DECENTRIQ

MEDIA WHITEPAPER

Decentriq Media Clean Rooms

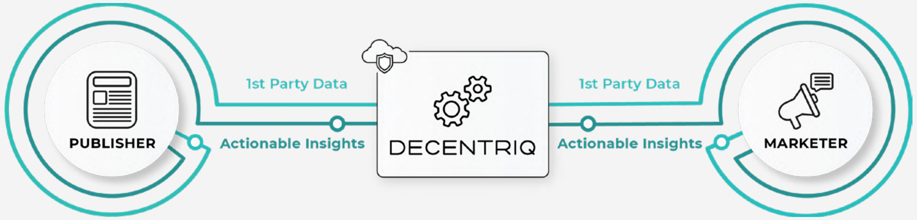
Reach high-value audiences and better monetize ad inventory in a first-party-data world.

1. Executive Summary

Data clean rooms (DCRs) offer a data privacy-compliant way for publishers and brands to join their first-party data and uncover new audience insights, making richer targeting possible without third-party cookies. **But up until now, DCR users had to make tradeoffs** between:

- DCRs where a trusted party, either a publisher or the data clean room provider itself, has control over all the data. This requires the other party to trust them and their promise to keep the data private and secure.
- DCRs with limited or rigid identity matching capabilities, limiting audience reach, and risking privacy exposure in the segments it produces
- DCRs that are based on complex cryptography methods that require a team of encryption experts to work with and offer little analytical flexibility

Decentriq Media Clean Rooms is a data clean room solution for brands, publishers and retailers who don't want to sacrifice privacy and control for usability. In Decentriq Media Clean Rooms, first-party data is verifiably never accessible to any party, not even to Decentriq. It enables advanced matching and lookalike audiences, immediately actionable from within a no-code SaaS environment. Setup takes only five minutes — no support needed from an engineering team.



With Decentriq Media Clean Rooms, advertisers can activate their data to target **consent-less lookalike segments**. These high-value segments within the publisher's inventory are called "consent-less" because brands or publishers don't need to collect additional consent to use first-party data to build these segments within the clean room. This is thanks to Decentriq's **unique combination of confidential computing and privacy-by-design approach**, where only anonymized and aggregated insights can be extracted from the data.

Read on to find out how to tap into privacy-first addressability with Decentriq Media Clean Rooms.

> “3rd party cookies have underpinned internet advertising for decades. With its deprecation, publishers and brands have to rethink entirely new ways to reach audiences in a privacy first world. With Decentriq and confidential computing, Goldbach enables a trust layer, allowing brands to onboard their 1st Party Data without compliance risks. - *Jochen Witte, CTO, Goldbach Group AG*

2. How to Evaluate Data Clean Rooms

A data clean room (DCR) is a secure, controlled environment where two or more parties — such as a publisher and a brand — can upload their encrypted first-party data and discover new insights that are only made possible by combining the data. However, this is usually where the similarities between DCRs end. **Data clean rooms provide very different levels of privacy, capabilities and interoperability** with your marketing stack depending on their design.

DCR Evaluation Checklist

- ✓ Data privacy method
- ✓ Anonimity of output
- ✓ Control and transparency
- ✓ Integration with ad tech stack
- ✓ Identity matching
- ✓ Ease of use

How does the DCR assure data privacy?

Most data clean rooms **can't guarantee that personal data is completely inaccessible** at all times. This is why brands and publishers usually have to rely on purely contractual data privacy agreements with the DCR provider. Legally, this is not considered hard proof of data privacy and constitutes data transfer. So brands and publishers **usually require consent** from their customers and subscribers for use of their data in the DCR.

Clean rooms built on **confidential computing technology** hard-wire security and data privacy into the platform itself, **guaranteeing that data remains private** during the entire process — from upload to storage to download, and uniquely, while calculations are running. This guarantee is verifiable through logging the running computations, removing the need to trust both vendor and cloud provider.

Are the insights that leave the DCR truly anonymous?

It depends on the approach, and often varies by the type of insight.

The most common approaches for activation **hide the personally identifiable information (PII)** used to match users, such as the customer email addresses, but **do reveal which users matched**. This can happen as part of the match, or may happen later when the audience is used to bid on ad placements. This provides some protection, but it is not truly anonymous because it's simple to reverse engineer the match keys (e.g. email addresses) of the advertisers' customers.

Aggregated analytics such as campaign measurement and audience insights are **more likely to be truly anonymous**.

Aggregated insights only reveal groups, so they provide “safety in numbers”. A DCR can add more protection by enforcing a minimum group size, rounding the answers slightly, placing limits on how much one person can affect the average, or adding a small amount of noise to the result. A combination of these techniques can ensure that an individual isn’t accidentally reidentified, providing truly anonymous results.

