THE VALUE OF 168

Legal & Compliance Meeting
Sensitive Personal Data

Jessica L. Medvec
Director of Legal and
Compliance Counsel

February 10, 2021

Personal Data

Personal data has slightly different definitions depending on the jurisdiction

Generally, you should consider any information that identifies or relates to an individual to be personal data

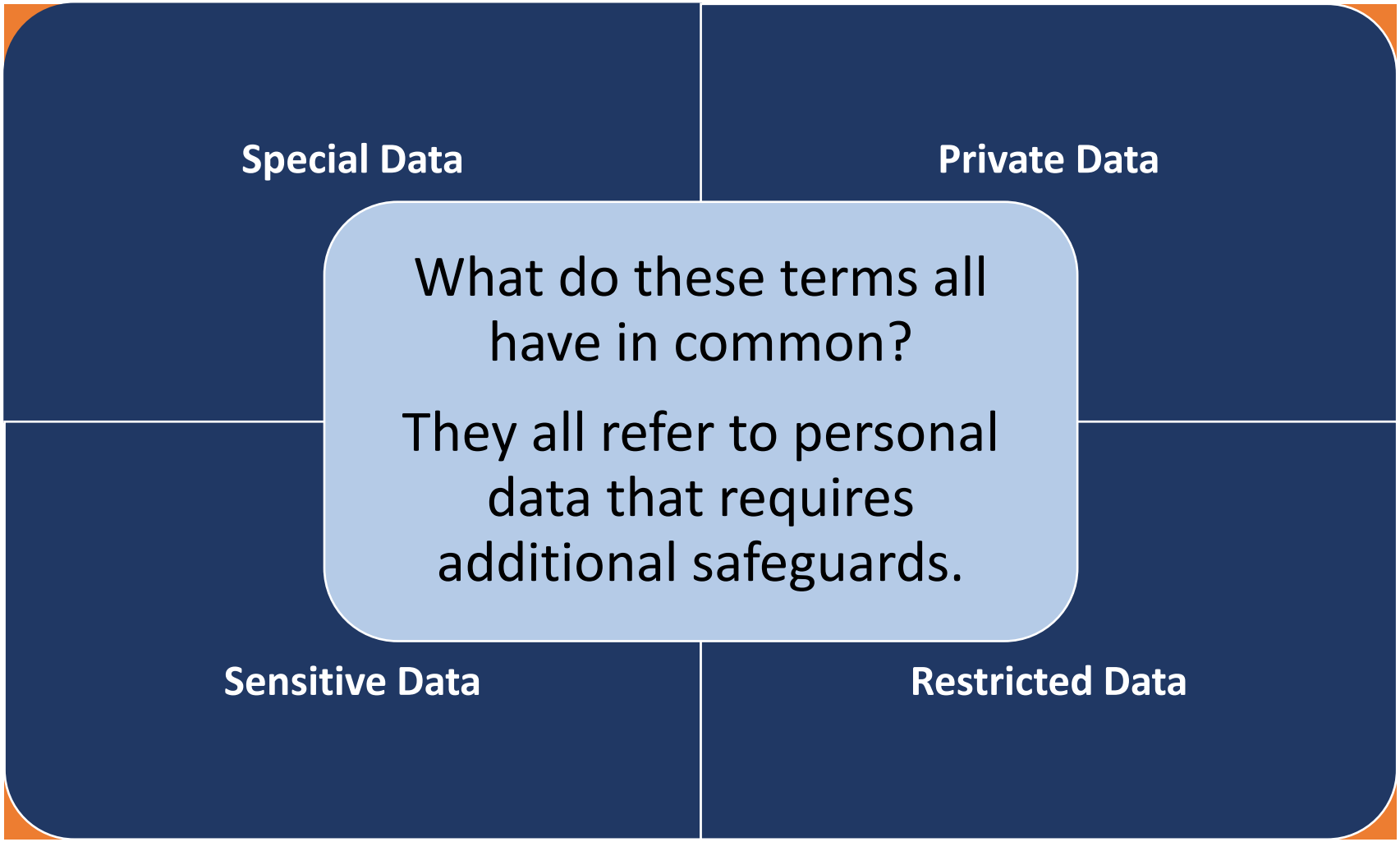
The data doesn't have to be obvious- if it can be connected with other accessible information and links back to an individual-it counts

Some Common examples of personal data include: a person's name, home address, email address, date of birth and image

Is there any information that is NOT personal?

