



Datenschutzrechtliche Betrachtungen von Use Cases für Data Clean Rooms (DCR)

Datenschutzrechtliche Betrachtungen von Use Cases für Data Clean Rooms (DCR)

1. Einleitung	2
2. Rechtliche Grundlagen und datenschutzrechtlicher Rahmen	3
2.1 Rechtsgrundlagen nach Art. 6 DSGVO	3
2.2 Rollenverständnis	3
2.3 Anwendungsbereich der DSGVO	4
3. Use Cases im Überblick	5
3.1 Use Case: Potenzialanalyse	5
3.2 Use Case: Audience Insights	7
3.3 Use Case: Activation – Retargeting	9
3.4 Use Case: Activation – Lookalike Audience (im DCR)	10
3.5 Use Case: Activation – Lookalike außerhalb DCR	13
4. Vertragliche Rahmenbedingungen	14
5. Bewertung der gemeinsamen Verantwortlichkeit	16
6. Handlungsempfehlungen	18
7. Ausblick	19
Autorenverzeichnis	20
Über uns	21
Impressum	21

1. Einleitung

Data Clean Rooms (im nachfolgenden „**DCR**“) sind in aller Munde, wenn es um datenschutzfreundliche Datenkooperationen zwischen Unternehmen geht. Dabei handelt es sich um sichere, neutrale Umgebungen, in denen beispielsweise Publisher oder Vermarkter (im nachfolgenden auch gemeinsam „**Sell-Side**“) und Werbungtreibende oder Agenturen (im nachfolgenden gemeinsam auch „**Demand-Side**“) ihre First-Party-Daten kontrolliert zusammenführen und analysieren können.

Ziel ist es, Auswertungen vorzunehmen (etwa zur Überschneidung ihrer Nutzergruppen) oder Werbemaßnahmen zu ermöglichen, ohne dass die Rohdaten direkt ausgetauscht oder offengelegt werden. Die einzelnen Datensätze verbleiben dabei pseudonymisiert im DCR. Die zentrale Herausforderung besteht darin, dass DCR zwar datenschutzfreundliche Datenkooperationen ermöglichen, die datenschutzrechtliche Bewertung aber stark vom jeweiligen Datenfluss, Zweck und Rollenverständnis abhängt.

Das Whitepaper richtet sich an Marktteilnehmer im Programmatic-Advertising-Ökosystem (insbesondere Publisher, Vermarkter, Werbungtreibende, Agenturen und Technologieanbieter), die DCR-Projekte rechtlich einordnen, planen oder umsetzen möchten. Im Paper werden typische Use Cases – von Audience Insights (Publikumsanalysen) bis hin zur Aktivierung von Zielgruppen (Retargeting- und Lookalike Audiences) – aus Sicht der Datenschutz-Grundverordnung (**DSGVO**) untersucht.

Die Use Cases sollen als Orientierung dienen, um typische Szenarien einzuordnen, rechtliche Herausforderungen und Fragestellungen zu erkennen und die Ausgestaltung von Datenkooperationen, Verträgen und Einwilligungsprozessen zu bewerten. Dafür werden zunächst rechtliche Grundlagen und Rollenverteilungen erläutert. Anschließend werden die einzelnen Use Cases vorgestellt und juristisch bewertet. Abschließend gibt das Whitepaper Empfehlungen für die datenschutzkonforme Ausgestaltung von DCR-Projekten sowie einen Ausblick auf Herausforderungen wie Interoperabilität und zukünftige Entwicklungen.

Hinweis:

Im Folgenden geht es vor allem um Use Cases, bei denen personenbezogene Daten von zwei oder mehr Parteien (z. B. Publisher und Werbungtreibende, im Folgenden auch: die „**Beteiligten**“) abgeglichen werden.

Use Cases, die KI-basierte Erkenntnisse im Rahmen von Insight-Analysen liefern, werden erst später in Folgeversionen des Dokuments mit steigender Marktreife aufgegriffen. Dabei werden nicht nur zwei Datensätze allein auf Basis eines identischen personenbezogenen Merkmals gematcht; DCR-basierte KI-Analysen erlauben künftig auch das Identifizieren gemeinsamer Muster multipler Datensets, um partnerübergreifende Zusammenhänge in Form von Insights abzuleiten. Jeder Partner trägt also einzeln zu einem Gesamt-Insights-Modell innerhalb dieser multiplen Partnerkollaboration bei.

2. Rechtliche Grundlagen und datenschutzrechtlicher Rahmen

Bevor wir in die konkreten Use Cases eintauchen, werden die wichtigsten DSGVO-Grundlagen skizziert, die für DCR relevant sind.

2.1 Rechtsgrundlagen nach Art. 6 DSGVO

Jede Verarbeitung personenbezogener Daten braucht einen Erlaubnistatbestand. Im Marketing-Kontext kommen typischerweise folgende Rechtsgrundlagen in Betracht:

- **Einwilligung** (Art. 6 Abs. 1 lit. a DSGVO) – die ausdrückliche Zustimmung der Nutzer*innen zur Nutzung ihrer Daten für personalisierte Werbung oder zum Abgleich in einem DCR;
- **Berechtigtes Interesse** (Art. 6 Abs. 1 lit. f DSGVO) – die Parteien können argumentieren, ein überwiegendes berechtigtes Interesse an der Datenkooperation zu haben, sofern die Verarbeitung die Rechte der Nutzer*innen nicht unverhältnismäßig beeinträchtigt; oder seltener
- **Vertragserfüllung** (Art. 6 Abs. 1 lit. b DSGVO) – etwa, wenn die Datenverarbeitung zur Erfüllung eines Vertrags mit dem Betroffenen erforderlich ist (in DCR Use Cases meist nicht direkt einschlägig, außer ggf. im Rahmen eines von den Nutzer*innen gewünschten Service).

Oftmals ist die Einwilligung für werbliche DCR-Szenarien der einschlägige Weg. Im Rahmen von ausschließlich statistischen Analysen ohne direkte Ansprache kann auch ein sorgfältig abgewogenes berechtigtes Interesse in Betracht gezogen werden.

2.2 Rollenverständnis

Die DSGVO unterscheidet zwischen Verantwortlichen (im nachfolgenden auch „**Controller**“), die über Zweck und Mittel der Verarbeitung entscheiden, und Auftragsverarbeitern (im nachfolgenden auch „**Processor**“), die weisungsgebunden im Auftrag eines Verantwortlichen handeln (Art. 4 Nr. 7 und 8 DSGVO).

Zudem kennt die DSGVO die gemeinsame Verantwortlichkeit (im nachfolgenden auch „**Joint Control**“, Art. 26 DSGVO). Sie liegt vor, wenn zwei oder mehr Verantwortliche Zweck und Mittel der Verarbeitung personenbezogener Daten gemeinsam festlegen. Sie müssen dann eine Joint-Controller-Vereinbarung (im nachfolgenden auch „JCA“) schließen, die regelt, wer welche Pflichten aus der DSGVO übernimmt.

Bei DCR-Projekten agieren die Beteiligten in der Regel zumindest initial jeweils als eigene Verantwortliche für ihre Daten: Jeder bringt Nutzerdaten in den DCR ein und entscheidet selbst, zu welchem Zweck (Analyse, Abgleich, Targeting) dies geschieht. Die spannende Frage ist, ob durch die Zusammenarbeit im DCR eine gemeinsame Verantwortlichkeit entsteht, insbesondere bei den Activation Use Cases, wo beide Parteien die Daten zusammenführen, um konkrete Personen (bzw. pseudonyme IDs) anzusprechen. Hierzu später mehr in Abschnitt 5. Bewertung der gemeinsamen Verantwortlichkeit.

Wichtig ist: Der DCR-Anbieter selbst (also die technische Plattform) ist in vielen Fällen ein Auftragsverarbeiter für die Parteien. Er stellt die Infrastruktur bereit und verarbeitet die Daten nur nach deren Weisung und festgelegten Regeln. Zwischen den Beteiligten und dem DCR-Dienstleister sind dann entsprechende Auftragsverarbeitungsverträge (Art. 28 DSGVO) abzuschließen.

2.3 Anwendungsbereich der DSGVO

Die DSGVO ist nur anwendbar, wenn personenbezogene Daten verarbeitet werden (Art. 2, Art. 4 Nr. 1 DSGVO). In DCRs wird häufig mit pseudonymisierten Daten gearbeitet – etwa mit gehashten E-Mail-Adressen. Wichtig: Pseudonymisierte Daten bleiben personenbezogene Daten, solange sie mit vertretbarem Aufwand wieder einer Person zugeordnet werden können. Für die Partei, die den Hash-Wert erzeugt hat, liegt in der Regel der Personenbezug vor (sie kennt den „Klarnamen“).

Im DCR-Kontext wird zwar oft von „anonymen“ Analysen gesprochen – durch doppelte Pseudonymisierung wird sichergestellt, dass die Beteiligten nicht direkt auf die Identität der jeweils anderen Betroffenen schließen können. Dennoch bleibt der Prozess, zumindest für die jeweiligen Parteien, die die Daten in den DCR selbst einbringen, in der Regel personenbezogen. Folglich müssen auch im DCR alle Datenschutzgrundsätze eingehalten werden, etwa Zweckbindung, Datensparsamkeit, Transparenz und Sicherheit. Die betroffenen Personen haben grundsätzlich Betroffenenrechte (Auskunft, Löschung etc.) gegenüber jedem Verantwortlichen.

