IAPP
Privacy.
Security.
Risk.
2019

Training September 22–23
Workshops September 23
Conference September 24–25

LAS VEGAS

LITERATURE HANDOUTS
The California Consumer Privacy Act
The California Consumer Privacy Act of 2018 (CCPA) requires organizations to demonstrate a new level of control and accountability over the personal information of California (CA) consumers. Policies and contracts alone will not allow companies to comply with these requirements. The breadth of this Act underscores how essential automation has become for personal information management.

Dataguise has the enterprise software and the experience to help impacted businesses comply with the CCPA.

Map the personal information of CA consumers
Organize personal information of CA consumers into an inventory of unique identities from across the entire organization.

Track disclosure of CA consumers’ personal information
Identify which third parties access CA consumers’ personal information and what data they process.

De-identify CA consumers’ personal information
Apply masking and encryption to decrease the risk of information before it is used and disclosed.

Control the processing of CA consumers’ personal information
Monitor compliance with identity-level monitoring to control how different entities (internal and external) process personal information.

Dataguise Benefits
Comprehensive
Dataguise supports the broadest range of data and repository types in the industry, both on premises and in the cloud.

Scalable
Proven across some of the world’s largest infrastructure deployments, Dataguise works just as efficiently and effectively for petabytes and terabytes as for bits and bytes.

Agile
Dataguise can accurately discover, protect, and monitor your personal information faster than other solutions on the market.

About Dataguise
We are used by Fortune 500 companies worldwide to discover, protect, and monitor personal information across their enterprise, on-premises and in the cloud. With Dataguise, organizations can focus less on managing risk and compliance, and more on using personal information to improve the products, services, and experiences that fuel business growth. To learn more, visit www.dataguise.com.
Minimize Time to Compliance

Choose Nymity’s Expert Privacy Platform for the GDPR, CCPA, LGPD, and the World’s Privacy Requirements

GET STARTED @ WWW.NYMITY.COM
ONETRUST FOR CCPA:  
A COMPLETE SOLUTION TO IMPLEMENT THE CCPA

Operationalize and Automate CCPA Requirements 
Across Do Not Sell, Consumer Rights, and Privacy Operations

Visit Booth 215 for a Demo

JOIN US FOR A SESSION

The Data Breach vs. The Ethics Breach: 
How to Prepare for Both 

Tuesday, September 24  1:30 p.m. - 2:30 p.m.

Featuring:
Moderator: Kabir Barday, CIPP/E, CIPP/US, CIPM, CIPT, FIP, CEO, OneTrust
James Casey, Associate General Counsel and Chief Data Protection Officer, Akamai Technologies
Mark Surber, Legal Compliance Manager, CIPP/US, MailChimp

‘Do Not Sell’: Comparing and Tackling CCPA and Nevada Requirements

Wednesday, September 25  11:45 a.m. - 12:45 p.m.

Featuring:
Emily Avant, VP, Business Affairs and Governance, WarnerMedia
Kabir Barday, CIPP/E, CIPP/US, CIPM, CIPT, FIP, CEO, OneTrust
Holly Gion, CIPP/US, Director of Data Privacy, Alaska Air
Chris Willard, VP & Chief Counsel, Marketing, Caesars Entertainment
OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

OneTrust DataGuidance is a platform used by privacy professionals to monitor regulatory developments, mitigate risk and achieve global compliance.

Review and compare regulations across multiple jurisdictions at a glance.

Cross-Border Charts help you to easily research and compare data protection requirements globally. Each country and topic is supported by specific Guidance Notes, to provide you with an in-depth analysis of the applicable requirements.

Cross-Border Charts are available on key areas such as:

- General Data Protection Regulation
- California Consumer Privacy Act
- Employee Monitoring
- Data Breach Notification
- Data Transfers
- Employment Record Retention
- Subject Access Requests
- Direct Marketing
- WH521391

Access all Cross-Border Charts HERE
Advanced Privacy and PI Protection
ML-based automation for GDPR and CCPA

Visit our booth #304

BigID

bigid.com  @bigidsecure  info@bigid.com

Smart PI/PII Discovery  AI Driven Classification  Data Subject Rights  Access Governance  Consent Tracking  Data-driven Compliance

schedule demo: bigid.com/demo
Integris Data Privacy Automation

Integris Software, the global leader in data privacy automation, helps enterprises discover and control the use of sensitive data in a way that protects privacy and fuels innovation.

