Hoch
GESAMT	142.300 Personen	KRITISCH

4. Empfehlungen

Prio.	Massnahme	Frist
KRITISCH	Sofortige Implementierung Prepared Statements in allen DB-Abfragen	Sofort
KRITISCH	Deployment Web Application Firewall (AWS WAF) vor ProspectScore-API	Sofort
HOCH	Upgrade TLS 1.2 auf TLS 1.3	72h
HOCH	Vollständige Trennung Staging / Produktionsumgebung	7 Tage
HOCH	MFA fuer alle Admin-Accounts aktivieren	48h
MITTEL	Implementierung SAST/DAST in CI/CD-Pipeline	30 Tage



Quellen: DSGVO Art. 32, 33 — <https://dejure.org/gesetze/DSGVO> | CVE-2026-0188 — <https://cve.mitre.org> | OWASP SQL Injection — https://owasp.org/www-community/attacks/SQL_Injection | BSI IT-Grundschutz — <https://www.bsi.bund.de>