Dazu noch ein Hinweis zur aktuellen Rechtsprechung: Der EuGH hat in der Rechtssache C-413/23 P (EDSB/SRB) festgestellt, dass der Personenbezug von Daten relativ zu beurteilen ist – d. h. aus der jeweiligen Perspektive der verarbeitenden Stelle und in Abhängigkeit von deren realistischen Möglichkeiten zur Re-Identifizierung. Zugleich hat der Gerichtshof klargestellt, dass die Pflichten aus der DSGVO bereits zum Zeitpunkt der Datenerhebung aus Sicht des Verantwortlichen entstehen und nicht durch nachträgliche Pseudonymisierung umgangen werden können.

Ob sich aus der Rechtsprechung ergibt, dass Daten, die aus der Perspektive des Verantwortlichen personenbezogen sind, diesen Status auch gegenüber gemeinsamen Verantwortlichen – unabhängig davon, ob der Zuordnungsschlüssel (also eine Re-Identifizierung bei allen Parteien möglich ist oder nicht) mitübermittelt wird – behalten, ist noch nicht abschließend geklärt. Entsprechendes gilt für den Auftragsverarbeiter. Vereinzelte Datenschutzaufsichtsbehörden haben in diesen Konstellationen die Anwendbarkeit der DSGVO bejaht. Innerhalb des Whitepapers gehen wir ebenfalls davon aus, dass der Anwendungsbereich der DSGVO eröffnet ist.

Nach abweichender Auffassung ist der Personenbezug auch bei gemeinsamer Festlegung der Mittel und Zwecke für jeden Akteur einzeln zu prüfen; Akteure, für welche die Daten keinen Personenbezug im Sinne von Art. 4 Nr. 1 DSGVO aufweisen, können danach definitionsgemäß keine (gemeinsam) Verantwortlichen im Sinne von Art. 4 Nr. 7 i.V.m. Art. 26 DSGVO sein.

Wenn pseudonymisierte Daten ohne Schlüssel an eine Organisation übermittelt werden, die weder gemeinsamer Verantwortlicher noch Auftragsverarbeiter ist, können diese jedenfalls als anonym zu qualifizieren sein, wenn eine Re-Identifizierung ausgeschlossen ist, mit der Folge, dass die DSGVO auf deren Verarbeitung durch diesen Empfänger keine Anwendung findet.

3. Use Cases im Überblick

Potentialanalyse

Der Use Case der Potenzialanalyse dient als vorgelagerter Schritt vor weiteren möglichen Use Cases (wie z. B. Aktivierung) und hat ausschließlich explorativen Charakter. Ziel ist es zunächst nicht, unmittelbar Werbekampagnen umzusetzen oder einzelne Nutzer*innen gezielt anzusprechen, sondern zu prüfen, ob zwischen den Datenbeständen der beteiligten Parteien überhaupt ein hinreichender Überschneidungsgrad besteht. Im Fokus steht damit die Frage, ob sich eine weitergehende Zusammenarbeit inhaltlich und wirtschaftlich lohnt.

Audience Insights

Hier kooperieren die Beteiligten, um Überschneidungen ihrer Nutzerbasis zu analysieren. Die Demand-Side möchte z. B. erfahren, welcher Anteil ihrer Kund*innen sich auf der Sell-Side wiederfindet und welche Merkmale diese gemeinsamen Nutzer*innen aufweisen (Interessen, Demografie usw.). Es geht um aggregierte Erkenntnisse, nicht um Einzelprofile – also eher Marktforschung als Werbung.

Activation – Re-Targeting

In diesem Szenario nutzt die Demand-Side den DCR, um gezielt ihre bestehenden Kund*innen oder Interessent*innen auf der Sell-Side anzusprechen. Vereinfacht: Zielgruppen, die auch Nutzer*innen bei der Sell-Side sind, sollen via DCR identifiziert und dann mit personalisierter Werbung auf der Sell-Side angesprochen werden.

Activation – Lookalike Audience (im DCR)

Hier werden mithilfe des DCR neue potenzielle Zielgruppen gefunden, die den bestehenden Zielgruppen der Beteiligten auf der Demand-Side ähneln. Dazu wird ein Lookalike-Modell innerhalb des DCR trainiert: Die gemeinsamen Kund*innen (Overlap) dienen als „Seed“, und anhand von deren Profilen identifiziert das Modell weitere ähnliche Zielgruppen. Die Selektion und Aktivierung dieser Lookalikes erfolgt innerhalb der DCR-Umgebung, sodass keine Rohdaten der neuen Zielgruppe direkt ausgetauscht werden.

Activation – Lookalike Audience außerhalb des DCR (Sell-Side Data Management Platform)

Dieser Anwendungsfall ähnelt dem vorherigen, jedoch wird das Lookalike-Modell außerhalb des DCR auf der Infrastruktur der Sell-Side angewendet (z. B. in der Data Management Platform, im nachfolgenden auch „DMP“). Der DCR dient hier nur zur initialen Identifikation der Overlap Audience (gemeinsame Zielgruppe). Anschließend erstellt die Sell-Side mit diesen Seeds in ihrem System eine erweiterte Audience von ähnlichen Zielgruppen. Die Aktivierung (Auspielung der Werbung) erfolgt dann ebenfalls über die Sell-Side-Systeme (z. B. über einen Ad-Server oder eine Demand-Side-Plattform, im nachfolgenden auch „DSP“).

In den folgenden Kapiteln werden wir jeden Use Case detailliert beleuchten: zunächst den technischen Datenfluss und dann die datenschutzrechtliche Bewertung (Anwendbarkeit der DSGVO, Rollen, Rechtsgrundlagen, Betroffenenrechte).

3.1 Use Case: Potenzialanalyse

In diesem Use Case nutzen die beteiligten Parteien den Data Clean Room zunächst ausschließlich zur Bewertung des grundsätzlichen Kooperationspotenzials. Ziel ist es, festzustellen, ob zwischen den jeweiligen Datenbeständen von Sell-Side und Demand-Side eine ausreichende Überschneidung besteht, um eine weitergehende Zusammenarbeit – etwa in Form von Audience Insights oder Activation Use Cases – sinnvoll erscheinen zu lassen. Eine unmittelbare Werbeansprache oder Zielgruppenaktivierung ist in dieser Phase ausdrücklich nicht vorgesehen.

Typischerweise möchte z. B. ein Werbungtreibender in einem ersten Schritt einschätzen, welcher Anteil seiner Kund*innen oder Interessent*innen grundsätzlich auf den Plattformen des Publishers erreichbar ist. Der Publisher wiederum kann bewerten, in welchem Umfang seine Nutzerbasis mit den Kundenbeständen potenzieller Werbepartner überlappt. Die Potenzialanalyse dient damit als vorgelagerte Entscheidungsgrundlage für eine weitere Zusammenarbeit und reduziert das Risiko, aufwendige Abstimmungen ohne ausreichende Datenbasis durchzuführen.

Datenflüsse und technische Verarbeitung:

Beide Parteien bereiten zunächst ihre Daten für den DCR vor. Konkret bedeutet das:

- **Pseudonymisierung der Identifikatoren:** Sowohl die Demand-Side als auch die Sell-Side wandeln die Identifikatoren ihrer Nutzer*innen in pseudonyme Werte um, beispielsweise durch das Hashing von E-Mail-Adressen oder Kundennummern. Häufig stellt der DCR-Anbieter hierfür entsprechende Tools oder einen sogenannten DCR-Bunker bereit, in dem die Rohdaten zunächst verschlüsselt und anschließend gehasht werden.

Hochladen der Daten in den DCR: Anschließend lädt jede Partei ihre pseudonymisierten Datensätze in die DCR-Umgebung. Die Datensätze der Beteiligten enthalten jeweils eine Liste von Hash-IDs.

- **Doppelte Pseudonymisierung / Matching:** Innerhalb des DCR erfolgt der Abgleich der beiden Datensätze. Die Plattform führt die Hash-Werte zusammen, um die Overlap Audience (gemeinsame Zielgruppe) zu ermitteln. Dabei kann eine erneute Pseudonymisierung stattfinden, indem der DCR intern einen neuen Identifier für jedes Match erzeugt, den weder Demand-Side noch Sell-Side ohne Weiteres zurückrechnen können. Lediglich der DCR (bzw. dessen Algorithmus) kennt die zugrunde liegende Verbindung.

- **Aggregation und Analyse:** Nachdem die Überlappung identifiziert wurde, werden aggregierte Kennzahlen berechnet. So kann beispielsweise ermittelt werden, dass von 100.000 vom Werbungtreibenden eingebrachten Kund*innen 20.000 auch im Datenbestand des Publishers enthalten sind.

- **Ergebnis:** Der Überschneidungsgrad zwischen den beiden Datensätzen beträgt in diesem Beispiel somit 20 %.

Die Ergebnisse der Potenzialanalyse werden den beteiligten Parteien ausschließlich in aggregierter Form zur Verfügung gestellt, beispielsweise als Kennzahlen oder einfache Übersichten. Rückschlüsse auf einzelne Personen oder die Identifikation konkreter Nutzer*innen sind nicht möglich und auch nicht Ziel dieses Use Cases.

Bewertung nach DSGVO:

Da personenbezogene Daten (pseudonymisierte IDs) verarbeitet werden, ist die DSGVO anwendbar. Die Ergebnisse (z. B. Statistiken) mögen teilweise anonym sein, aber der Weg dorthin involviert echte Nutzerdaten beider Parteien. Beide müssen also eine Rechtsgrundlage für die Datenverarbeitung und die Weitergabe der Daten untereinander haben und ihre Pflichten erfüllen.