Privacy is now critical to an effective data protection strategy. By sitting upstream from security, Integris tells you what data is important and why so you can be precise in your InfoSec controls.

Integris works securely, at scale, no matter where sensitive data resides. You get a live map of your sensitive data where you can apply policies, surface issues, fulfill data subject access requests, and automate remediations via your broader ticketing and InfoSec ecosystem.

Regulations like GDPR and the California Consumer Privacy Act (CCPA) are triggering knee-jerk reactions as companies lock down their data for fear of misuse. With Integris, there is finally a way to use your data without fear.

How It Works

- **Map**
  Data mapping tells you what data you have and where.

- **Monitor**
  You apply policies to your sensitive data which we continuously monitor for issues.

- **Control**
  We remediate issues by tying into your broader ticketing and InfoSec ecosystem.

- **Search**
  You fulfill data subject requests by running a deep search to locate customer data.

Please contact sales@integris.io to schedule a demo or call Nick Brandreth, VP of sales at 503.701.3702 or nickbr@integris.io
Automated, Scalable Data Privacy Rights Management

There’s a better way to efficiently:
- Fulfill subject access requests (SARs)
- Manage consent preferences
- Deliver data privacy rights

Unlike most privacy tools which only automate part of your workflow or help you manage tasks, Truyo brings true end-to-end automation to your privacy rights operations. Built for the enterprise and backed by industry leaders.

truyo.com/IAPP
Where is your data traveling?
Cisco Webex Meetings Data Map

For full details, please refer to the corresponding Privacy Data Sheet

Data Input
- Customer
  - Users generate data (including recordings & files)
- Subprocessor
  - Contract

Data Processing
- Admin / Logistics
- Provide Services
- Service Related / Others
- Data can be viewed, modified, deleted by user preferences or Customer policy
- User can view their content with other platforms
- Create account, enable use of service features
- Providing the Service and enabling the use of certain features
- Improve the Service
- Third parties may retain data at different rates depending on specific usage and needs

Deletion Timeline
- No retention
- Days
- Weeks
- Months
- Years
- By request

Personal Data Processing
- Registration data
  - Name, Email Address, Password, Public IP Address, Browser, Phone Number (optional), Mailing Address (optional), Avatar (optional), Billing Information
- User-generated data
  - Meetings and Call Recordings, Uploaded Files
- Hosting and usage data
  - IP Address, User Agent Identifier, Hardware Type, Operating System Type and Version, Client Version, IP Addressess Along the Network Path, MAC Address of Your Endpoint (if applicable), Service Version, Version Details, Meeting Session Information (title, date and time, frequency, removal and email distribution, ongoing status, website action, network connection), Number of hosts, Guest Name, Screen Resolution, Join Method, Performance/Troubleshooting/Diagnostics Information

Access Key
- Icons on the right show who has access
- Details of access are listed in the datasheet
- What’s being done
- User
  - Customer
  - Cisco
  - Subprocessor
- Columns show category of purpose
- Rows show who processes the data
- Text inside indicates purpose

Data Center Locations
- Amsterdam, Netherlands
- Bangalore, India
- Beijing, China
- Berlin, Germany
- Hong Kong, China
- London, UK
- New York, USA
- Singapore, Singapore
- Sydney, Australia
- Tokyo, Japan
- Toronto, Canada
- Virginia, USA
- trust.cisco.com
- Cisco Public © 2019 Cisco and/or its affiliates. All rights reserved.
CCPA Requires Companies to Implement Reasonable Security

The California Consumer Privacy Act (CCPA) sends companies a clear message: implement “reasonable security” or pay the price...

Starting January 1, 2020, CCPA establishes a private right of action for consumers whose personal information is breached resulting from a company’s failure to implement “reasonable security procedures.”

$100  $750
PER INDIVIDUAL or
ACTUAL DAMAGES
FOR SECURITY INCIDENTS

ACHIEVING REASONABLE SECURITY

What Does “Reasonable Security” Look Like in Practice?

There’s no one size fits all security program. The threat landscape is ever changing. How to organizations find the right balance?

“Reasonable” is a level of security appropriate to the sensitivity of the information.

Safeguards should be in line with the sensitivity of the information, and informed by the risk of harm that would result from a compromise.

Prepared companies will use cybersecurity risk assessments to find the level of security appropriate to their environment

The answer comes from an evaluation of cyber risk to:
• Identify threats and vulnerabilities
• Assess the likelihood of occurrence and impacts
• Consider benefits gleaned from implementing a control vs. the costs of those safeguards

Where the benefits outweigh the costs the control is reasonable.