Look for robust support of truly anonymous insights for the approaches you plan to use, especially for activation, since many providers do not offer an anonymous activation option.

Do you have control and transparency over how your data is used?

Closed ecosystems or **walled gardens**, often provided by big-tech players like Google and Meta, give marketers the ability to combine their first-party data with consumer data that lives within the walls of their partners’ environments. Marketers typically give up control and transparency over how their data is used and have to trust the tech giants to not misuse their data.

Independent providers provide a neutral ground for parties who want to collaborate on their first-party datasets. These parties can agree together on the scope of collaboration within the data clean room. The degree of control and transparency varies among independent providers and most of them have access to the data processed in their platform. Some providers make it possible for each party to set individual controls over the use of their own first-party data.

How does the DCR fit into your adtech stack?

The more complex and modular tech stacks become, the more interoperability is a primary concern. Consider how **compatibility** with demand-side, supply-side and other platforms impacts your internal workflows and operations. The strongest clean rooms will offer multiple overlapping approaches, such as direct integrations with popular platforms, an application programming interface (API) to handle automated workflows, and a graphical user interface (UI) to ease exploration and manual analysis. The **most important trait is flexibility** – how quickly a DCR can be adapted to try a new workflow or integrate with a new partner. This ensures the clean room will remain viable as your business needs grow and change.

How are user identities matched in the DCR?

Some data clean rooms have fixed methods for **establishing the identity** of a unique user between two datasets, for example email addresses, telephone numbers or ID5 identifiers. It’s essential that this aligns with how both brand and publisher track their users within their own first-party data, or else it won’t be possible to match audiences at all. Other data clean rooms are **identity-method agnostic**, meaning as long as the two parties have some overlapping identifier or can pull in an identity graph, they can combine the datasets and get insights.

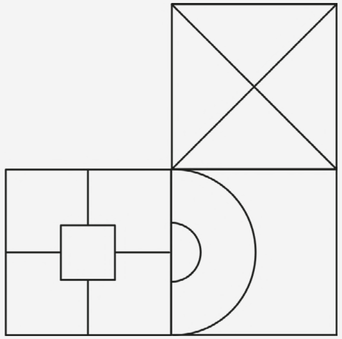
Do you need additional developer or data science resources to use it?

Data clean rooms are designed for a variety of purposes and user groups. **More flexible providers give data science teams freedom to apply their own logic** and models to the data and extract insights they define. While powerful, not every team has access to these resources, or has a use case that’s unique enough to warrant this level of customization.

If the use case is clearly defined and a marketer or other business role is responsible for achieving results with the clean room, they may need an out-of-the-box solution with predefined logic and results, and a **UI that they can manage without code.**

3. Decentriq Media Clean Rooms: Activate First-Party Audiences

Decentriq Media Clean Rooms is a data clean room designed for privacy-conscious brands, publishers, and retailers. It allows them to **directly identify and activate audiences by joining first-party data**, without compromising on data security, flexibility or control.



Data privacy as a verifiable guarantee

Data privacy is not just a promise. It's **verifiable**. Data is never exposed at any point in time to any party—and the computation logs can prove it. No trust in Decentriq or the cloud provider is needed, and each party maintains full control over their data at all times. For proof, see the Decentriq technical whitepaper.

Integrates with any DSP, SSP, DMP or CDP

Brands and publishers have **full ad tech stack flexibility.** Decentriq's APIs make it easy to integrate a Media Clean Room with the user's DSP, SSP, DMP or CDP of choice, so they can tap into the value of their data faster.

Identity matching across any identifier

As long as there's at least **one matching identifier of any kind** in the two datasets, the Media Clean Room can identify the overlap and run its advanced calculations to find and target new high-value segments in the publisher's audience.

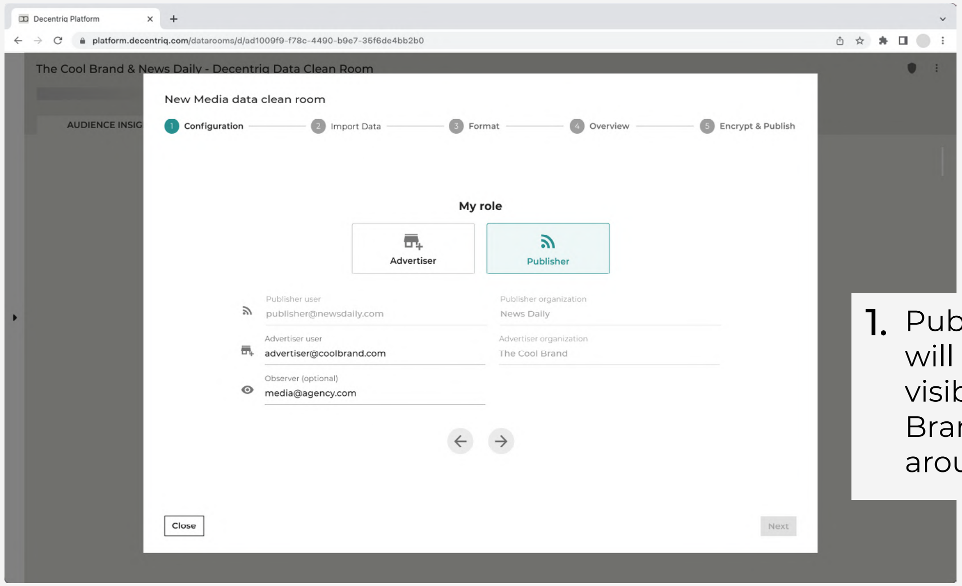
Consent-less lookalikes while maintaining privacy