- Data that has no connection to a living person
- Mathematical equations
- Aggregated information
- Anonymized information
- Business information
- Information that is not processed in the context of a commercial transaction

Personal Data Categories



What Does it all Mean?

Different jurisdictions may use different terminology to classify data categories

The thing to remember:

- Any information that, if publicly released, has the potential to lead to harm, such as discrimination, identity theft or financial fraud, is almost always held to a higher standard of care
- This information has the potential to significantly and negatively impact an individual
- The greater the risk of harm the more protection required
- In some instances explicit consent is required prior to collection and/or processing of sensitive data

Examples of Sensitive Data

- Race
- Sex Life
- Health Information
- Financial Information
- Government Issued ID
- Criminal Background
- Trade Union Membership
- Political or Religious Affiliations
- Biometric Data

Employee Sensitive Personal Data

Businesses have large amounts of sensitive personal data about employees. Some examples include:

- Employment contracts
- Offer letters
- Benefits information
- Lists of next of kin
- Medical Information, including COVID related screenings

What Should We Do with Sensitive Data?

- **Know why and where you have it.** *[DPIA]*
  - Only collect it if its necessary
- **Physically protect it.**
  - Paper documents can also contain sensitive data
- **Electronically protect it.**
  - Secure it in all stages of its electronic life
- **Contractually protect it.**
  - Include a DPA
- **Limit its Transfer and Access**
  - Only send it and/or share it when necessary
- **Minimize Retention of it.**
  - Don’t keep sensitive data for longer than you need it

What Should We Do if There is a Problem?

- **Speak Up**
- **Report Incidents.** https://rpminc.ethicspointvp.com/custom/rpminc/forms/mgr/form_data.asp?lang=en
- **Contact Your Group Lawyer**
- **Be Transparent with Your Lawyer, IT & Compliance**
- **Refrain From Deleting**
- **Don’t Discuss Incidents with Outside Parties without Clear Direction**

THE VALUE OF 168

Jessica L. Medvec
Director of Legal and Compliance Counsel
RPM International Inc.
2628 Pearl Rd.
Medina, Ohio 44258
Jmedvec@rpminc.com
Office: (330) 273-8894
Cell: (330) 241-9116

THE VALUE OF 168

Legal and Compliance Meeting 2021

Sunny Sandhu
Data Subject Access Requests

10 February 2021

Data Subject Access Request (DSAR) UK Example…..

Jim has been an employee of RPM for 15 years. He is a manger in a manufacturing plant. He has been having difficulties with one of his team, who Jim believes is stealing. Unfortunately the CCTV footage in the plant is inconclusive, but nonetheless Jim believes that he has enough evidence and calls Bob into a disciplinary meeting. The meeting does not go well and Bob storms out. Following advice from a solicitor, Bob brings a claim against RPM for constructive dismissal.

Two days after submitting his claim, Bob sends a Data Subject Access Request Letter to HR requesting all the information RPM has on him.

Please consider the following:

- What are your next steps?
- How should you respond to Bob?
- Do you have to provide all the information requested?
- What do you do if the data includes details of other employees?

Data Subject Rights

- Rights of **access and information:**
  - Is personal data being processed
  - information provided on collection
  - information on source of personal data (where not collected from data subject)
- Right to have **inaccuracies rectified** without undue delay
- Right to **erasure** of personal data, including where:
  - data no longer necessary in relation to purposes for which collected
  - consent is withdrawn and no other ground for processing applies
  - unlawful processing

Data Subject Rights (Cont'd)

- Right to **restrict processing:**
  - accuracy of data is contested
  - processing is unlawful
- Right to **data portability:**
  - allows individuals to move their data to another controller
  - in a structured, commonly used and machine-readable format
- Rights to **object** to:
  - processing on basis of "legitimate interests", including profiling
  - a decision based solely on automated processing, including profiling, unless
  - processing is necessary for entering into or performing a contract
  - decision is based on explicit consent

What does a request look like?

"Please may I have copies of all of my personal data from the beginning of time until the present day on absolutely everything and anything?"

I would like access to ….. ?

How do we verify someone's identity?

What is personal data?

Scope of request?

Third party checklist

- Can consent be requested/given?
- Is it reasonable to disclose without consent?

Consider:

- duty of confidentiality
- steps taken to seek consent
- any refusal to give consent

"You must not apply a blanket policy of withholding third party data".

Code of Practice

Tick tock .....

