Privacy & Security Best Practices

OMEDA WEBINAR

omeda

Your Host

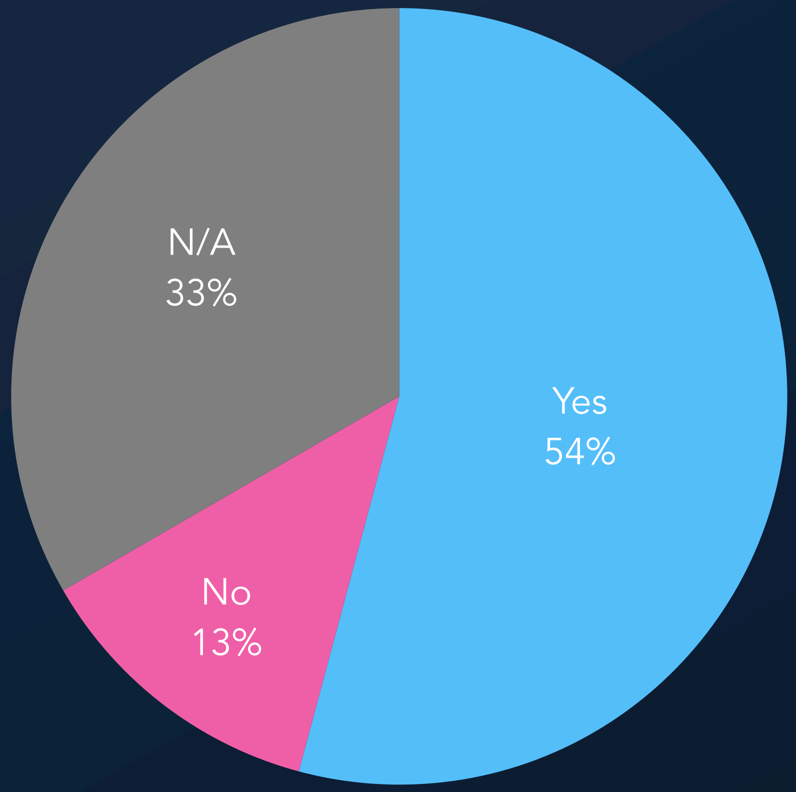
Bettina Lippisch

VICE PRESIDENT, PRIVACY & DATA GOVERNANCE

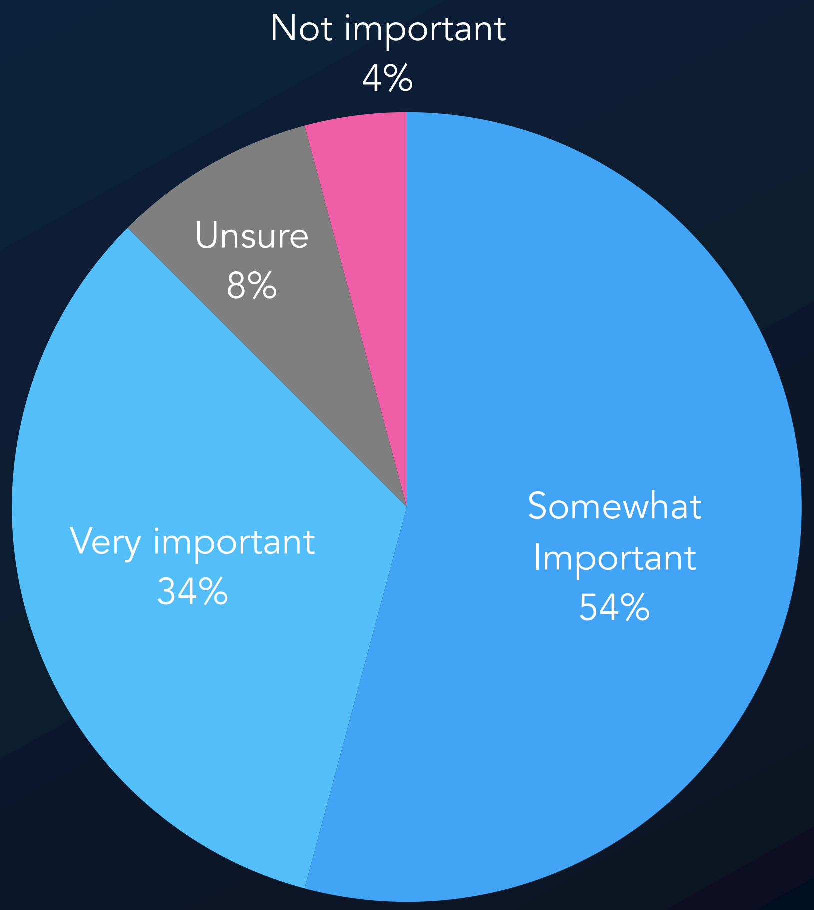
omeda

Privacy in your organization – Survey results

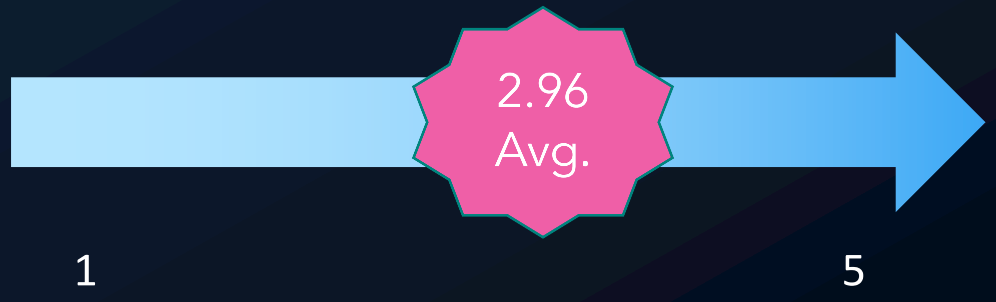
Do you work with legal counsel to review what privacy laws apply to you?



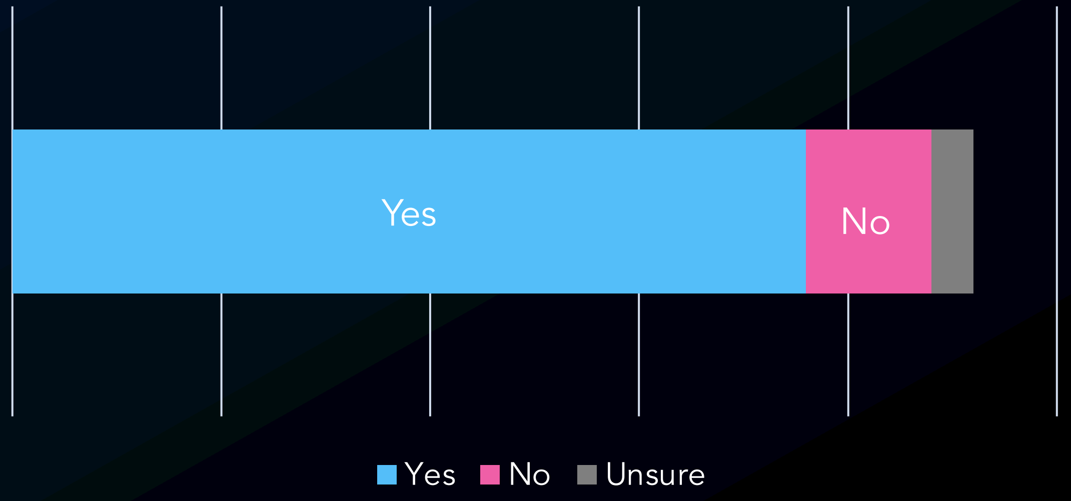
How prominently does Privacy feature in your organization's culture?



Describe your knowledge level around privacy and data governance



Does your organization have a dedicated privacy program or practice?



omeda

Why privacy matters more than ever in 2023

Cyber incidents are on the rise:

- A single attack – be it a data breach, malware, ransomware or DDoS attack – cost companies in the U.S. a median of $18,000 in 2022. *Source: Hiscox Cyber Readiness Report 2022.*
- Though 43% of attacks are aimed at SMBs, only 14% of these businesses are prepared to defend themselves. *Source: State of Cybersecurity Resilience 2021, Accenture.*
- More than 33 billion records will be stolen by cybercriminals by 2023, an increase of 175% from 2018. *Source: TechTarget.com*
- The human element is the most common threat vector; it was the root cause of 82% of data breaches. *Source: Verizon's "2022 Data Breach Investigations Report"*

Why privacy matters more than ever in 2023

Lawsuits & settlements/fines leveraged for bad privacy practices

- Facebook parent Meta will pay $725M to settle a privacy suit over Cambridge Analytica.
- Plaid Data paid $58M Class Action Settlement for accessing private data from payment apps without their consent.
- Google settles for $391.5M over its location tracking practices.

Don’t be that company in the news for bad privacy practices

- Privacy is now a competitive advantage and good practices will protect your brand & revenue.