Für reine Analysezwecke könnte ein berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO) ausreichen. Beide Parteien haben ein legitimes Interesse an der Feststellung, ob eine Zusammenarbeit in Frage kommt. Da zunächst nur ein begrenzter Umfang von Daten verwendet wird, sind die Risiken für die Betroffenen begrenzt. Wichtig wäre hier die Durchführung einer Interessenabwägung. Alternativ kann auch eine Einwilligung eingeholt werden.

In diesem Use Case ist keine gemeinsame Verantwortlichkeit im engeren Sinne zwingend. Jeder verarbeitet seine Daten selbstständig und erhält lediglich aggregierte Ergebnisse zurück. Die Verarbeitung dient in erster Linie der eigenen Abschätzung, ob es zu einer Zusam-

menarbeit kommen soll. Man kann argumentieren, dass Demand-Side und Sell-Side hier nicht gemeinsam den Zweck bestimmen, sondern jeweils eigene Zwecke verfolgen (Demand-Side: Analyse des Potenzials der Reichweite; Sell-Side: Wertanalyse des Inventars). Sie nutzen nur denselben Dienst (den DCR) parallel. Somit könnten beide als separate Verantwortliche agieren, die einen Datenaustausch via DCR vornehmen, ohne als „gemeinsam Verantwortliche“ im Sinne von Art. 26 DSGVO zu gelten. Der DCR-Anbieter wäre ein Auftragsverarbeiter für beide Seiten.

3.2 Use Case: Audience Insights

In diesem Use Case nutzen Demand-Side und Sell-Side den DCR zur Gewinnung von Insights über ihre überschneidende Nutzerbasis.

Ein Beispielszenario: Eine Agentur möchte wissen, welche demografischen Merkmale und Interessen der Kund*innen einer ihrer Klienten auf der News-Plattform eines Publishers aufweisen. Der Publisher wiederum interessiert sich ggf. dafür, wie wertvoll bestimmte Segmente seiner Nutzer*innen für Werbekund*innen sind. Wichtig: Es findet keine Werbeansprache oder individuelle Profilerweiterung statt – das Ergebnis sind aggregierte Statistiken.

Datenflüsse und technische Verarbeitung:

Beide Parteien bereiten zunächst ihre Daten für den DCR vor. Konkret bedeutet das:

- **Pseudonymisierung der Identifikatoren:** Sowohl die Demand-Side als auch die Sell-Side wandeln die Daten ihrer Nutzer*innen in pseudonyme Werte um (z. B. Hashing von E-Mail-Adressen oder Kundennummern). Oft stellt der DCR-Anbieter dafür Tools oder einen sogenannten DCR-Bunker bereit, in dem die Rohdaten verschlüsselt und dann gehasht werden.
- **Hochladen der Daten in den DCR:** Anschließend lädt jede Partei ihre pseudonymisierten Datensätze in die DCR-Umgebung. Der Datensatz der Sell-Side könnte etwa eine Liste von Hash-IDs enthalten, angereichert mit Attributen pro ID (z. B. Segmentzugehörigkeiten wie „Sport“, „Finance“ oder demografische Kategorien wie Altersgruppe und Geschlecht). Die Demand-Side lädt die Hash-IDs seiner Kund*innen oder Interessent*innen hoch, evtl. mit Eigeninformationen.
- **Doppelte Pseudonymisierung / Matching:** Im DCR erfolgt dann ein Abgleich der beiden Datensätze.
- **Aggregation und Analyse:** Nachdem die Überlappung identifiziert ist, werden aggregierte Kennzahlen berechnet. Zum Beispiel: Von den hochgeladenen 100.000 Kund*innen der Demand-Side wurden 20.000 bei der Sell-Side gefunden. Diese 20.000 verteilen sich auf die Publisher-Segmente wie folgt: 5.000 in „Sport“, 8.000 in „Finance“, 3.000 in „Fashion“ etc. Auch demografische Aufteilungen (falls vorhanden) können dargestellt werden, z. B. 60 % weiblich, 40 % männlich; größter Alterscluster 30–40 Jahre. Wichtig ist, dass dies ohne Nennung konkreter Personen geschieht – es handelt sich um Statistiken.
- **Ergebnisbereitstellung:** Die Demand-Side erhält Zugang zu den Audience Insights über die Zielgruppe auf der Sell-Side, meist in Form von Dashboards oder Berichten innerhalb des DCR-Tools. Die Sell-Side kann ebenfalls aggregierte Reports einsehen (z. B. wie sich die Zielgruppen in den Segmenten verhalten). Keiner der beiden erhält jedoch Einzeldatensätze der jeweils anderen Seite – nur zusammengefasste Informationen oder abstrahierte Werte. Die Beteiligten erhalten Zugriff jeweils nach Freigabe der anderen Partei.

Bewertung nach DSGVO:

Je nach Tiefe und Ausgestaltung der Analyse kann hier noch die Rechtsgrundlage des berechtigten Interesses, Art. 6 Abs. 1 lit. f) DSGVO, herangezogen werden oder bereits eine Einwilligung notwendig sein. Hier kommt es entscheidend auf die Anzahl der Parameter und

die angestrebten Rückschlüsse und Einblicke über die jeweiligen Betroffenen an. Ebenso kann die Erwartungshaltung der Betroffenen eine wichtige Rolle spielen.

In diesem Use Case liegt in der Regel eine gemeinsame Verantwortlichkeit vor. Demand-Side und Sell-Side bestimmen hier gemeinsam den Zweck und die Mittel und nutzen den DCR als Auftragsverarbeiter.¹

Verarbeitungsschritte und Rollen – Use-Case-Audience Insights		
Verarbeitungsschritt	Sell-Side – Rolle/Aktion	Demand-Side – Rolle/Aktion
Datenerhebung	Erhebt Nutzerdaten (z. B. Login-E-Mails, Nutzungsprofile) – Verantwortlicher für eigene Nutzerdaten.	Erhebt Kundendaten (z. B. E-Mails, CRM-Daten) – Verantwortlicher für eigene Kundendaten.
Pseudonymisierung	Pseudonymisiert eigene Nutzer-IDs (z. B. Hash der E-Mails)	Pseudonymisiert eigene Kunden-IDs (z. B. Hash der E-Mails)
Datenbereitstellung im DCR	Stellt pseudonymisierte Datensätze (IDs + Attribute) in dem DCR zur Verfügung – auf Basis eines AV-Vertrags mit dem DCR-Anbieter.	Stellt pseudonymisierte Kunden-IDs (ggf. mit eigenen Merkmalen) im DCR zur Verfügung – ebenfalls auf Basis eines AV-Vertrags mit dem DCR-Anbieter.
Matching & Analyse	(Im DCR): der DCR führt den Abgleich durch. Die Sell-Side hat keine Einsicht in Demand-Side-Daten währenddessen.	(Im DCR): DCR führt Matching durch. Keine Einsicht in Sell-Side-Rohdaten.
Ergebnis / Insights erhalten	Erhält vom DCR aggregierte Reports (z. B. % Überschneidung in Segmenten) – nutzt diese für eigene Zwecke (Analysen, Sales-Strategie). Verantwortlich für die Ergebnisauswertung.	Erhält vom DCR aggregierte Insights über eigene Kund*innen (z. B. demografische Verteilung auf Publisher-Seite) – interne Nutzung. Verantwortlich für die Ergebnisverwertung.
Nutzung der Ergebnisse	Verwendet aggregierte Erkenntnisse zur Planung von Werbeangeboten oder Zielgruppenauswahl.	Nutzt Erkenntnisse für Marketingplanung (z. B. Segmentüberschneidungen mit Publisher-Publikum).

¹ Vorbehalten bleibt die abweichende Auffassung unter Ziff. 2 c) und Ziff. 5, wonach Sell-Side und Demand-Side für die Verarbeitung ihrer jeweiligen Daten im DCR als eigenständige Verantwortliche agieren.

3.3 Use Case: Activation – Retargeting

Ziel des Retargetings ist, dass die Demand-Side ihre bestehenden Kund*innen gezielt auf der Sell-Side erneut anspricht. Beispiel: Ein E-Commerce-Anbieter möchte Personen, die bei ihm etwas gekauft haben, auf der Nachrichten-Website des Publishers mit Werbung für ein ergänzendes Produkt erreichen. Die gemeinsamen Nutzer*innen werden identifiziert und anschließend gezielt beworben.

Datenflüsse und technische Verarbeitung:

Der initiale Prozess ähnelt dem Potenzialanalyse-Use-Case, mit dem Unterschied, dass am Ende konkrete Identifier zur Werbeansprache generiert werden:

- **Vorbereitung der Daten:** Wieder pseudonymisieren beide Parteien ihre Identifier. Falls für das Targeting relevant, kann die Sell-Side zusätzlich Verhaltensdaten (z. B. Interessenkategorien) bereitstellen.

Matching: Die Demand-Side stellt die Hashes ihrer Zielgruppe in den DCR bereit; die Sell-Side stellt die Hashes aller aktiven Nutzer*innen (oder ihrer registrierten Nutzer*innen) bereit. Im DCR werden die Overlap-Nutzer*innen ermittelt, d. h. diejenigen Hash-IDs, die in beiden Mengen vorkommen. Das sind genau die Nutzer*innen, die bei beiden bekannt sind – und somit von der Demand-Side auf der Sell-Side erreichbar wären.