- Waiting to receive ID verification?
- When can we extend the timeframe?
- What amounts to a 'complex request'?

"Any decision should reflect the fact that the right of subject access is fundamental to data protection"

Code of Practice

'Just say no?'

- When is a request ‘manifestly unfounded’ or excessive?
- What do we do if the decision is 'no’?
- What about archived and deleted data?

"While the principle of proportionality cannot justify a blanket refusal to comply with a SAR, it does limit the scope of the efforts that a data controller must take in response": Ittihadieh

Annoying and Annoyed

Other considerations:

- Interaction with grievance and disciplinary processes
- Litigation Privilege
- Settlement agreements and waiving DSAR

Data Subject Access Request (DSAR) Example.....

Jim has been an employee of RPM for 15 years. He is a manger in a manufacturing plant. He has been having difficulties with one of his team, who Jim believes is stealing. Unfortunately the CCTV footage in the plant is inconclusive, but nonetheless Jim believes that he has enough evidence to go on and calls Bob into a disciplinary meeting. The meeting does not go well and Bob storms out. Following advice from a solicitor, Bob brings a claim against RPM for constructive dismissal.

Two days after submitting his claim, Bob sends a Data Subject Access Request Letter to HR requesting all the information RPM has on him.

Please consider the following:

- What are your next steps?
- How should you respond to Bob?
- Do you have to provide all the information requested?
- What do you do if the data includes details of other employees?

THE VALUE OF 168

ANY QUESTIONS?

THE VALUE OF 168

Data Processing Agreements/Addendums/Provisions

Tracy D. Crandall
Vice President, Associate General Counsel and Assistant Secretary

February 10, 2021

What

- **What is a Data Processing Agreement (Addendum, Provision)?**

- Whether we call it a DPA or there is a provision about data privacy in your service agreement with a vendor, any contract language that addresses a service provider's duties to protect personal data is a data processing agreement.
- While DPAs address data security, this is not necessarily intended to be a data security requirements document.

- **Where can I find a DPA form?**

- http://rpmpolicies.rpminc.com/media/1196/data-processing-addendum.pdf

When/Why do you need a DPA?

- A third party (vendor) maintains, accesses, stores or processes personal data for the Company (a “Data Processor”)
- Cloud Storage Providers, IT Service Providers, Software as a Service Vendors, Payroll Processors, ERP Providers and HRIS Providers are all Data Processors

Know Your Supplier (Due Diligence)

- **What to do before the DPA?**
- Review Data Processor personal data security measures -- work with IT to evaluate against our minimum security measure requirements
  - Meet or exceed ISO/IEC 27001:2013 or
  - Standards substantially similar
  - At a minimum, commercially reasonable standards for the Data Processors in that industry
  - Needs to include network and system security monitoring, authentication and access controls, and encryption protocols designed to protect personal data

What To Do Before Engaging

- **What does the DPA need to say?**
  - Contain minimum security requirements
  - Require that the Data Processor only process our data on instruction from Company
  - Requirement to keep our data Confidential
  - Requirement to immediately notify Company of breaches and assist Company related thereto
  - Requirement to obtain company Consent to subprocess or transfer data
  - Audit Rights

THE VALUE OF 168

THE VALUE OF 168

Legal and Compliance Meeting 2021

Brian Frasier
Director Global Compliance

Policies, Resources & Projects

Available Policies & Resources

- Password Policy
- Cookies Banner Policy
- Data Processing Addendum
- Direct Marketing Guidance – Dos & Don’ts
- EEA Employee Privacy Rights Notice Policy
- Employee Data Privacy Policy (US/Canada
- Encryption Instructions
- Encryption Instructions
- Employee Data Privacy Policy (US/Canada
- Global Data Protection Policy
- Individual Rights Guidelines Champion Policy
- Privacy by Design Guidelines
- Subsidiary Employment Applicant Privacy Notice
- Website Privacy Policy

Available Policies & Resources

Where to Find Them?

Available Policies & Resources

The RPM website!

https://rpmpolicies.rpminc.com/rpm-policies/

- These policies and resources and all RPM policies are on the RPM website. However, you can only access them by having this link.
- Periodic Data Privacy related posters
- Questions on any of the Data Privacy topic or documents, can be emailed to the Legal and Compliance department at: dataprotection@rpminc.com.

One Trust - Update

OneTrust Privacy

PRIVACY MANAGEMENT SOFTWARE

Assessment Automation

Operationalize privacy by design, PIAs, DPIAs to achieve and maintain compliance.