Visit us at booth 318 to learn more about our approach to security.
We create trust through transparency

Google Cloud offers detailed data processing and security related terms that describe our commitment to protecting your data. These terms, which are available for you to review on our website, reflect the following important commitments:

- We implement and maintain state-of-the-art technical and organizational measures to protect customer data
- We maintain certifications against international standards for information security and privacy
- We notify customers promptly if we become aware of a security incident
- We only process customer data in accordance with our customers’ instructions

GCP Data Processing and Security Terms: cloud.google.com/terms/data-processing-terms

GSuite Data Processing Terms: gsuite.google.com/terms/dpa_terms.html

We are your trusted partner in security. We created and abide by six trust principles that guide our end-to-end security model so you can:

1. Know that your security comes first in everything we do.
   We promptly notify you if we detect a breach of security that compromises your data.

2. Control what happens to your data.
   We process customer data according to your instructions. You can access it or take it out at any time.

3. Know that customer data is not used for advertising.
   You own your data. Google Cloud does not process your data for advertising purposes.

4. Know where Google stores your data and rely on it being available when you need it.
   We publish the locations of our Google data centers; they are highly available, resilient, and secure.

5. Depend on Google’s independently-verified security practices.
   Our adherence to recognized international security and privacy standards is certified and validated by independent auditors - wherever your data is located in Google Cloud.

6. Trust that we never give any government entity "backdoor" access to your data or to our servers storing your data.
   We reject government requests that are invalid, and we publish a transparency report for government requests.

See the data processing terms for G Suite and Google Cloud Platform for further details.

Learn more about how Google protects the privacy of business’s data at privacy.google.com/businesses

©2019 Google LLC
Promote privacy, differentiate, build trust and grow your business

Proliferating privacy regulations have organizations struggling to protect personal data.

— **Build a strong data privacy program**
  Implement a holistic, continuous and dynamic privacy foundation.

— **Gain privacy insights**
  Increase visibility into risks and use privacy insights to generate business impact.

— **Automate privacy controls**
  Protect personal data at rest and in motion, on premises and in the cloud.

IBM Security solutions
- IBM Security Guardium
- IBM Security Guardium Analyzer
- IBM Data Risk Manager
- IBM Cloud Identity
- IBM Resilient Security Orchestration, Automation and Response (SOAR) Platform
- IBM Data Privacy Services
- IBM Promontory

Join us at booth #307

Learn more
PRIVACI is the world’s first PrivacyOps platform that helps automate all major functions needed for privacy compliance in one place.
Manage Compliance for CCPA, GDPR, HIPAA and Other Privacy Regulations

TrustArc Privacy Compliance Solutions

Privacy Platform
- Data Inventory Hub
- Assessment Manager
- Cookie Consent Manager
- Website Monitoring Manager
- Marketing Consent Manager
- Individual Rights Manager
- Ads Compliance Manager

Privacy Consulting & Training
- Compliance Assessments
- Vendor Risk Management
- DPIA / PIA Program Development
- Breach Response Plans
- Policies and Procedures
- GDPR and CCPA Implementation
- Employee Privacy Training

Privacy Certifications
- GDPR Validation
- EU Privacy Shield Verification
- APEC CBPR and PRP Certification
- Children's / COPPA Certification
- TRUSTe Enterprise Certification
- EDAA Certification
- Dispute Resolution Service
Find the perfect balance with our Privacy by Design Consultancy

Our expertise in technology, infosecurity and data privacy legislation, enables us to Analyze, Design and Deliver your IT project, ensuring it’s neither constrained nor neglectful of privacy obligations.

**Analyze**
Your dedicated team of Privacy Architects will assess the IT and business objectives of the project as well as identify the privacy regulations it is subject to.

**Design**
We will guide you through the design of the service, ensuring balance between performance requirements and regulatory obligations.

**Deliver**
The team will provide ongoing assessments of performance and the service or application’s adherence to data privacy requirements.

For more information or to enquire about our Privacy by Design Consultancy visit: www.calligo.cloud/privacy-by-design
Our breach response services can be tailored to fit your needs. We ensure a timely and managed response and provide peace of mind to those affected.

ID Experts at a glance:
- Protecting more than 30 million Americans
- Largest provider of identity protection services to the federal government
- Highest level of government certified security built into our MyIDCare software
- 96% of our clients would recommend ID Experts and would select us again.
Make sure your workforce is actively protecting sensitive data.