- **ID:** Nach dem Abgleich erzeugt der DCR für jeden gefundenen Overlap eine ID (man kann es sich als neuen Schlüssel vorstellen). Nach dem Abgleich markiert der DCR für jeden gefundenen Overlap eine ID in dem jeweiligen Data Set. Die Markierungen im jeweiligen Data Set bilden letztlich das Targeting-Segment für die Kampagne.
- **Export/Integration für Ad-Ausspielung:** Nun muss dieses Segment in die Werbeausspielung gebracht werden. Hier gibt es verschiedene Ansätze:

Demand-Side-Aktivierung: Die Demand-Side kann die IDs in ihre DSP einspeisen, um nur diese Nutzer*innen anzusprechen. In der Praxis müssten die DSP und die Sell-Side eine gemeinsame ID-Basis haben – denkbar ist, dass die ID z. B. mit einem Login-basierten Identifier des Publishers verknüpft ist. Oft übernimmt der DCR-Anbieter oder die Sell-Side die Aufgabe, das Segment ins Ad-System zu überführen.

Sell-Side-Aktivierung: Alternativ erstellt die Sell-Side auf einem Ad-Server oder in ihrer DMP ein privates Segment mit diesen IDs. Die Ausspielung erfolgt dann so, dass nur Nutzer*innen, die zu diesem Segment gehören, die spezifische Demand-Side-Werbung sehen. Die Demand-Side bucht dieses Segment bei der Sell-Side für die Kampagne.

Bewertung nach DSGVO

Retargeting greift deutlich stärker in die Privatsphäre der Betroffenen ein als eine reine Analyse. Hier werden individuelle Nutzer*innen gezielt angesprochen, basierend auf der Zusammenführung ihrer Daten aus zwei Quellen.

In den meisten Fällen wird man für DCR Retargeting eine informierte Einwilligung der Nutzer*innen benötigen. Die Sell-Side sollte im Consent-Banner den Zweck der personalisierten Werbung (auch mit Partnerdatenabgleich) enthalten und nur Nutzer*innen im DCR abgleichen, die dem zugestimmt haben. Der Hash ihres Identifiers würde dann nur bei Consent gebildet/weitergegeben. Auch die Demand-Side muss ihre Zielgruppe informieren und deren Einwilligung einholen, dass die Daten für personalisierte Werbung bei Dritten genutzt werden. Falls die Daten ursprünglich im Rahmen eines Kaufs erhoben wurden, reicht die Vertragserfüllungsgrundlage nicht automatisch für die nachgelagerte Verarbeitung.

Bei Retargeting sind Demand-Side und Sell-Side gemeinsame Verantwortliche im Sinne von Art. 26 DSGVO. Beide entscheiden gemeinsam, dass bestimmte Personen identifiziert und

mit Werbung angesprochen werden: Die Sell-Side stellt ihre Nutzerdaten und ihre Werbeplattform bereit, die Demand-Side initiiert die Kampagne und definiert die Zielgruppe (ihre eigenen Kund*innen). Ohne diese Kooperation käme die Verarbeitung nicht zustande. Damit legen beide den Zweck – gezielte Werbung an gemeinsame Kund*innen – gemeinsam fest. Folglich sollten Sell-Side und Demand-Side ein Joint Controller Agreement (JCA) schließen. Zusätzlich zum JCA zwischen Sell-Side und Demand-Side bleibt der DCR-Anbieter Auftragsverarbeiter. Mit ihm wird jeder separat einen AV-Vertrag haben, der sicherstellt, dass die Daten im DCR nur für den definierten Zweck (Matching und Segmentbildung) genutzt werden.

Verarbeitungsschritte und Verantwortlichkeiten – Use-Case Activation (Retargeting)		
Verarbeitungsschritt	Sell-Side – Rolle/Aktion	Demand-Side – Rolle/Aktion
Consent & Datenerhebung	Holt Nutzer-Einwilligung auf seiner Plattform ein („Datenabgleich zu Werbezwecken“); markiert nur einwilligende Nutzer*innen zur Teilnahme. Verantwortlich für eigene Nutzerdaten inkl. Consent-Management.	Holt Einwilligung von Kund*innen ein und informiert über Nutzung der Daten zu Werbezwecken auf Drittplattformen. Verantwortlich für eigene Kundendaten.
Pseudonymisierung	Hasht die IDs der einwilligenden Nutzer*innen und lädt diese mit ggf. Werbe-IDs in den DCR. Gibt keine Klardaten heraus.	Hasht Kunden-IDs, lädt sie in den DCR. Keine Weitergabe von Klardaten.
Matching im DCR	Stellt Daten bereit, DCR führt Abgleich durch. Beide Parteien wirken gemeinsam am Abgleich mit, legen Matching-Kriterien fest. Gemeinsame Verantwortlichkeit; DCR = Auftragsverarbeiter.	Siehe links – Matching-Prozess gemeinsam mit Sell-Side abgestimmt. Auch hier gemeinsame Verantwortlichkeit.
Segment-Erstellung (Activation IDs)	Erhält vom DCR pseudonyme Activation IDs (Overlap User) und erstellt daraus ein Segment im eigenen Ad-System. Verantwortlich für die Ad-Aussteuerung an diese IDs.	Nutzt typischerweise nur die Möglichkeit, im DSP auf das Segment zu bieten. Gemeinsame Verantwortlichkeit bzgl. Zielgruppendefinition und Werbeansprache.
Werbeausspielung	Spielt die Werbung an Segment-Nutzer*innen auf der Website aus. Verantwortlich für die Auslieferung. Bei gemeinsam definiertem Zweck: Mitverantwortlichkeit mit Demand-Side.	Verantwortlich für Werbeinhalte und Kampagnenparameter. Mitverantwortlich für Auswahl der Zielgruppe, wenn gemeinsam festgelegt.

3.4 Use Case: Activation – Lookalike Audience (im DCR)

Beim Lookalike-Use-Case möchte die Demand-Side neue Zielgruppen erreichen – also Personen, die sie bisher nicht als Kund*innen hat, die aber ihren bestehenden Kund*innen ähneln und daher mit hoher Wahrscheinlichkeit ebenfalls interessiert sind. Der DCR kann auch hierfür eingesetzt werden. Die Identifikation der ähnlichen Zielgruppen erfolgt mittels Machine

Learning – also Algorithmen, die aus bestehenden Daten Muster lernen und auf neue Fälle anwenden. Die Berechnung kann entweder direkt im DCR stattfinden oder auf der Infrastruktur der Sell-Side.

Modelltraining und Anwendung im DCR:

Technisch lässt sich der Prozess so zusammenfassen:

- **Seed Audience definieren:** Zunächst wird wieder die Overlap Audience zwischen Demand-Side und Sell-Side bestimmt, ähnlich wie beim Retargeting. Diese gemeinsamen Nutzer*innen dienen als Trainingsdaten (positive Beispiele). Gegebenenfalls könnten auch Nicht-Overlap-Nutzer*innen als negative Beispiele herangezogen werden (je nach Modellansatz).
- **Feature-Bereitstellung:** Die Sell-Side speist zusätzlich Attribute/Merkmale ihrer Nutzer*innen in den DCR ein, damit das Lookalike-Modell etwas zum Analysieren hat. Das können sein: besuchte Kategorien, Interessenprofile, demografische Daten, Kaufverhalten etc. Diese Features liegen pro Nutzer*in als pseudonymisierte Profilinformationen vor.
- **Trainieren des Lookalike-Modells:** Innerhalb des DCR (z. B. in einer separaten sicheren Umgebung) wird ein Algorithmus ausgeführt, der die Charakteristika der Overlap User gegenüber anderen Nutzer*innen herausarbeitet. Zum Beispiel könnte ein Modell feststellen: Verbraucher*innen sind überproportional häufig an Sport- und Finanz-Inhalten interessiert und meist im Alter 30–40, während sie seltener z. B. Gaming-Interessen zeigen. Das Modell könnte maschinelles Lernen oder statistische Scoring-Methoden nutzen. Wichtig: Die Rohdaten verlassen den DCR nicht – das resultierende Modell kann als mathematische Funktion oder Regelset innerhalb des DCR verbleiben.
- **Anwenden des Modells (Scoring):** Im nächsten Schritt wird dieses Modell auf die gesamte Sell-Side-Nutzerdatenbasis angewendet. Das heißt, alle pseudonymisierten Sell-Side-IDs werden durch das Modell bewertet (gescored), um diejenigen herauszufiltern, die dem „Idealprofil“ der Demand-Side am nächsten kommen. Das Ergebnis ist eine Lookalike Audience: eine Liste von pseudonymen User-IDs, die nicht zur bestehenden Zielgruppe auf der Demand-Side gehören (weil diese ja als Seeds schon identifiziert wurden), aber ähnliche Merkmale aufweisen. Die Größe dieser Audience kann je nach gewünschter Reichweite eingestellt werden.
- **Aktivierung der Lookalikes:** Anschließend wird – analog zum Retargeting – für diese neuen IDs wieder ein Segment erstellt. Die Werbekampagne wird dann auf diese IDs ausgerichtet.