Why privacy matters more than ever in 2023

What did we learn from the above?

- Data retention practices & data minimization are critical for all data companies.
- Security is a mandatory priority.
- Privacy & security principles (best practices) are the foundation of all major U.S. (and international) privacy laws.

Legal Refresher – 2023 U.S. State Privacy Laws

Effective Dates	State Privacy Regulation/Law
January 1, 2023	California Privacy Rights Act Virginia Consumer Data Protection Act
July 1, 2023	Colorado Privacy Act Connecticut Data Privacy Act
December 31, 2023	Utah Consumer Privacy Act

All these bills coming into law in 2023 give consumers a Right of Access, Deletion, Portability and Right to Opt-out of Sales, as well as to dictate business obligations around Notices & Transparency.

Most also require covered businesses to conduct risk assessments, limit processing based on purpose, and ensure that they do not discriminate against customers who exercise their privacy rights.

Let's talk Best Practices

1. Know your data
2. Govern your data
3. Maintain your data
4. Champion privacy & security
5. Choose the right tech stack

omeda

1 Best Practice: Know your data

Perform Data Discovery/Audits

Customer/Subscriber Data & Internal/Employee Data

- Know what data is considered sensitive
- How sensitive?
- How do you protect it?

Processing

- Can you identify all processing activities?
- Does it align with your Privacy Notices/Consent?

3rd Party Partners/Vendors

Use partners and processing tools that are transparent and whose data can be easily audited. Questions to ask a data partner:

- Can I track consent across the customer lifecycle?
- Can I easily comply with Data Subject Right (DSR) requests?
- What options do you have to ensure easy opt-ins AND opt-outs?
- Can I easily audit what data is tied to a data subject?
- What tools or features do you have that will protect my business interest AND privacy best practices?

2 Best Practice: Govern your data

Access Control – Build on your data discovery

- Who has access and what security risks are connected?
- Principle of least privilege – only need to know, never nice to know

Data Security – Have strong protections & processes

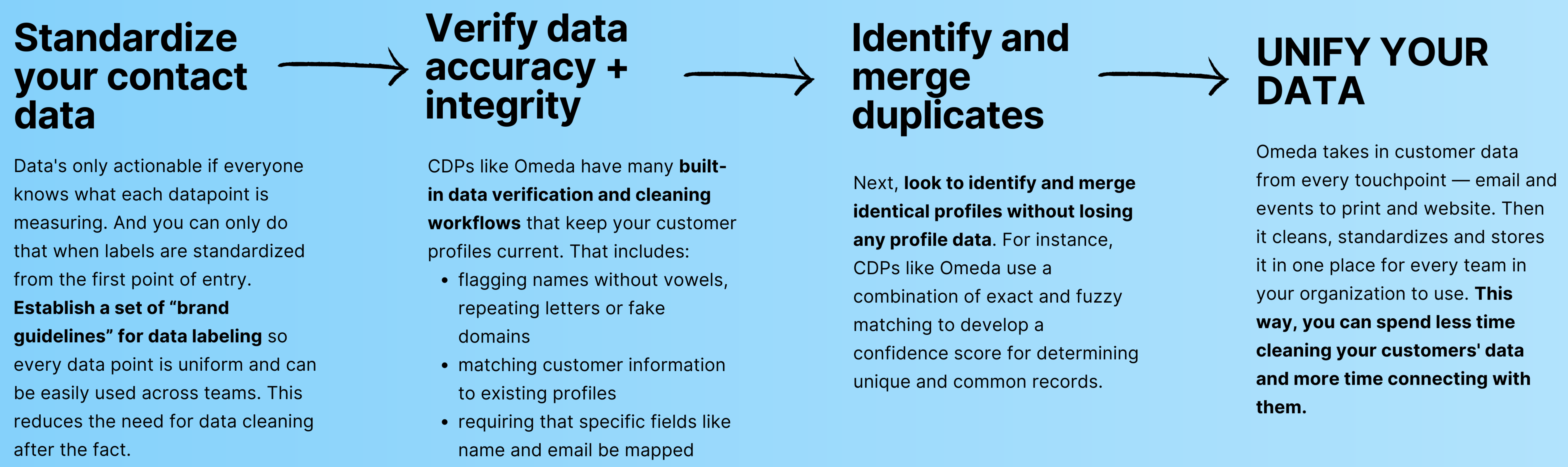
- Employee onboarding/offboarding: ensure access is up-to-date
- Consent management: use ONLY data for which you have a user's permission

Data Minimization

- Only collect and keep what you need
- Align your privacy notice/terms with what you collect

3 Best Practice: Maintain your data

Data Cleanup / Maintenance – Follow these steps to boost your data hygiene:



Standardize your contact data

Data's only actionable if everyone knows what each datapoint is measuring. And you can only do that when labels are standardized from the first point of entry. **Establish a set of “brand guidelines” for data labeling** so every data point is uniform and can be easily used across teams. This reduces the need for data cleaning after the fact.