DataGuidance

Access a central repository of research, regulatory guidance, best practices and news.

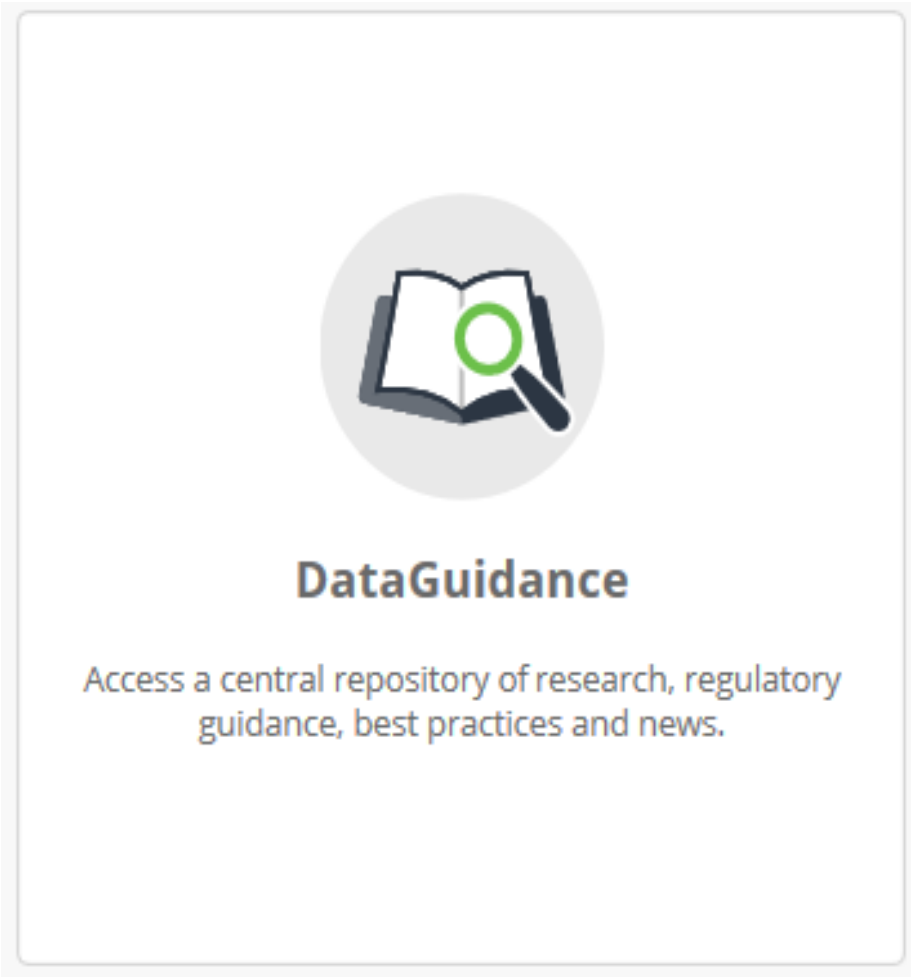
Data Mapping

Maintain an evergreen map of data flows and complete records of processing.