Datenschutzrechtliche Bewertung:

Auch hier agieren Sell-Side und Demand-Side im Verbund, um den Zweck „Erweiterung der Zielgruppe um ähnliche Nutzer*innen“ zu erreichen. Das spricht für gemeinsame Verantwortlichkeit. Die Demand-Side bringt den initialen Zweck ein (neue Kund*innen finden, die ähnlich zu den bestehenden sind), die Sell-Side entscheidet mit, indem sie ihr Datenmaterial und die Plattform dafür bereitstellt. Beide legen gemeinsam die Kriterien fest (z. B. wie streng die Ähnlichkeit definiert wird, welche Attribute genutzt werden dürfen). In der Praxis wird die Sell-Side meist die technische Hoheit haben, das Modell zu trainieren (entweder selbst oder über das DCR-Tool). Aber die Demand-Side muss zustimmen und profitiert direkt. Folglich: ein Joint-Controller-Setup analog zum Retargeting, da nun auch Nutzer*innen betroffen sind, die bisher nur im Sell-Side-Universum waren.²

Die Sell-Side muss von den Nutzer*innen eine Einwilligung eingeholt haben, die auch eine solche Profilbildung und Weitergabe umfasst. Die Demand-Side selbst kann von diesen Personen keine Einwilligung haben (sie hatte ja keinen Kontakt), aber sie muss sich auf die Einwilligung stützen, die die Sell-Side (und ggf. der DCR-Anbieter) für die gemeinsame Verarbeitung eingeholt hat. Praktisch muss also im Joint Controller Agreement klar vereinbart sein,

² Vorbehalten bleibt die abweichende Auffassung unter Ziff. 2 c) und Ziff. 5, wonach Sell-Side und Demand-Side für die Verarbeitung ihrer jeweiligen Daten im DCR als eigenständige Verantwortliche agieren.

dass die Sell-Side für die Einholung der Nutzerzustimmung zuständig ist. Zusätzlich muss die Demand-Side sicherstellen, dass die Nutzung ihrer Kundendaten zur Modellierung durch die Sell-Side von ihrer Kundeneinwilligung gedeckt ist.

Lookalike Profiling könnte eine Datenschutz-Folgenabschätzung (im nachfolgenden auch „DSFA“) erfordern, da hier Daten zusammengeführt und neue Vorhersagen über Personen getroffen werden, was in Art. 35 DSGVO als Risikoverarbeitung kategorisiert sein kann. Unternehmen sollten prüfen, ob eine DSFA nötig ist, und diese durchführen, um die Risiken (z. B. Diskriminierung, Intransparenz) zu bewerten und zu mitigieren.

Verarbeitungsschritte und Verantwortlichkeiten – Activation (Lookalike im DCR)		
Verarbeitungsschritt	Sell-Side – Rolle/Aktion	Demand-Side – Rolle/Aktion
Consent & Datenerhebung	Holt Einwilligung für Profilbildung (inkl. Lookalike). Bereitet pseudonymisierte Profile (IDs + Attribute) für den DCR auf.	Holt Einwilligung zur Analyse/Kooperation. Stellt pseudonymisierte Kunden-IDs bereit. Verantwortlich für die eigenen Daten.
Overlap-Ermittlung (Seed)	DCR führt Matching durch (wie bei Retargeting). Sell-Side und Demand-Side bestimmen gemeinsam, welche Nutzer*innen als Seed dienen. Gemeinsame Verantwortlichkeit für den Abgleich.	Siehe links – gemeinsame Verantwortlichkeit bei Abgleich & Seed-Auswahl.
Modell-Training	Modell wird im DCR trainiert. Sell-Side entscheidet mit, welche Attribute zulässig sind. Mitverantwortlich, da Modell auf seinen Daten basiert.	Gibt Ziele/Anforderungen an das Modell vor (z. B. Zielgruppen-Definition). Technische Ausführung liegt bei Sell-Side/DCR. Bleibt mitverantwortlich für Modellzweck (Neukundengewinnung).
Modellanwendung (Scoring)	Modell wird auf alle pseudonymen Nutzer*innen angewendet. Sell-Side achtet auf sachliche Richtigkeit und dass nur Nutzer*innen mit Consent einbezogen sind. Verantwortlich für Anwendung des Modells auf seine Datenbasis.	Nimmt aktiv nicht teil, ist aber mitverantwortlich für Entscheidung zur Durchführung des Modell-Scorings. Joint Controller für diesen Zweck.
Segment/Audience-Erstellung	Erhält vom DCR pseudonyme Activation IDs (Lookalikes). Erstellt daraus ein Werbesegment im Ad-Server/DSP. Verantwortlich für den Einsatz in der Werbung.	Erhält typischerweise nur aggregierte Informationen (z. B. Reichweite). Initiiert Kampagne auf das Lookalike-Segment. Mitverantwortlich für zulässige Nutzung der Ergebnisse.
Werbeausspielung	Spielt Werbung an Lookalike-User aus. Ist Verantwortlicher für die Werbeauslieferung auf seiner Plattform.	Definiert Inhalte und Ziele der Anzeige. Ist verantwortlich für Kampagneninhalte.

3.5 Use Case: Activation – Lookalike außerhalb DCR

In einigen Fällen entscheiden sich Sell-Side und Demand-Side dafür, den Lookalike-Prozess außerhalb des DCR durchzuführen, insbesondere wenn die Sell-Side über eine leistungsfähige eigene Data Management Platform (DMP) oder ähnliche Systeme verfügt. Der DCR wird dann nur genutzt, um die Overlap Audience sicher zu ermitteln; danach verlässt man sich auf die Tools der Sell-Side. Dies kann z. B. der Fall sein, wenn die Sell-Side ihre gesamten Nutzerdaten gar nicht in einen externen DCR laden möchte oder wenn die Demand-Side einer Lösung zustimmt, die auf dem etablierten System der Sell-Side aufsetzt.

Unterschied zum Lookalike-Modell im DCR:

Der Hauptunterschied ist, dass das Lookalike-Modell in der Sell-Side DMP läuft statt im DCR. Das hat mehrere Implikationen:

Datenfluss:

Zunächst werden wie gehabt die gemeinsamen Nutzer*innen (Overlap) im DCR identifiziert. Diese Overlap-IDs werden dann jedoch der Sell-Side offenbart – zumindest insofern, als die Sell-Side sie in ihrem eigenen System als „Seed“ markieren muss. Praktisch könnte der DCR der Sell-Side z. B. eine Datei mit pseudonymen internen IDs liefern, die den Overlap darstellen. Da die Sell-Side diese IDs aus ihrem eigenen Nutzerstamm erkennt, kann sie sie nun in ihrer DMP als Segment „Demand-Side-X-Zielgruppe“ anlegen. Das bedeutet, die Sell-Side weiß jetzt konkret, welche ihrer Nutzer*innen Zielgruppe der Demand-Side sind.

- **Modellierung in der DMP:** Die Sell-Side führt dann in ihrer DMP oder Analytics-Plattform eine Lookalike-Berechnung durch. Das ist technisch ähnlich wie im DCR, nur dass es in ihrer eigenen Umgebung geschieht. Sie kann dabei auf alle möglichen internen Daten zugreifen und andere Algorithmen nutzen, die der DCR nicht bietet.
- **Generierung der Lookalike Audience:** Die DMP erstellt ein neues Segment. Dieses Segment enthält eine Anzahl von Sell-Side-Nutzer*innen (durch interne IDs oder Cookies identifizierbar), die das Modell als ähnlich eingestuft hat.
- **Aktivierung:** Die Sell-Side kann dieses Segment nun im Ad-Server nutzen oder der Demand-Side anbieten, darauf zu bieten.

Nachdem die Seeds einmal aus dem DCR entnommen wurden, ist der DCR selbst nicht mehr beteiligt. Die Zusammenarbeit läuft nun bilateral zwischen Sell-Side (die die neuen Nutzer*innen anspricht) und Demand-Side (die die Ads liefert/bucht).

Datenschutzrechtliche Bewertung

Hier liegt eine gemeinsame Verantwortlichkeit vor, da das letztliche Ziel – neue Lookalikes zu finden und zu targeten – gemeinsam verfolgt wird. Allerdings verschiebt sich die operative Verantwortlichkeit stärker zur Sell-Side: Sie übernimmt den gesamten Modellierungsvorgang eigenständig in ihrer Umgebung.

Es braucht im Ergebnis eine Einwilligung.

Verarbeitungsschritte und Verantwortlichkeiten – Activation (Lookalike außerhalb DCR)		
Verarbeitungsschritt	Sell-Side – Rolle/Aktion	Demand-Side – Rolle/Aktion
Consent & Overlap-Abgleich	Holt Einwilligung wie zuvor ein. Stellt IDs dem DCR zur Verfügung, erhält Activation IDs der Overlap-Nutzer*innen. Gemeinsame Verantwortung mit Demand-Side (Joint Control) für Matching.	Liefert pseudonymisierte Kunden-Hashes an den DCR, autorisiert Matching. Ebenfalls Joint Control für diesen Abgleichsschritt.
Übertragung Seeds an DMP	Importiert Overlap IDs in eigene DMP oder internes System. Trägt Verantwortung für diesen Datenimport (vertraglich gedeckt).	Überlässt Daten (pseudonymisiert) der Sell-Side zu Lookalike-Zwecken.
Lookalike-Modellierung (DMP)	Führt Lookalike-Berechnung eigenständig im DMP durch (Eigene Algorithmen, Kriterien, Umfang).	Gibt Input zu Zieldefinition (z. B. Reichweite), hat aber operativ keine Kontrolle.
Neue Audience-Erstellung	Erstellt das Lookalike-Segment im DMP (basierend auf eigenen IDs mit Consent). Verantwortlich für Segmentqualität und Konformität.	Erhält ggf. Rückmeldung über Segmentverfügbarkeit.
Werbeausspielung	Erkennt bei Besuch, ob Nutzer*in im Lookalike-Segment ist und zeigt entsprechend Werbung. Kennt die Nutzer*innen im Segment, trägt Verantwortung für Ausspielung und Segmentkontrolle.	Bucht Kampagne auf das Segment. Verantwortlich für Werbeinhalte.