Decentriq's privacy-enhancing technologies make it impossible from a technical standpoint for personal data to be disclosed. This fact, combined with the Media Clean Room's default setting of outputting only aggregated insights, means full user privacy is protected at all times, and brands can **build and activate first-party segments without needing additional consent from their customers**. With appropriate consent, the Media Clean Room can also be configured to provide precision retargeting.

5-minute setup, no code needed to use

Decentriq Media Clean Rooms are built for publishers and brands to use **without the support of a data science team**. Setup takes only 5 minutes, and business users can manage the platform, see insights and activate audiences immediately in a no-code SaaS interface.

How it works



Decentriq Platform

platform.decentriq.com/datarooms/d/ad1009f9-f78c-4490-b9e7-35f6de4bb2b0

The Cool Brand & News Daily - Decentriq Data Clean Room

AUDIENCE INSIG

New Media data clean room

1 Configuration — 2 Import Data — 3 Format — 4 Overview — 5 Encrypt & Publish

My role

Advertiser | Publisher

Publisher user: publisher@newsdaily.com

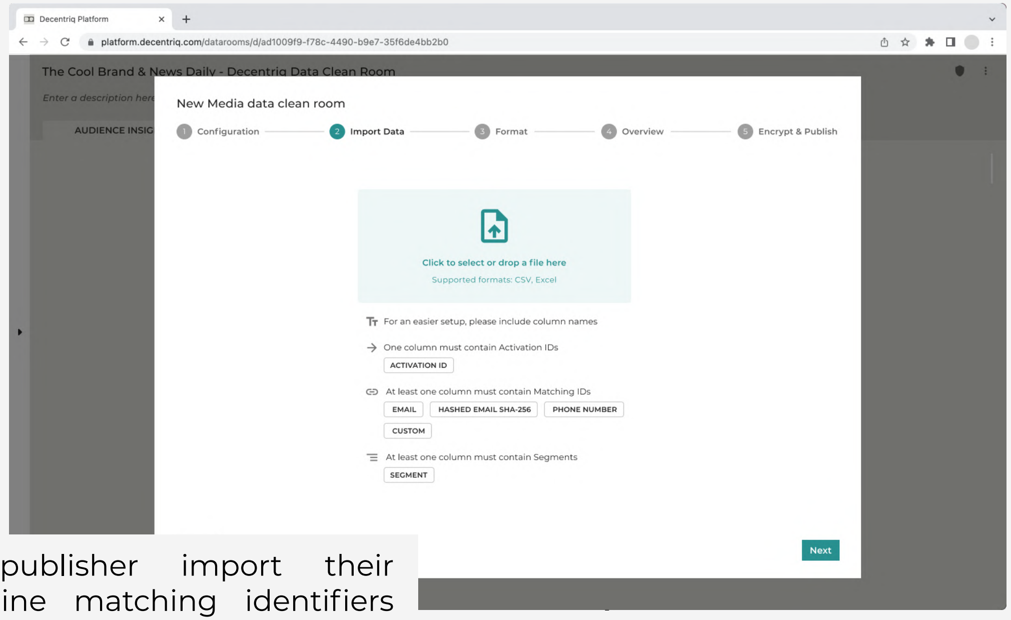
Publisher organization: News Daily

Advertiser user: advertiser@coolbrand.com

Advertiser organization: The Cool Brand

Observer (optional): media@agency.com

1. Publishers configure the Media Clean Room they will share with a brand, controlling what level of visibility the brand user has to their audience data. Brands or their agencies can also set guardrails around use of their own first-party data.