MediaPRO’s privacy training solutions are used by organizations of all sizes to protect sensitive data, demonstrate compliance, and reduce the risk to their reputation and bottom line.

- Pre-Assessment Functionality
- Reinforcement Materials
- Tailor Courses
- Microlearning Courses
- Customer Success Manager
- Phishing Simulator*
- Additional Languages*
- MediaPRO Customization*
- Learning Management System (LMS)*

Learn More at MediaPRO.com

*Optional
Privacy, risk, security?

**WE HAVE THE SOLUTION FOR YOU.**

With more cyberthreats everyday, your clients need more protection than ever. To help safeguard your clients’ personal information in today’s evolving digital universe, Norton LifeLock has a new solution for Breach Response. As part of Symantec, we are backed by the world’s largest civilian cyber intelligence network allowing us to see and protect against advanced cyber threats.

You can trust our team to help safeguard your client’s personal information in today’s evolving digital universe. Our Breach Response Services include:

- **LifeLock Identity Theft Protection**
- **Call Center Services**
- **Breach Notification**
- **Norton Security Deluxe (90-Day Subscription)**
- **Call Center, Enrollment and Notification Metrics**

We have a dedicated Cyber Risk Executive to assist you through the process. Your clients will get 24/7 agents, Dark Web Monitoring, an agile Mobile App and much more.

No one can prevent all identity theft or cybercrime.

VISIT BOOTH 218, OR CONTACT A CYBER RISK EXECUTIVE: 844-698-8647 OR LIFELOCK.COM/BREACH
Privacy Management Software
Less Work, More Automation

Data Mapping
Automated data discovery and mapping allows you to locate customer PII quickly.

Subject Access Rights
Provide customers and users the ability to access and delete their data.

Vendor Management
Identify and manage PII data flows to your vendors.

Consent Management
Collect customer preferences and opt-outs to improve trust.

Transparency
Ensure users understand your privacy practices.

Automation
Make privacy compliance easier.

Privacy Audits
Check enterprise compliance requirements against actual practices.

Recordkeeping
Maintains audit trail and demonstrate compliance with privacy requirements.

+ DATA RISK Intelligence!

Get Ready for the CCPA!

Find out more at www.clarip.com or call us toll free at (888) 252-5653

BOOTH #119

iMac Giveaway
The creation of state privacy laws is a constantly-changing landscape. Without a federal privacy law, states are proposing their own individual laws and they vary widely. Some focus on internet and social media privacy, some focus on general consumer privacy protection, but all of them will affect companies doing business in the US.

Consumers in the US will now be able to request that their data not be shared, sold, or collected. They can request that their data be deleted outright or edited. But not under every new state law. Meanwhile, businesses have a variety of new obligations, such as data breach notifications, processing limitations and more. But not in every state.

How can you, as a company, identify what applies to you?

Stop by booth 406 to discuss how we can help you with managing consumer privacy rights!

Consulting Services: Maintaining compliance with the growing data and privacy regulations is daunting. CompliancePoint provides the following consulting services related to CCPA and other emerging states’ rights:

- Determine if and how each specific state legislation applies to you
- Conduct a data mapping process to locate data and document how it is used
- Establish what you should be doing today to prepare for CCPA and other emerging regulations
- Improve your overall security and compliance position

Technology: Our OnePoint Privacy Management Solution is a compliance automation tool that allows you to enhance your privacy programs by allowing you to quickly stand up a consumer privacy request portal. OnePoint’s robust workflow engines will manage consumer privacy requests across your organization, including defining workflows, tasks, and assigning task owners for completing the steps necessary to satisfy the consumer rights.

Consumers are provided access to the Consumer Privacy Request Portal which allows them to submit requests related to their privacy rights including Right to Access, Deletion, Disclosure of Information Collected, Disclosure of Information Sold and to the Right to Opt-out. They are provided a confirmation code to track the status of their request and are notified when it is completed.

Upon completion of a set of tasks or workflows, an auditor can view all work, evidentiary data articles, and other documentation related to the completion of a task and approve it or reject it if it doesn’t meet the required standard. All evidential artifacts are stored in a central repository for validation and audit purposes.
The only purpose-built platform for sustained privacy compliance.

DataGrail's direct integrations make data mapping, in the traditional sense, an obsolete need. Our live data map is automatically updated and continuously refreshed.