4. Vertragliche Rahmenbedingungen

Weil die Rollenverteilungen in DCR-Use-Cases komplex sind, sind vertragliche Vereinbarungen zwischen den Beteiligten unerlässlich, um Übersichtlichkeit hinsichtlich der Rechte und Pflichten herzustellen. Im Folgenden werden die wichtigsten Verträge skizziert, die in den geschilderten Szenarien abgeschlossen werden sollten, sowie besondere Herausforderungen wie die Interoperabilität verschiedener DCR-Systeme.

Joint Controller Agreement (Art. 26 DSGVO): Immer dann, wenn Sell-Side und Demand-Side als gemeinsam Verantwortliche anzusehen sind, sollten beide in transparenter Form festlegen, wer welche Pflichten erfüllt. Ein sogenanntes Joint Controller Agreement (JCA) regelt unter anderem:

- **Zwecke und Mittel:** Es wird dokumentiert, für welche konkreten Zwecke die Parteien gemeinsam Daten verarbeiten (z. B. „Abgleich und Targeting gemeinsamer Kund*innen zur personalisierten Werbung“) und welche Mittel/Technologien dafür eingesetzt werden (z. B. Nutzung DCR XYZ).

- **Aufgabenteilung bei Informationspflichten:** Typischerweise übernimmt die Sell-Side (in der Regel der Publisher) die Erstinformation der Nutzer*innen (da er den Kontakt über Website/App hat), und die Demand-Side ergänzt Informationen in ihrer eigenen Datenschutzerklärung hinsichtlich der Kooperation. Im JCA wird festgelegt, dass der wesentliche Inhalt der Vereinbarung den Betroffenen zur Verfügung gestellt wird (Art. 26 Abs. 2 DSGVO) – praktisch z. B. durch einen Hinweis in der Privacy Policy à la „Wir arbeiten mit ausgewählten Partnern in sogenannten Data Clean Rooms zusammen...“.
- **Betroffenenrechte und Anlaufstellen:** Es muss entschieden werden, wie z. B. Auskunftersuchen gehandhabt werden. Häufig vereinbart man, dass jeder Verantwortliche für Anfragen zu den eigenen Daten zuständig ist, aber sie sich gegenseitig unterstützen. Aus Nutzersicht sollte es egal sein, an wen er sich wendet. In der Praxis wird wohl derjenige, der den direkten Kundenkontakt hat, auch das Verfahren hauptsächlich bearbeiten.
- **Verteilung der Verantwortlichkeit bei Verstößen**
- **Laufzeit, Beendigung, Zweckbindung:** Die JCA sollten regeln, wie lange die Kooperation läuft, was mit erhobenen Daten danach geschieht (Löschung oder Rückgabe), und dass die Daten nur für den gemeinsam festgelegten Zweck genutzt werden dürfen.

Auftragsverarbeitungsverträge (Art. 28 DSGVO): In praktisch allen Szenarien tritt ein Dritter als Dienstleister auf – der DCR-Anbieter. Mit diesem muss jede Partei einen Auftragsverarbeitungsvertrag (im nachfolgenden auch „AVV“) schließen, sofern der DCR nur als weisungsgebundener Verarbeiter agiert. Übliche Inhalte: die Beschreibung der verarbeiteten Daten (z. B. Kundendaten, Nutzungsdaten), der Umfang und Zweck (z. B. „Abgleich zweier Datensätze und Bereitstellung aggregierter Ergebnisse/Segmente“) sowie Verpflichtungen des Dienstleisters zu Vertraulichkeit, Sicherheitsmaßnahmen, Unterstützung bei Betroffenenrechten, Audits etc. Jeder DCR-Anbieter wird solch einen Standard-AVV vorhalten.

Sell-Side und Demand-Side schließen idealerweise jeweils separat einen AVV mit dem DCR-Anbieter ab. Der DCR muss intern sicherstellen, dass die Daten der beiden Parteien nur so verarbeitet werden, wie von beiden autorisiert. In manchen Fällen könnte der DCR-Anbieter argumentieren, er sei ein „neutraler Treuhänder“ und vielleicht gar kein reiner Auftragsverarbeiter, aber in der Regel wird man ihn als Auftragsverarbeiter behandeln, um Klarheit zu haben.

Vertragslogik bei Nutzung durch Agenturen: Häufig beauftragt ein Werbungtreibender eine Media-Agentur, die für ihn Kampagnen durchführt und ggf. auch den DCR-Prozess operativ bedient. Hier entstehen weitere Verträge:

- **Werbungtreibender ↔ Agentur:** Die Agentur kann entweder als Auftragsverarbeiter des Werbungtreibenden agieren (wenn sie weisungsgebunden nur für ihn Daten managt), oder als eigenständiger (Mit-)Verantwortlicher, wenn sie z. B. mehrere Kunden-Datenpools verwaltet und eigene Entscheidungen trifft. Oft wird die Agentur als AV im datentechnischen Sinne gesehen, da sie Kundendaten nur im Auftrag nutzt. Dann braucht es einen AVV zwischen Werbungtreibendem und Agentur.
- **Agentur ↔ Publisher:** Direkt eigentlich kein Vertrag in Bezug auf personenbezogene Daten, denn die Agentur erhält die Publisher-Daten nicht. Sie könnte aber als Vermittler in der Joint-Controller-Vereinbarung mitbenannt werden, falls sie Prozesse steuert. Meist wird das nicht getan – die Agentur handelt im Auftrag des Werbungtreibenden, also deckt der Vertrag zwischen Werbungtreibendem und Agentur das ab. Die Joint-Controller-Vereinbarung bleibt zwischen Werbungtreibendem und Publisher.
- **Geheimhaltung:** Zwischen allen Parteien sollten Vertraulichkeitsverpflichtungen vereinbart werden, da sensible Geschäfts- und Nutzerinformationen ausgetauscht werden. Diese können entweder als gesonderter NDA abgeschlossen oder als Geheimhaltungsklauseln in die bestehenden Verträge (JCA, AVV, Agenturvertrag, etc.) integriert werden.

- **Agentur ↔ DCR-Anbieter:** Die Agentur könnte als Vertreter des Werbungtreibenden im DCR agieren. Hier muss vertraglich geklärt sein, dass die Agentur befugt ist, für den Werbungtreibenden zu handeln (z. B. im AVV mit dem DCR-Anbieter in Unterauftragskonstellation). Diese Konstellationen sollten im Vertrag zwischen Werbungtreibendem und Agentur sauber adressiert werden (Stichwort: Unterauftragsverarbeiter).

5. Bewertung der gemeinsamen Verantwortlichkeit

Ein zentrales Thema bei DCR Use Cases ist die Frage: Wann liegt gemeinsame Verantwortlichkeit zwischen den beteiligten Unternehmen vor und wann nicht? Die Antwort bestimmt, ob Art. 26 DSGVO greift und wie die rechtlichen Pflichten verteilt sind. Schauen wir uns zur Bewertung nochmals die Use Cases unter diesem Aspekt an.

Die DSGVO definiert gemeinsame Verantwortliche als solche, die „gemeinsam die Zwecke und Mittel der Verarbeitung“ festlegen (Art. 26 Abs. 1 Satz 1 DSGVO).

„Gemeinsam“ ist dabei nicht als gleichberechtigte Mitbestimmung zu verstehen. Es reicht aus, wenn die Entscheidungen zweier Stellen einander ergänzen und für die Verarbeitung personenbezogener Daten so erforderlich sind, dass sie einen spürbaren Einfluss auf deren Durchführung nehmen. Eine ausdrückliche Koordinierung oder formelle Kooperation ist nicht nötig; es genügt, wenn die Verarbeitung ohne die Beteiligung beider Parteien schlicht nicht möglich wäre und jede Partei von den Beiträgen der anderen weiß und diese billigt. Auch muss keine Partei Zugang zu den personenbezogenen Daten der anderen haben: Schon das Initiieren des Abgleichprozesses kann ausreichen.³ Die Verantwortlichkeit kann zudem asymmetrisch sein – ein Partner kann mehr Einblicke oder Einfluss haben als der andere, und dennoch sind beide verantwortlich.

Bei den Activation-Szenarien, insbesondere Retargeting und Lookalike, sprechen folgende Gründe für gemeinsame Verantwortlichkeit:

- **Gemeinsamer Zweck:** Beide Parteien wollen konkret bestimmte Personen mit Werbung ansprechen. Das ist ein klar umrissener Zweck (personalisierte Werbung für Demand-Side durch Sell-Side-Plattform), der nur gemeinsam erreicht werden kann. Keiner könnte allein dieses Ziel verwirklichen, es bedarf der Kooperation.
- **Verzahnte Mittel:** Die Mittel (Datenabgleich, Segmentbildung, Ausspielung) werden zwischen den Parteien abgestimmt. Die Demand-Side liefert die Datenbasis (ihre Kundenliste), die Sell-Side liefert ihre Nutzerprofilbasis, der DCR/die DMP wird gemeinsam genutzt, und am Ende findet auf der Sell-Side-Infrastruktur die Ansprache statt, wofür aber die Demand-Side die Werbemittel liefert. Diese Verkettung ist ein Indiz dafür, dass sie zusammenwirken wie ein einheitlicher Prozess, auch wenn intern Aufgabenteilung herrscht.