Decentriq Platform

platform.decentriq.com/datarooms/d/ad1009f9-f78c-4490-b9e7-35f6de4bb2b0

The Cool Brand & News Daily - Decentriq Data Clean Room

Enter a description here

AUDIENCE INSIG

New Media data clean room

1 Configuration — 2 Import Data — 3 Format — 4 Overview — 5 Encrypt & Publish

Click to select or drop a file here

Supported formats: CSV, Excel

For an easier setup, please include column names

One column must contain Activation IDs

ACTIVATION ID

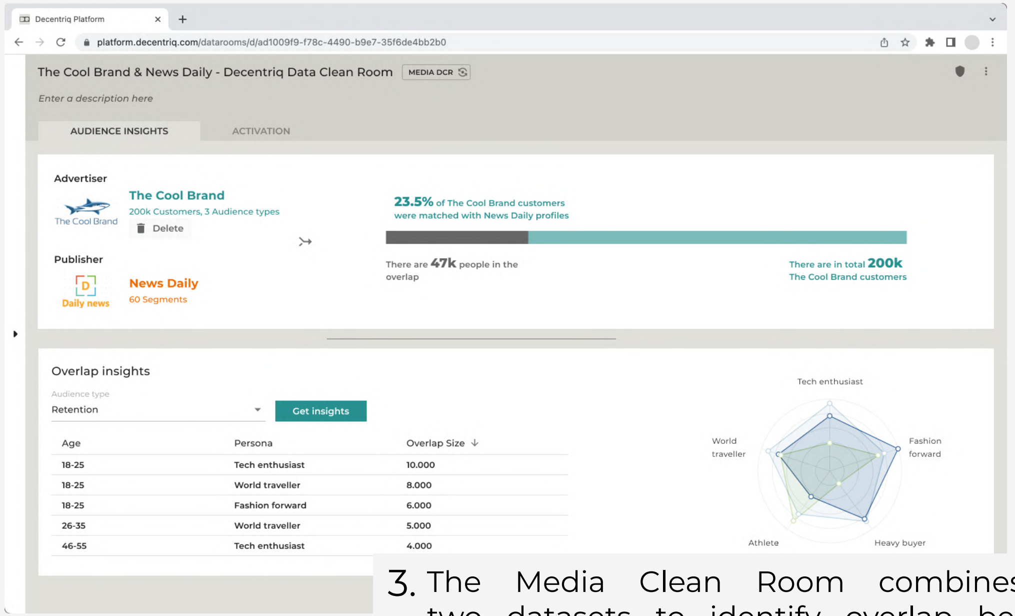
At least one column must contain Matching IDs

EMAIL | HASHED EMAIL SHA-256 | PHONE NUMBER | CUSTOM

At least one column must contain Segments

SEGMENT

2. Brand and publisher import their audiences, define matching identifiers and segmentation. Decentriq encrypts and uploads the datasets.



The Cool Brand & News Daily - Decentriq Data Clean Room

Enter a description here

Advertiser

The Cool Brand
200k Customers, 3 Audience types

Publisher

News Daily
60 Segments

23.5% of The Cool Brand customers were matched with News Daily profiles

There are **47k** people in the overlap

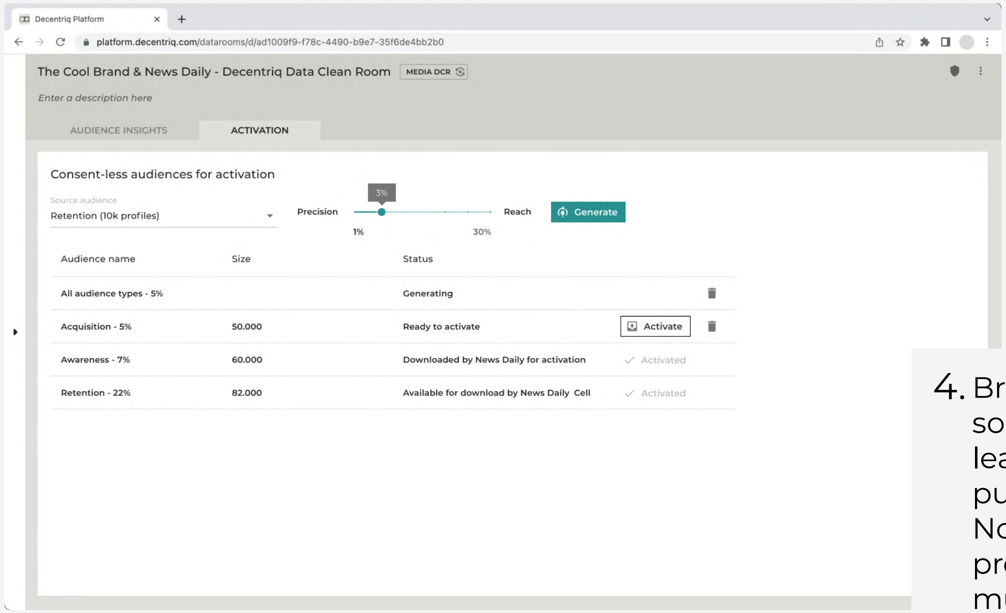
There are in total **200k** The Cool Brand customers

Overlap insights

Audience type: Retention

Age	Persona	Overlap Size ↓
18-25	Tech enthusiast	10.000
18-25	World traveller	8.000
18-25	Fashion forward	6.000
26-35	World traveller	5.000
46-55	Tech enthusiast	4.000

3. The Media Clean Room combines the two datasets to identify overlap between the advertiser and publisher's audiences. Data remains encrypted and secure while calculations are running. Both parties receive anonymized insights about the overlapping segments, and brands can choose which audience to target with ads.