Cookie Compliance

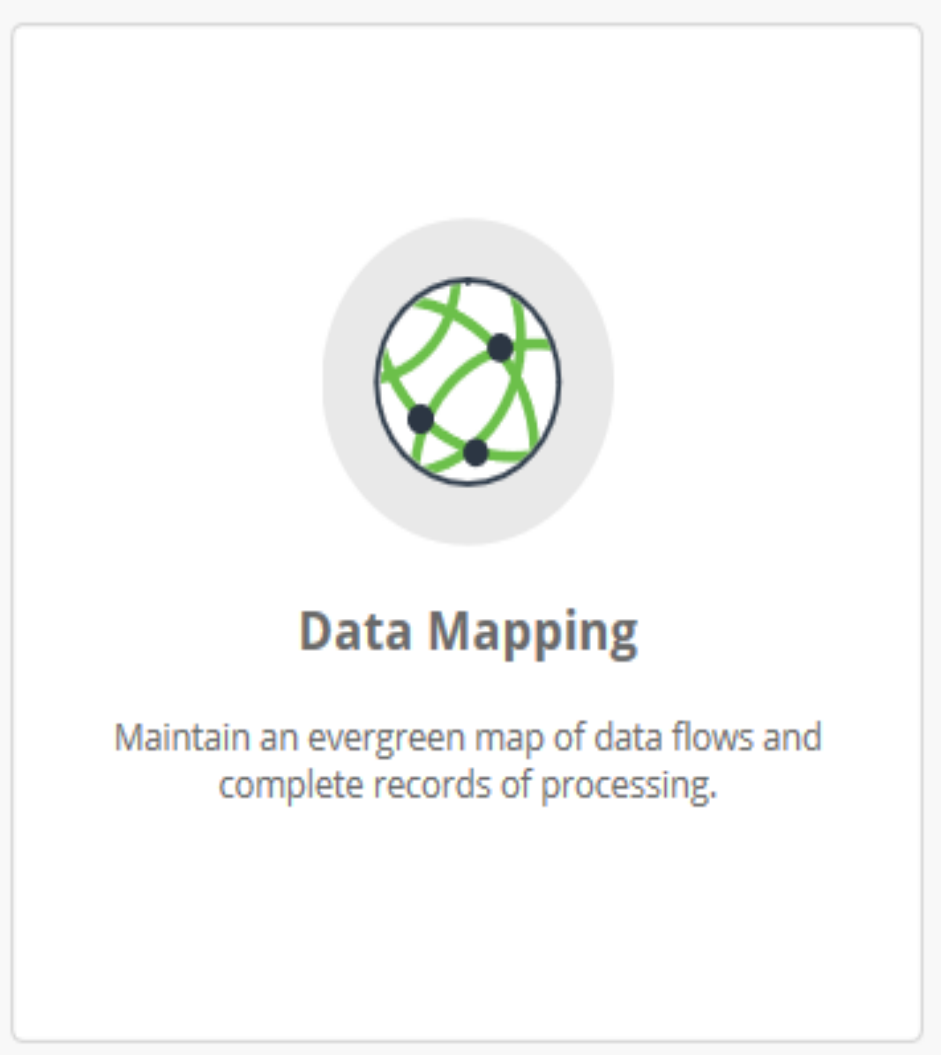
Generate a geo-specific cookie banner, preference center and cookie policy.

One Trust – Data Guidance



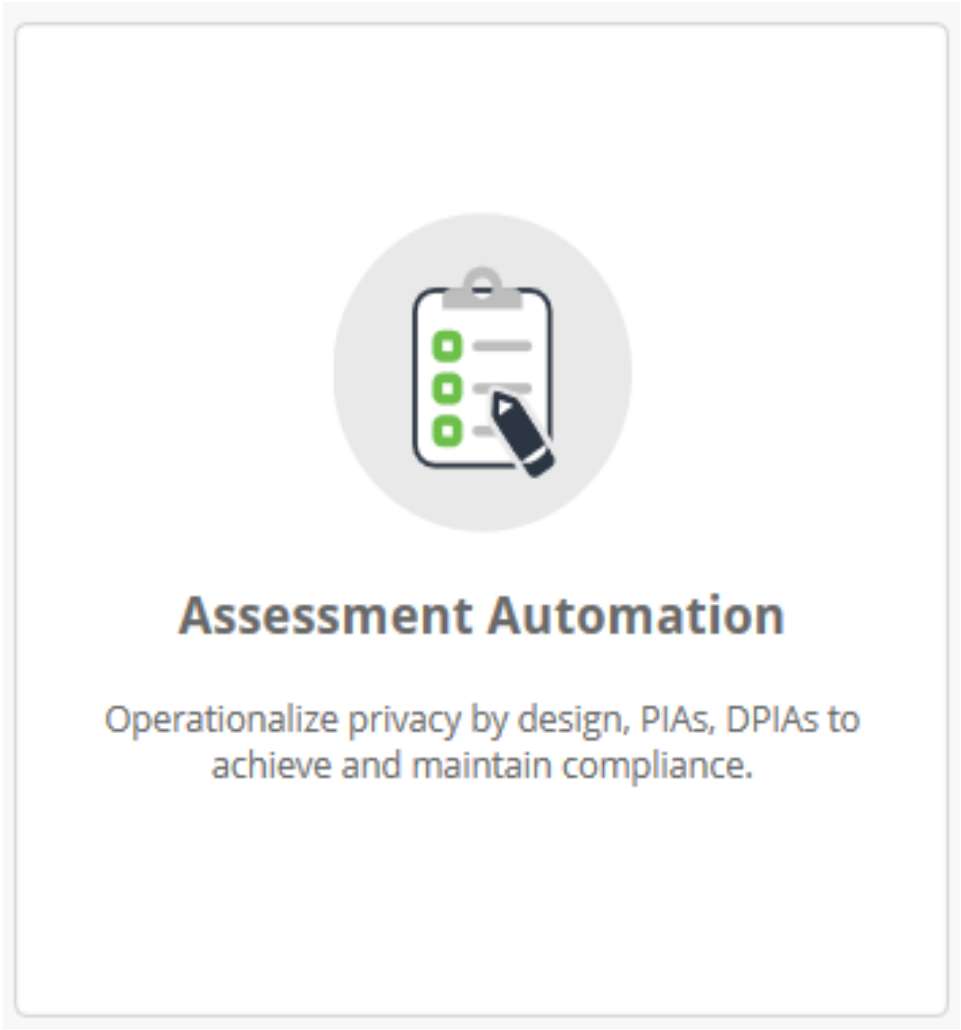
Assists in making sure we stay in the know on a rapidly changing landscape of various countries and states enacting their own data privacy laws and regulations.