³ Die in der Rechtsprechung entwickelte Aussage, eine gemeinsame Verantwortlichkeit setze keinen Zugang zu den Daten voraus (EuGH, C-210/16 – Wirtschaftsakademie; C-40/17 – Fashion ID), betrifft nach der unter Ziff. 2.c. erwähnten abweichenden Ansicht die Frage der datenschutzrechtlichen Rolle und nicht die vorgelagerte Frage, ob die Daten aus Sicht des jeweiligen Akteurs überhaupt personenbezogen sind. Fehlender Zugang und fehlender Personenbezug können nach dieser Ansicht dogmatisch verschiedene Kategorien sein: Wer über rechtlich-realistische Mittel zur Identifizierung verfügt, kann auch ohne unmittelbaren Datenzugang Personendaten verarbeiten; umgekehrt folgt aus der Entbehrlichkeit des Zugangs nicht, dass der Personenbezug aus Sicht des betreffenden Akteurs unerheblich wäre.

- **Beidseitiger Nutzen:** Die Demand-Side erreicht Person X mit ihrer Werbung, die Sell-Side verdient an Person X durch die geschaltete Werbung. Die Daten von Person X (dass sie Kund*in ist, dass sie angesprochen wird) stehen im Zentrum. Nach Auffassung der Gerichte begründet schon das gemeinsame Profitieren von einer personenbezogenen Datenverarbeitung eine Mitverantwortlichkeit – man muss dafür nicht gleichen Zugriff haben; es reicht, dass jeder das Seine beiträgt.⁴

Dennoch bleibt wichtig: Gemeinsame Verantwortlichkeit heißt nicht, dass beide für alle Prozesse gemeinsam verantwortlich sind. Intern muss klar sein:

- **Die Sell-Side** ist insbesondere für alles verantwortlich, was mit ihren Nutzerprofilen und der Ausspielung zu tun hat.
- **Die Demand-Side** ist verantwortlich für ihre Kundendaten.
- **Im Überschneidungsbereich** (Matching, Segmentbildung, Auswahl der Zielgruppe) sind sie gemeinsam verantwortlich.

Aus der gemeinsamen Verantwortlichkeit folgen vier praktische Konsequenzen: Erstens ist die Art. 26-DSGVO-Vereinbarung (im Nachfolgenden auch „JCA“) keine Voraussetzung der gemeinsamen Verantwortlichkeit, sondern deren Rechtsfolge – sie muss also nach Feststellung der gemeinsamen Verantwortlichkeit abgeschlossen werden, kann diese aber weder begründen noch ausschließen. Zweitens besteht zwischen gemeinsam Verantwortlichen kein Verarbeitungsprivileg: Jede Datenübermittlung zwischen ihnen – etwa die Übergabe gehashter ID-Listen vor dem Matching – bedarf einer eigenständigen Rechtsgrundlage nach Art. 6 DSGVO. Drittens haftet jeder gemeinsam Verantwortliche im Außenverhältnis grundsätzlich gesamtschuldnerisch (Art. 82 Abs. 4 DSGVO); Bußgelder hingegen werden nach dem jeweiligen individuellen Verantwortlichkeitsanteil verhängt (Art. 83 DSGVO). Viertens müssen die Betroffenen über die wesentlichen Inhalte des JCA informiert werden.

Nach einer abweichenden Auffassung setzt gemeinsame Verantwortlichkeit auch voraus, dass die verarbeiteten Daten aus der Perspektive jedes beteiligten Akteurs personenbezogene Daten im Sinne von Art. 4 Nr. 1 DSGVO sind. Danach kann ein Akteur, für den die betreffenden Daten mangels realistischer Re-Identifizierungsmöglichkeit keinen Personenbezug aufweisen, bereits begrifflich kein Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO und folglich auch kein gemeinsam Verantwortlicher im Sinne von Art. 26 DSGVO sein. Diese Sichtweise stützt sich darauf, dass jeder gemeinsam Verantwortliche für sich genommen die Voraussetzungen des Verantwortlichen-Begriffs erfüllen muss. In der Rechtssache IAB Europe wurde zunächst geprüft, ob der TC-String aus Sicht von IAB Europe personenbezogen ist, bevor die Rolle als gemeinsam Verantwortlicher beurteilt wurde; in der Rechtssache EDSB/SRB betont der EuGH die relative Betrachtung des Personenbezugs bei pseudonymisierten Daten und stellt nicht auf einen zwingend einheitlichen Personenbezug gegenüber allen Empfängern ab.

Für DCR-Kollaborationen würde dies bedeuten, dass eine gemeinsame Verantwortlichkeit nicht schon deshalb angenommen werden kann, weil die Beteiligten Zwecke und Mittel eines Analyse- oder Aktivierungsprozesses abstimmen. Vielmehr wäre zusätzlich zu prüfen, ob die Daten des jeweils einen Beteiligten auch aus Sicht des jeweils anderen Beteiligten personenbezogen sind. Fehlt es daran – etwa, weil der andere Beteiligte nur aggregierte Ergebnisse erhält oder pseudonymisierte Werte ohne realistische Re-Identifizierungsmöglichkeit verarbeitet –, käme nach dieser Auffassung keine gemeinsame Verantwortlichkeit in Betracht.

⁴ Die zugrunde liegenden Entscheidungen betrafen jeweils Konstellationen, in denen der Personenbezug der verarbeiteten Daten gegenüber dem als (gemeinsam) verantwortlich qualifizierten Akteur entweder unstreitig vorlag (C-210/16 – Wirtschaftsakademie; C-40/17 – Fashion ID) oder eigens festgestellt wurde, bevor die Verantwortlicheneigenschaft geprüft wurde (C-604/22 – IAB Europe). Ein Fall, in dem ein Akteur trotz fehlenden Personenbezugs aus seiner Perspektive als gemeinsam Verantwortlicher behandelt worden wäre, ist bislang nicht entschieden. Die Vorfrage des Personenbezugs und die nachgelagerte Rollenfrage wurden damit – soweit ersichtlich – noch nicht in ein und demselben Urteil mit Blick auf einen Akteur ohne Personenbezug entschieden.

Beide Parteien brauchen dann zwar immer noch:

- **eine datenschutzrechtliche Vereinbarung** mit dem DCR-Anbieter,
- **eine eigene Rechtsgrundlage für die Verarbeitung** der eigenen Daten im DCR,
- **sowie eine eigene Rechtsgrundlage für die Weitergabe** der Daten an die anderen Parteien. Die anderen Parteien würden aber für die Verarbeitung der fremden Daten, mangels Re-Identifizierungsmöglichkeit, nicht in den Anwendungsbereich der DSGVO fallen.

Hiervon sind primär die Use Cases Audience Insights und Lookalike Audience im DCR betroffen. Bei den Use Cases Lookalike Audience außerhalb DCR und Re-Targeting liegt in der Regel eine gemeinsame Verantwortlichkeit vor, weil beide Seiten erfahren, welche Nutzer*innen zur jeweils anderen Partei gehören.

Vor diesem Hintergrund empfiehlt sich die Rollenbewertung in DCR-Projekten zu dokumentieren und anhand der konkreten Re-Identifizierungsmöglichkeiten, Datenflüsse und Ergebnisformen zu begründen.

6. Handlungsempfehlungen

Datenschutzfreundliche Gestaltung von DCR-Projekten: Unternehmen sollten bereits bei der Planung eines DCR-Use-Cases den Privacy-by-Design-Ansatz verfolgen. Folgende Aspekte sind dabei essenziell:

- **Einsatz personenbezogener Daten minimieren:** So wenig direkte Identifikatoren wie möglich verwenden. Pseudonymisierung ist Pflicht, eventuell sogar mehrstufig (doppelt gehashte IDs). Wenn möglich, nur aggregierte oder statistische Daten aus dem DCR exportieren.
- **Zweckbeschränkung technisch durchsetzen:** DCRs bieten oft die Möglichkeit, bestimmte Suchanfragen oder Auswertungen einzuschränken (z. B. Mindestgrößen für Kohorten, sodass keine Rückschlüsse auf Einzelpersonen möglich sind). Solche Features sollten genutzt werden, um sicherzustellen, dass kein Beteiligter die Plattform missbrauchen kann, um doch einzelne Personen herauszufiltern.
- **Einwilligungs-Management integrieren:** Der Datenfluss in den DCR sollte mit bestehenden Consent Management Platforms (CMPs) verbunden werden. D. h. nur IDs von Nutzer*innen, die zugestimmt haben, werden exportiert. Zudem sollte es Mechanismen geben, um Widersprüche zu berücksichtigen (z. B. jemand widerruft seine Einwilligung – seine ID muss dann im DCR gelöscht oder für künftige Abgleiche gesperrt werden).
- **Transparenz gegenüber Nutzer*innen sicherstellen:** Schon in der Datenschutzerklärung sollte das Konzept eines Data Clean Rooms auf verständliche Weise erläutert werden. Nicht-technische Begriffe können helfen, z. B. „Datenkooperation in geschützter Umgebung“. Nutzer*innen sollten erfahren, welche Daten getauscht oder gemeinsam genutzt werden und zu welchem Zweck. Ideal ist ein leicht zugängliches Info-Portal: z. B. der Publisher könnte eine Seite bereitstellen „Unsere Datenpartnerschaften“, wo er auch die DCR-Projekte auflistet. Auch könnte man dort einen Kontakt für Rückfragen anbieten.