The Cool Brand & News Daily - Decentriq Data Clean Room

Enter a description here

Consent-less audiences for activation

Source audience: Retention (10k profiles)

Audience name	Size	Status	
All audience types - 5%		Generating	
Acquisition - 5%	50.000	Ready to activate	Activate
Awareness - 7%	60.000	Downloaded by News Daily for activation	✓ Activated
Retention - 22%	82.000	Available for download by News Daily Cell	✓ Activated

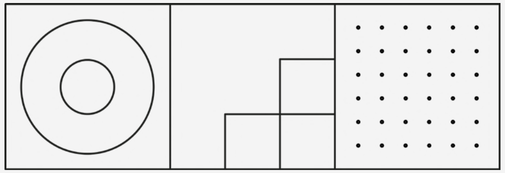
4. Brands can also create consent-less lookalikes based on source audiences from the overlap segment. Machine learning models identify segments of users within the publisher's audience that have high potential value. No individual user information is revealed. Level of precision defines how tightly the lookalikes fit and how much reach is possible.

A first-party path forward for publishers and retail media networks

Decentriq Media Clean Rooms give publishers and retail media networks an immediate, actionable method for **securing themselves and their inventory against a cookieless future**. Together with their advertising and brand partners, they're able to create new high-value audience segments and better monetize their inventory in the cookieless era.

Beyond the immediate segmentation and targeting options predefined in the Media Clean Rooms, publishers and retailers can **customize the targeting models to their own unique business logic** with the support of their in-house data science teams.

With Decentriq Media Clean Rooms, publishers and retailers can manage one-to-one first-party data collaborations with their brands in a scalable, easy-to-use platform that **integrates with any SSP**. Without ever compromising on security and privacy, thanks to Decentriq's use of the most advanced privacy-enhancing technologies available.



Ringier

Swiss Media Group Enables Cookieless Addressability with Decentriq

With the deprecation of third-party cookies, addressing the right audience is an enormous challenge for media owners and brands alike. Some publishers are moving to invent new ways to defend their revenues while relying on their most valuable asset: first-party data, and their direct relationship with readers.

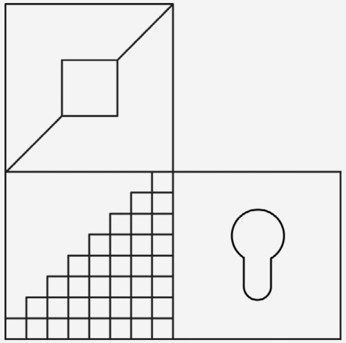
Swiss media group **Ringier AG** positioned themselves ahead of the curve and adopted a new approach to first-party addressability by collaborating with data partners on Decentriq's confidential computing-based data clean room platform.

"Confidential computing and data clean rooms present us with a great chance to exchange information in a legal, efficient and effective way," says Zhao Wang, Head of Data Technology at Ringier. *"This allows us to do better media planning and advertising, targeting more accurately – and in the end driving more revenue whilst complying with all data protection regulations."*

READ MORE

4. How Decentriq Enables Consent-less Activation on First-Party Data

Confidential computing provides a verifiable guarantee, embedded into the hardware itself, that no one can access user data at any point — even when calculations are running. From a compliance perspective, this means **the consent framework that an organization has to follow to use the platform depends exclusively on the type of audience the clean room delivers to them**.



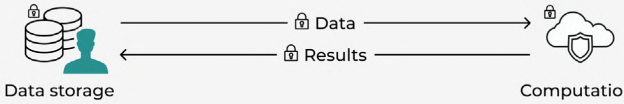
Confidential Computing

Confidential computing is an advanced privacy enhancing technology that **encrypts data throughout its lifecycle.** Previously, data could be encrypted "at rest" (when it's being stored), and "in transit" (when it's being transferred). The breakthrough in confidential computing is its ability to **encrypt sensitive data while it's in use**, something previously not possible.

Because data is always encrypted, **not even Decentriq or the cloud provider can access or view the data at any point**. This can be proven as the technology enables the independent verification of this fact by every user of the platform.

In addition, confidential computing **only allows pre-approved analytics to run** in Decentriq Data Clean Rooms, ensuring that data owners always remain in control of their data at all times. Privacy filters enforce that the results leaving the data clean room do not contain sensitive information.