Verify data accuracy + integrity

CDPs like Omeda have many **built-in data verification and cleaning workflows** that keep your customer profiles current. That includes:

- flagging names without vowels, repeating letters or fake domains
- matching customer information to existing profiles
- requiring that specific fields like name and email be mapped

Identify and merge duplicates

Next, **look to identify and merge identical profiles without losing any profile data**. For instance, CDPs like Omeda use a combination of exact and fuzzy matching to develop a confidence score for determining unique and common records.

UNIFY YOUR DATA

Omeda takes in customer data from every touchpoint — email and events to print and website. Then it cleans, standardizes and stores it in one place for every team in your organization to use. **This way, you can spend less time cleaning your customers' data and more time connecting with them.**

4 Best Practice: Champion privacy & security

Privacy is a team sport

Create champions in each area of your organization:

- Educate on the types of data you hold
- Share how data may or may not be handled in each area of the business

Prioritize security

Security should be a priority for every organization:

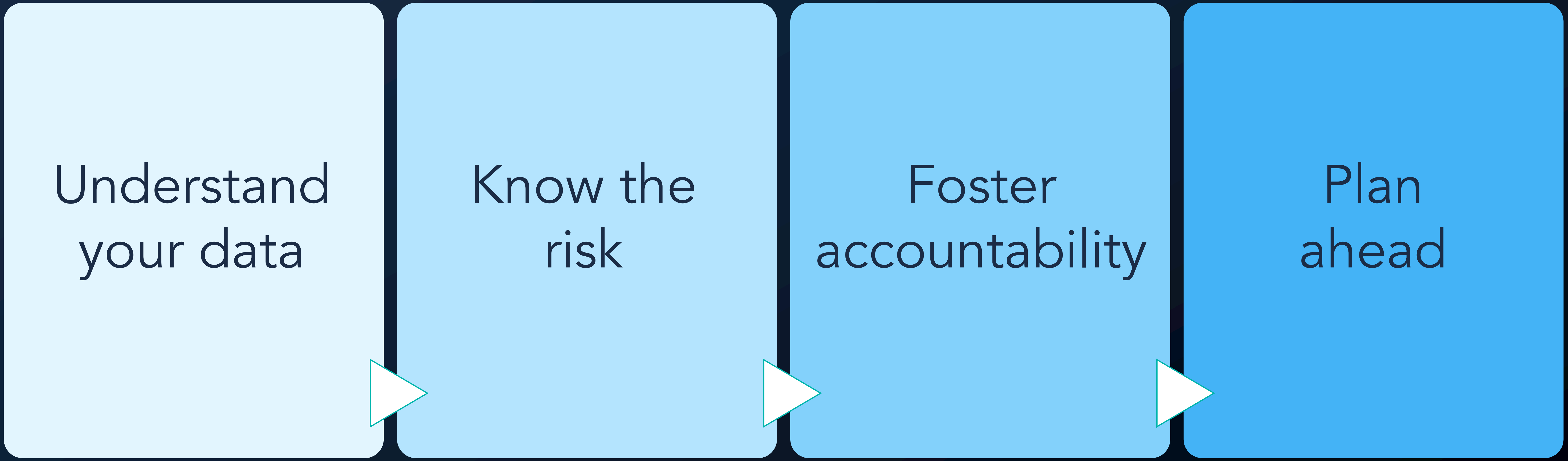
- Train, train, train and test against industry benchmarks to ensure your organization has a solid awareness baseline
- Plan for worst-case scenarios
- Know the most common attack vectors: Phishing (Email), Smishing (SMS), Vishing (Voicemail), etc.

5 Best Practice: Choose the right tech stack

Have a tech stack that supports privacy & security best practices. User technologies to store and manage data that allow:

- Access control & Retention management
- Transparency around processing & what data is attached to a data subject (Customer-centric view)
- Strong opt-in and consent management features that cover BOTH: opt-in AND opt-out

Best Practices Summary



Understand your data

Know the risk

Foster accountability

Plan ahead

omeda

Questions?

omeda

Thank you!

VISIT OMEDA.COM FOR MORE INFO

omeda