**Live Data Inventory and Mapping**

DataGrail orchestrates the tedious task of processing and fulfilling data subject requests. Eliminate manual processes, emails and workflows.

**Process Requests In Minutes**

DataGrail is the only company that directly integrates with 100+ business systems, like Marketo, Oracle, Zoom, Salesforce, Coupa, Okta, making for a seamless and easy onboarding process.

**No Code Onboarding**

View the status of all requests from a centralized system, where you can manage personal data across your entire business.

**Instant Visibility**

DataGrail is the only company that directly integrates with 100+ business systems, like Marketo, Oracle, Zoom, Salesforce, Coupa, Okta, making for a seamless and easy onboarding process.

**Delight Customers & Reduce Unsubscribe Complaints**

Unify customer email preferences with a company-wide preference management system.

---

"Every business runs on technology and every company has customer data. Third-party systems, particularly in the sales, marketing, and adjacent spaces, were not built to be GDPR and CCPA compliant. DataGrail provides control and transparency to comply with these laws efficiently and effectively."

Mallun Yen, COO & Co-founder at SaaStr

"I don’t know how many emails (we) get but if we had to keep track of all the data subject requests, there would be a high likelihood something would fall through the cracks."

Justin Olsson, Associate General Counsel, Product & Privacy at Databricks

---

**Trust**

- Scale seamlessly with new regulations
- SOC 2 compliant
- Compliance log maintenance

**Trusted by**

- Intercom
- Outreach
- Plexus
- Sendoso
- Sales Hacker
- SaaStr

**datagrail.io/demo-iapp**
PERFORMANCE. RELIABILITY. CONSISTENCY.

EXPERIENCE

For more than 30 years, Kingston has been an integral component in the IT backbone of Fortune 500 companies. An experienced business solutions partner, Kingston offers products with consistent and reliable performance along with award-winning solutions required by enterprise environments.

DID YOU KNOW?

If a USB is lost or stolen and the data on it is encrypted then this is a Security Breach not a data breach and may not have to be reported.

Visit Booth Number: 219

Ultimate Security
Encrypted USB Drives

Enterprise Solid-State Drives (SSD)
Incredible Speeds & Rock Solid Reliability

Server Memory
Accelerate Performance

Server Virtualization
IT Applications
EMPOWERING BUSINESS THROUGH TECHNOLOGY

VISIT PROTIVITI AT BOOTH 410

Protiviti’s Data Security and Privacy services help companies preserve business value by protecting sensitive data and ensuring compliance with respective regulations. Our offerings address the design, implementation and assessment of technical and procedural controls focused on identification, classification, protection and compliance for sensitive data. *We bring expertise in security and privacy regulations as well as innovative approaches for reducing compliance obligations and risk.*

UNDERSTAND PERSONAL INFORMATION CATEGORIES …

<table>
<thead>
<tr>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal Identifiers &amp; Biometric Information</td>
</tr>
<tr>
<td>Financial Records &amp; Purchasing Information</td>
</tr>
<tr>
<td>Online Identifiers &amp; Online Activity</td>
</tr>
<tr>
<td>Geolocation Information</td>
</tr>
<tr>
<td>Healthcare Insurance &amp; Medical Records</td>
</tr>
<tr>
<td>Individual Profile &amp; Protected Characteristics</td>
</tr>
<tr>
<td>Education, Professional &amp; Employment-Related Information</td>
</tr>
</tbody>
</table>

MEET OUR EXPERTS AND LEARN HOW TO …

- Design, implement, operationalize and validate data security and privacy programs including programs supporting PCI, HIPAA, GLBA, CCPA or FTC compliance requirements
- Help execute third-party/vendor security programs
- Implement data governance and protection

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 75 offices in over 20 countries.

CONTACT US:

- Jeff Sanchez
- Kevin Strope

Protiviti.com/GDPR
Security Compromises are Increasingly Privacy Compromises and Vice Versa

Large volumes of intellectual property and personally identifiable information are stolen, leaked, or corrupted every year. As more sensitive and confidential information becomes exposed, more data privacy laws emerge at state, federal, and global levels. Security and privacy continue to converge, with unauthorized data access introducing new and pressing business challenges.

Visit Virtru at booth #407 to learn how to gain a competitive advantage while advancing both security and privacy through data sharing.