SECURING DATA IN ALL POSSIBLE STATES



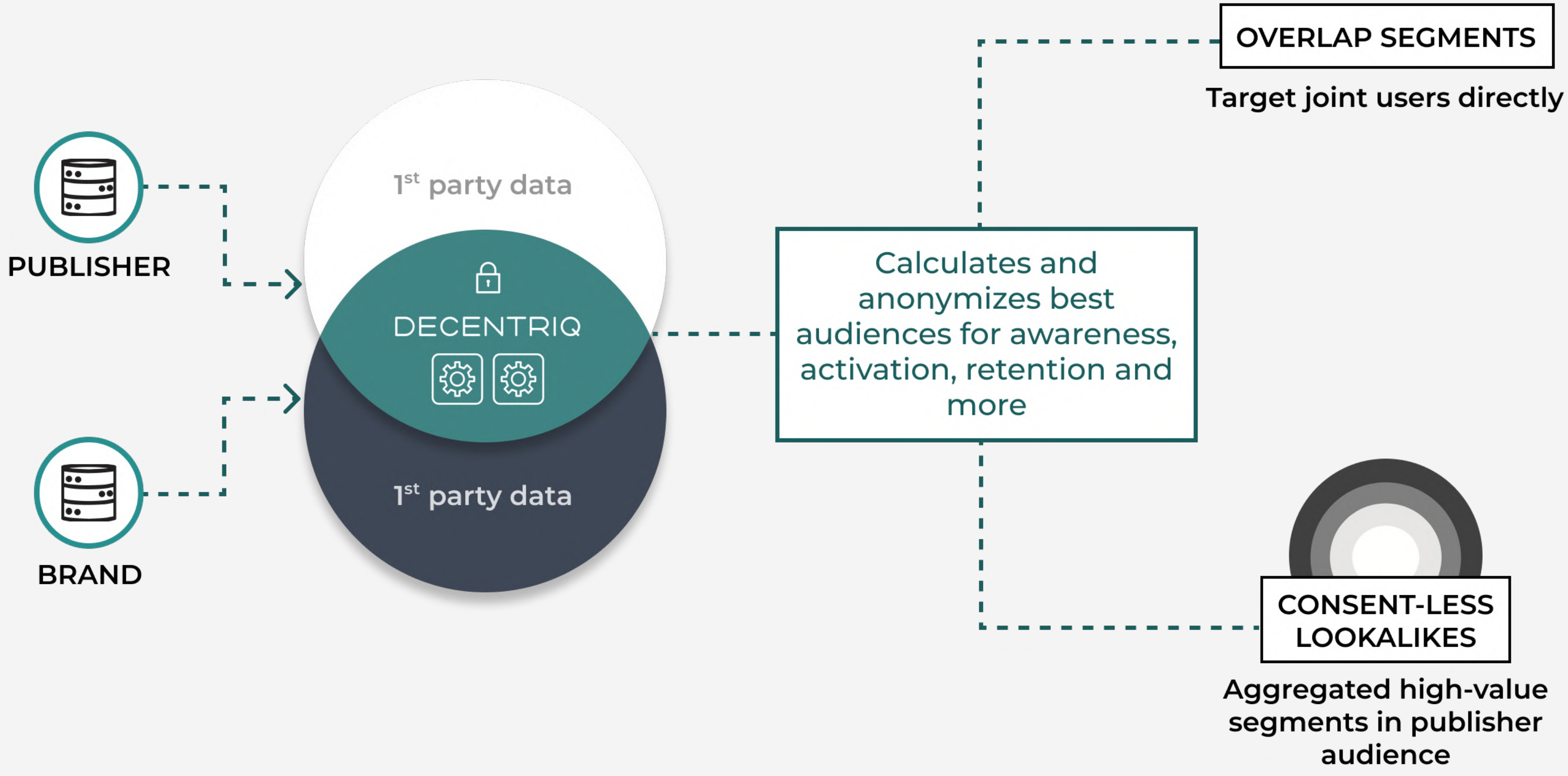
Data at rest	Data in transit	Data in use
Data is encrypted when stored on hard disks	Data is encrypted when transferred (HTTPS/TLS)	Now data can be encrypted also when computed
standard for decades	standard for decades	impossible before confidential computing

FIND OUT MORE

For consent-less lookalike targeting with Decentriq Media Clean Rooms, the audience an advertiser sees is **always fully anonymized and only available as aggregated insights.** They never know who within a publisher's audience they're targeting. They only know the proportion of the publisher audience that matches one of their source segments, and how closely they match.

Both **parties still need consent to collect a user's first-party data on their properties** in the very beginning, but its use in Decentriq clean rooms — and its use for targeting anonymized, aggregated segments within a publisher's audience — doesn't require additional consent.