Daneben kommt es in der Praxis entscheidend darauf an, wie die Kooperation technisch, organisatorisch und kommunikativ umgesetzt wird. Die nachfolgenden Aspekte sollten frühzeitig mitgedacht werden, um eine Zusammenarbeit erfolgreich zu gestalten.

- **Transparenz und Nutzerakzeptanz:** Letztlich wird der Erfolg von DCR-Lösungen davon abhängen, wie akzeptiert sie von der Öffentlichkeit und Regulierungsbehörden sind. Wenn Nutzer*innen das Gefühl haben, hier passiert etwas Geheimes mit ihren Daten, könnte es zu Akzeptanzproblemen kommen. Daher sollten Unternehmen aktiv kommunizieren, warum Data Clean Rooms eingesetzt werden – z. B. „Wir schützen Ihre Privatsphäre, indem wir Ihre Daten nur verschlüsselt mit unseren Partnern matchen und keine unbekannten Dritten Ihre Identität erfahren.“ Diese Pro-Privacy-Argumentation kann das Vertrauensniveau erhöhen.
- **Zweckbindung und Weiterverwendung:** Unternehmen sollten strikt darauf achten, die Zweckbindung einzuhalten. Daten, die für einen bestimmten Abgleich bereitgestellt wurden, dürfen nicht anschließend für andere Zwecke genutzt werden. Zum Beispiel: Der Publisher sollte die gewonnenen Overlap-Informationen nicht nachträglich für eigene Marketingaktionen verwenden – das wäre ein Verstoß gegen die Zweckbindung, sofern nicht ausnahmsweise eine Zweckänderung zulässig ist. Daher sollten interne Policies erlassen werden, damit DCR-Daten isoliert bleiben.
- **Sicherheit:** Nicht zu vergessen – auch im DCR gelten Datensicherheitsanforderungen (Art. 32 DSGVO). Die beteiligten Daten sind pseudonymisiert, aber ein Zusammenführen großer Datenmengen kann ein attraktives Ziel für Angreifer sein. Firmen sollten Sicherheitsaudits der DCR-Anbieter durchführen und ggf. eigene Maßnahmen ergreifen (z. B. zusätzliche Verschlüsselungsschichten, strenge Zugriffskontrollen – nur wenige berechtigte Personen dürfen DCR-Exporte anstoßen etc.).

7. Ausblick

Data Clean Rooms werden voraussichtlich in den nächsten Jahren weiter an Bedeutung gewinnen – vor allem, wenn die Nutzung von Third Party Cookies weiter zurückgeht und First-Party-Daten-Kooperationen wichtiger werden.

Die fehlende Standardisierung ist aktuell noch ein Problem. Wünschenswert wäre, dass Brancheninitiativen Standards für DCRs entwickeln – sowohl technisch (Formate für ID-Abgleich) als auch rechtlich (Standardklauseln für gemeinsame Verantwortlichkeit). Bis dahin müssen Unternehmen bilateral Lösungen finden. Möglicherweise entstehen auch Broker-Dienste, die zwischen verschiedenen DCRs vermitteln.

Aus regulatorischer Sicht ist insbesondere auf die erwarteten Leitlinien des Europäischen Datenschutzausschusses zur Anonymisierung und Pseudonymisierung hinzuweisen, die voraussichtlich auch mehr Klarheit über die Abgrenzung von Anonymisierung und Pseudonymisierung sowie die damit verbundene Rollenverteilung der Verantwortlichen bringen werden.

Zum Schluss sei betont: DCRs bieten eine Chance, Datenkooperationen fair und datenschutzkonform zu gestalten. Sie sind aber kein Selbstläufer. Nur wer die juristischen Spielregeln (DSGVO) beachtet und Vertrauen zwischen allen Beteiligten (inklusive der Nutzer*innen) schafft, wird langfristig von diesen innovativen Ansätzen profitieren. Mit klaren Verträgen, transparenter Kommunikation und dem Willen, Datenschutz tatsächlich umzusetzen, können Data Clean Rooms zu einer „sauberen“ Lösung werden.

Autorenverzeichnis

Hakim Benabdelmoumene, Senior Data Business Development Manager, Ad Alliance

Christine Blaes, Director Data & Privacy, Media Impact

Jens Depenau, Expert Partner Data Strategy, WPP Media

Matthias Eigenmann, Legal Counsel, Decentriq AG

Eric Hall, Founder & Advisor, Halls of ...

Andreas Hamdorf, Lead Strategic Partner Management, esome advertising technologies

Cara Hönkhaus, Senior Global Communications Manager, InfoSum

Jasmin Schaub, Topic Lead Data Clean Rooms, Annalect Germany,
Omnicom Media Germany

Friedrich Schenk, Head of Targeting & Data Products, United Internet Media

Melanie von Lennep, Director Data Privacy, Omnicom Media Germany

Sven Wegholz, Director Client Data Solutions, Publicis Media Germany

Über den BVDW

Der Bundesverband Digitale Wirtschaft (BVDW) e.V. ist die Interessenvertretung für in Deutschland ansässige Unternehmen, die digitale Geschäftsmodelle betreiben oder deren Wertschöpfung auf dem Einsatz digitaler Technologien beruht. Die Grundlage dafür ist die intelligente Verbindung von Daten und Kreativität bei gleichzeitig maßgeblicher Orientierung an ethischen Prinzipien. Mit seinen über 600 Mitgliedsunternehmen – von großen und kleinen Digitalunternehmen über Agenturen bis hin zu Publishern – vertritt der Verband die Belange der digitalen Wirtschaft gegenüber Politik und Gesellschaft. Sein Netzwerk von Expertinnen und Experten liefert mit Zahlen, Daten und Fakten Orientierung zu einem zentralen Zukunftsfeld. Mehr Informationen finden Sie unter www.bvdw.org.

Über die Working Group Programmatic Advertising Ecosystem

Programmatic Advertising ist mit zweistelligen Wachstumsraten in Deutschland weiter auf Erfolgskurs. Es ist ein zentraler Erfolgsfaktor im Mediabusiness der Zukunft und einer der wichtigsten Vorteile der digitalen Kanäle im Wettbewerb um die Mediabudgets. Den programmatischen Handel digital adressierbarer Medien in Deutschland weiterzuentwickeln und nachhaltig zu gestalten, ist das Ziel dieser Working Group. Wir fördern Qualität, definieren Standards und ermöglichen Kooperationen.

Mehr Informationen finden Sie unter

<https://www.bvdw.org/gremien/programmatic-advertising-ecosystem/>.

Über das Lab Data Clean Rooms

Das Thema Data Clean Rooms gewinnt zunehmend an Bedeutung für das gesamte Programmatic-Advertising-Ökosystem. Dabei spielen neben anderen vor allem Aspekte wie Datenschutzkonformität, digitale Vermarktung in der Cookieless Future, First-Party-Data-Strategien und Supply Path Optimization eine große Rolle. Oft herrschen auch noch Unklarheiten über die Funktionsweise von Data Clean Rooms, zu den verschiedenen Anwendungsfällen (Analytics, Activation) sowie über die Begrifflichkeiten. Ziel des Labs sind Aufklärungsarbeit und Education für die einzelnen Marktpartner, unter anderem über die Erarbeitung und Veröffentlichung von Whitepapern, Anbieterübersichten und Anwendungsfällen sowie über die Teilnahme an Veranstaltungen.



Impressum

Datenschutzrechtliche Betrachtungen von Use Cases für Data Clean Rooms (DCR)

Erscheinungsort und -datum	Berlin, Juli 2026
Herausgeber	Bundesverband Digitale Wirtschaft (BVDW) e.V. Obentrautstraße 55, 10963 Berlin, +49 30 2062186-0, info@bvdw.org , www.bvdw.org
Vorstand gem. § 26 BGB	Carsten Rasner
Präsident	Dirk Freytag
Vizepräsident*innen	Thomas Duhr, Anke Herbener, Corinna Hohenleitner, Dr. Moritz Holzgraefe, Björn Kaspring, Julian Simons
Kontakt	Ina Franke, Senior Program Managerin, franke@bvdw.org
Vereinsregisternummer	Vereinsregister Düsseldorf VR 8358
Rechtshinweise	Alle in dieser Veröffentlichung enthaltenen Angaben und Informationen wurden vom Bundesverband Digitale Wirtschaft (BVDW) e.V. sorgfältig recherchiert und geprüft. Diese Informationen sind ein Service des Verbandes. Für Richtigkeit, Vollständigkeit und Aktualität können weder der Bundesverband Digitale Wirtschaft (BVDW) e.V. noch die an der Erstellung und Veröffentlichung dieses Werkes beteiligten Unternehmen die Haftung übernehmen. Die Inhalte dieser Veröffentlichung und / oder Verweise auf Inhalte Dritter sind urheberrechtlich geschützt. Jegliche Vervielfältigung von Informationen oder Daten, insbesondere die Verwendung von Texten, Textteilen, Bildmaterial oder sonstigen Inhalten, bedarf der vorherigen Zustimmung durch den Bundesverband Digitale Wirtschaft (BVDW) e.V. bzw. die Rechteinhaber (Dritte). Deutsches Lobbyregister R000257 EU-Transparenzregister-Nummer 479540331468-69