About Virtru
At Virtru, we understand that data is an organization's most valuable asset and sharing it is critical for business success. But sharing data creates significant risk. We believe no one should have to choose between protecting data and sharing it. We help more than 5,000 organizations, large and small, across almost every industry, protect data wherever it's created or shared so they can collaborate with confidence. Virtru provides the power to get the job done. For more information, visit www.virtru.com or follow us on Twitter at @virtruprivacy.
Wirewheel's platform is your end-to-end path to compliance helping your organization comply with today's CCPA and GDPR requirements while remaining ready for any future regulatory regimes, minimizing legal risks and reducing time & effort it takes to respond to data subject requests.

**WIREWHEEL CAN HELP YOU:**

- Verify and Authenticate All Requestors Identities
- Track, Review, and Approve Requests
- Automatically Ticket and Assign Requests
- Collect, Manage, and Review Internal Data to Fulfill Requests
- And, encrypt and Securely Deliver Information

Visit us at **Booth #502** to learn how WireWheel can simplify, structure, and automate your management of Subject Rights Requests.

[www.wirewheel.io](http://www.wirewheel.io)
CENTRL’s Privacy360 is an enterprise privacy compliance management platform. It is scalable and adaptable to current and evolving privacy management requirements worldwide, including compliance requirements for the GDPR, ePrivacy, and the California Consumer Privacy Act. The CENTRL platform scales for large organization enterprise needs and is flexible enough for companies of all sizes. It is easy to get up and running with minimal configuration and implementation effort. The CENTRL solution has a full suite of modules for privacy compliance – spanning assessments, data mapping, data subject rights management and consent management, while including complete third party and vendor risk management capabilities to complement an enterprise’s privacy management needs.

Privacy360 is purpose built to help companies achieve compliance with multiple privacy regulations. The platform currently comes in two editions: GDPR Edition and CCPA Edition. Privacy360 consists of several core modules that are highly flexible and can be configured to specific privacy regulations or be used to comply with multiple regulatory requirements.

- **Individual Rights Management**
  - Customizable request intake form that can be branded and tailored to client requirements
  - Communicate within a secure portal with configurable access limits and data retention
  - Simplify execution with communication templates, task management, assignment rules, and automatic reminders
  - Automate disclosures and task creation for internal users and third parties with data inventory lookups
  - Connect to external systems and APIs to fulfill requests and verify subject identity

- **Data Mapping & Data Inventory**
  - Map of all processing activities including the personal data categories, data elements, purpose of data collection, systems and locations where personal data resides
  - Dual approach to automation: eDiscovery tools and survey harvesting to populate and maintain your data inventory
  - Visualize the flow of data across your systems and to third parties with whom personal data is shared and sold

- **Assessment Automation**
  - Conduct assessments on internal processes, service providers and third parties to determine security and privacy gaps
  - Create action plans to remediate issues and ensure that all necessary controls are implemented internally and at partners
  - Save time by populating previous answers and tracking what has changed
  - Collaborate with internal users and third parties to create, evaluate, and respond to assessments

- **Enterprise Ready**
  - Configure processing activities, subject access requests, and data maps with custom attributes to meet your specific business needs
  - Secure with advanced role-based access, single sign-on, and comprehensive data encryption
  - Choose where to host data to meet residency requirements

- **Reporting & Analytics**
  - Comprehensive business intelligence suite to manage and monitor your data inventory and subject access requests
  - 360-degree view of processing activity by data subject, data categories, systems, third parties, and other attributes
  - Operational dashboard to track day-to-day activity like consumer request backlog, risk activities, and statuses of assessments
  - Executive-level dashboard to manage GDPR, CCPA and other laws’ privacy compliance across the organization

For more information visit [oncentrl.com](http://oncentrl.com)
Schedule a demo at [oncentrl.com/request-demo](http://oncentrl.com/request-demo) or call 877.367.9094
The Only Identity and Credential Verification Platform that Prioritizes Privacy

- Distributed Data Model
- End-to-End Encryption
- Cryptographically-Enforced ACLs
- Enables Data Minimization
- Embeds Privacy by Design and Default
- 6,500+ Authoritative Data Sources
- Supports Compliance with Global Data Protection Regulations

BOOTH #105
evidentid.com
Is this data breach notifiable?
Cut your incident response efforts in half

**Reduce Risk**
Consistent incident risk scoring and notification guidance eliminates subjectivity and over-reporting

**Save Time**
Automated guidance based on state, federal, and global data breach notification regulations

**Build Trust**
Make correct breach notification decisions, every time. Protect your brand from reputational risk