First-Party Activation with Decentriq Media Clean Rooms


PUBLISHER
BRAND
1st party data
DECENTRIQ
1st party data
Calculates and anonymizes best audiences for awareness, activation, retention and more
OVERLAP SEGMENTS
Target joint users directly
CONSENT-LESS LOOKALIKES
Aggregated high-value segments in publisher audience

5. Decentriq: The Switzerland of Data Collaboration

Decentriq's data clean rooms provide a secure, neutral environment for organizations to combine their first-party data, collaborate, and uncover insights that are only possible by joining the datasets. Each organization has full control and transparency over how its data is used, at all times in the process. **First-party data is never exposed or accessible to any other party** — not the cloud provider, and not even Decentriq itself.

This high level of security is made possible through Decentriq's privacy-first design, and their use of the latest advancements in encryption and privacy enhancing technologies such as synthetic data, differential privacy, and confidential computing. Decentriq data clean rooms, running on trusted execution environments including **Microsoft Azure Confidential Computing infrastructure**, are designed to protect the world's most sensitive data.

Trusted by the world's most privacy-minded organizations

Ringier

GOLDBACH

M ASSOCIATES
HEALTHCARE EXPERTS

PostFinance

Roche

Stadt Zürich

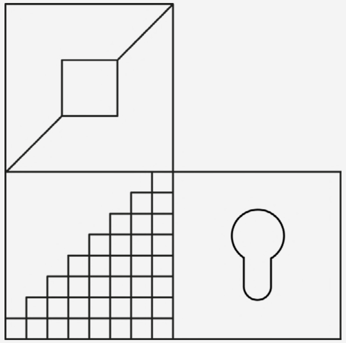
Swiss Armed Forces
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

swisscom

Microsoft

6. Expert Uses of Decentriq Data Clean Rooms for Publishers and Brands

Decentriq users that have data science resources at their disposal can solve more unique challenges and implement complex targeting models with **Decentriq's flexible Data Clean Rooms**. These offer a truly neutral ground for secure collaboration, and full flexibility in analyzing and collaborating on data. Here are a few examples of advanced use cases:



Pixel-less measurement

Brands can define a conversion KPI, gather conversion data and import this data into the data clean room. The publisher contributes ad impression data from the ad server. **The data clean room then calculates the conversion rate and sends aggregated metrics back** to brand and publisher, allowing them to measure the effectiveness of a campaign without third-party cookies. If the brand collaborates with multiple publishers, they can use this technique to achieve cross-channel measurement.

User attribute modeling

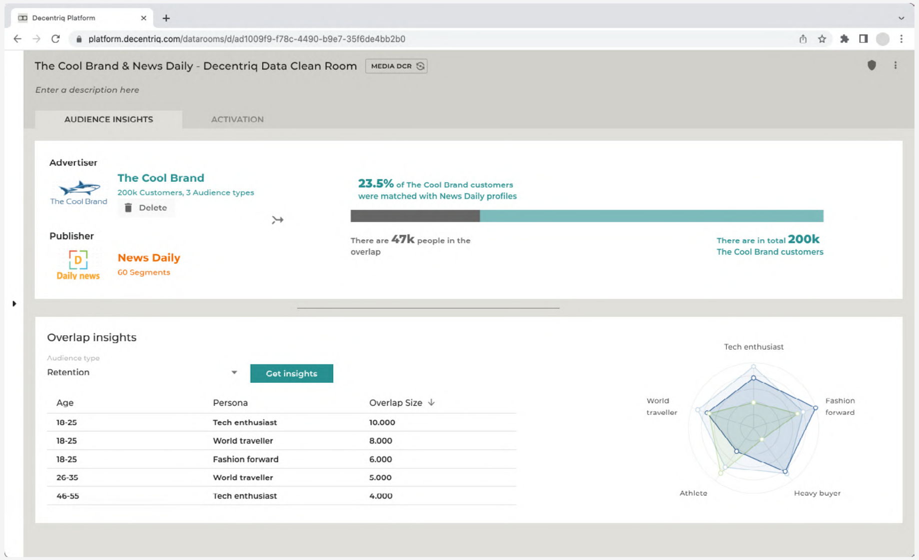
Publishers can make up for the loss of third-party enriched segments by collaborating with their brand partners on first-party data. By training their models on attribute insights gleaned from linking the two datasets, publishers can **increase the attribute prediction accuracy for their audience**, deliver more efficient targeting campaigns, and better calculate the value of their inventory.

Next-best-product modeling

Brands can also augment their product recommendation models with insights they discover by pairing their user data with a partner's. Through this collaboration, they can better **understand which attributes lead a customer to repurchase or purchase a related product**, and use these insights for cross-selling or upselling tactics.

7. Next Steps to First-Party Activation with Decentriq Media Clean Rooms

1. **Evaluate the impact** of cookie deprecation and changing consumer privacy regulations on your marketing strategy. What tactics will need a new approach?
2. **Examine your first-party user data.** Are you collecting the information — and consent — you need to build rich user profiles? Does your data pipeline align with the goals you're trying to reach? How sensitive is your user data?
3. **Identify your use case.** What tactics are rife for testing first-party targeting? What segments would you like to target if you could?
4. **Identify potential partners.** Which media networks, retail partners, publishers or brands could benefit from collaboration and have complementary data that you can combine with yours to build rich segments?



The Cool Brand & News Daily - Decentriq Data Clean Room

Enter a description here

Advertiser

The Cool Brand

200k Customers, 3 Audience types

Publisher

News Daily

60 Segments

23.5% of The Cool Brand customers were matched with News Daily profiles

There are 47k people in the overlap

There are in total 200k The Cool Brand customers

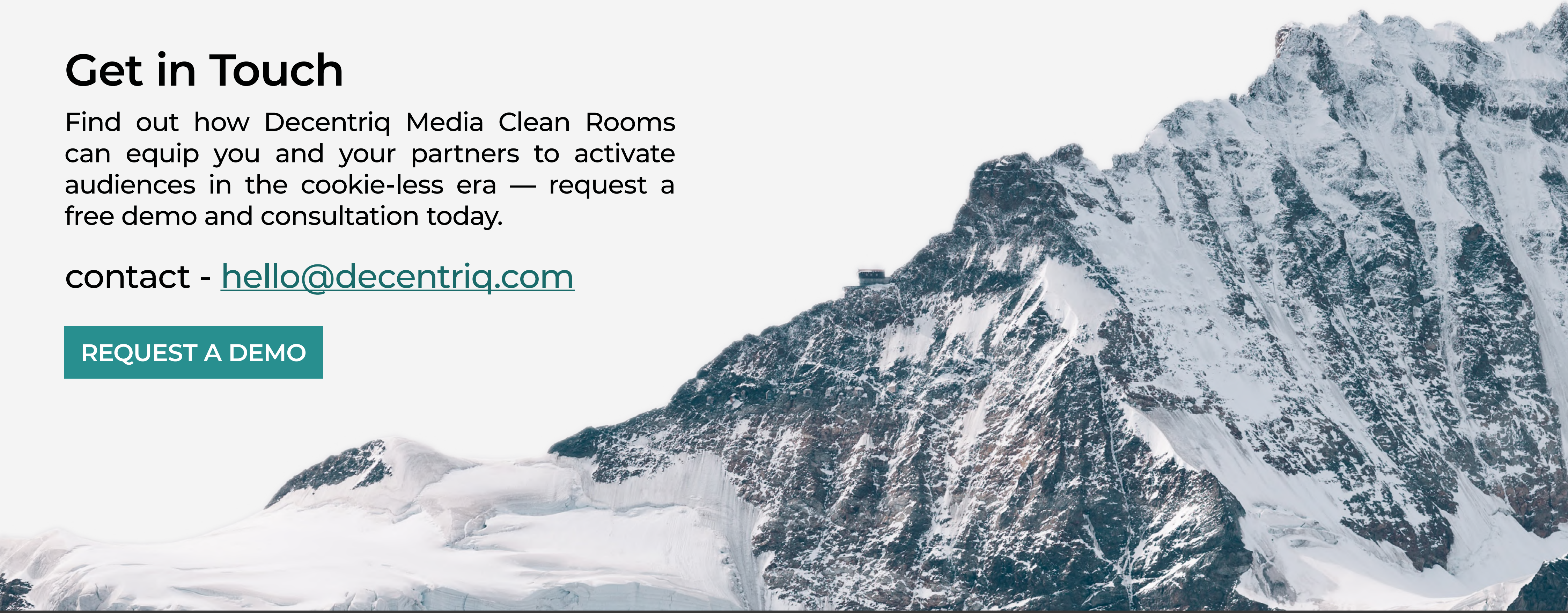
Overlap insights

Audience type: Retention

Age	Persona	Overlap Size ↓
18-25	Tech enthusiast	10.000
18-25	World traveller	8.000
18-25	Fashion forward	6.000
26-35	World traveller	5.000
46-55	Tech enthusiast	4.000

Key benefits

FOR PUBLISHERS	FOR BRANDS
• Build high-value audience segments without third-party cookies	• Activate new high-value targets in publisher and retail media networks
• Discover new ways to monetize inventory	• Tap into hidden value in first-party user data
• Scale first-party targeting across brands	• Use without data science resources
• Customize the targeting models based on own business logic	• Secure and private enough for even the most sensitive verticals (banks, healthcare)
• Integrate with any SSP and DMP	• Integrate with any DSP, CDP or DMP



Get in Touch

Find out how Decentriq Media Clean Rooms can equip you and your partners to activate audiences in the cookie-less era — request a free demo and consultation today.

contact - hello@decentriq.com

REQUEST A DEMO

DECENTRIQ

www.decentriq.com

Follow us on