One Trust - Data Mapping



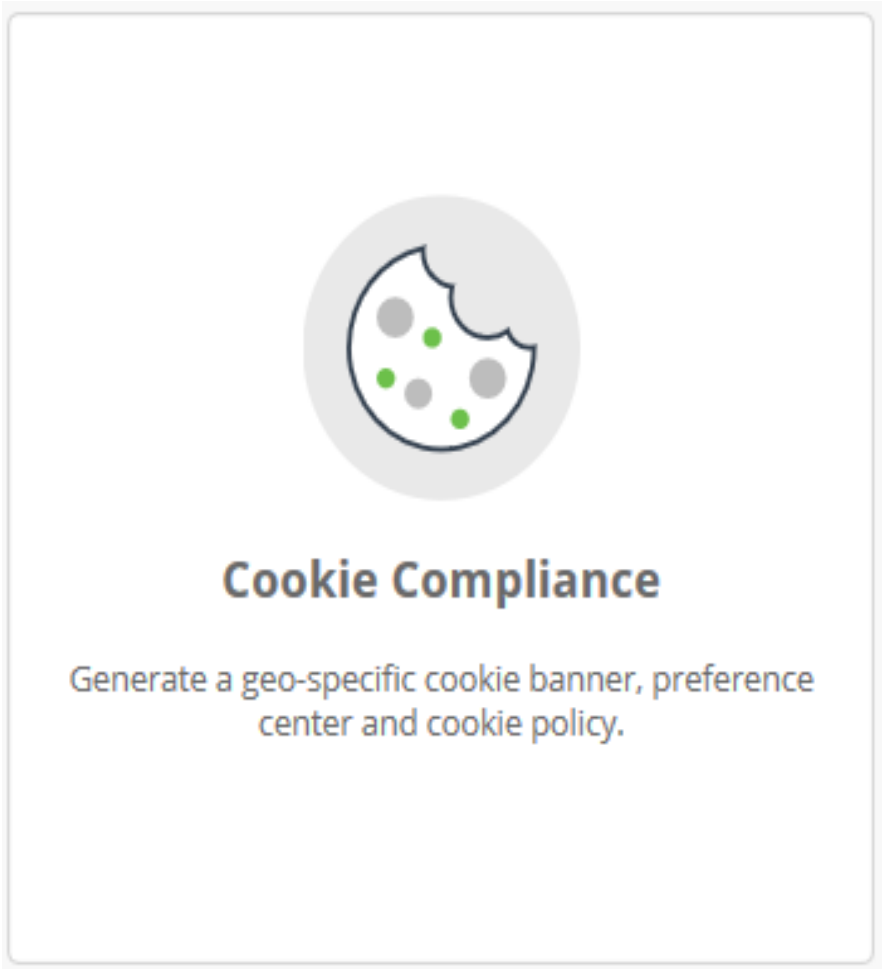
- Central registry to easily reference what assets we have, where personal data is at, how it got there, and where it goes.
- Especially needed in a decentralized company with numerous subsidiaries.
- Kirker/Consumer Europe completed; in que: USL, Viapol, DAP, Legend Brands

One Trust – Assessment Automation



- Designed to identify assets and processing activities that are under consideration, planned, or are in use currently but are changed or updated to ensure data privacy issues are identified and any risks are addressed.
- Currently under design to finalize and roll out with updated policy.

One Trust – Cookie Compliance



- Trial launch is forthcoming with CPG-Europe sites to test out One Trust's Cookie Compliance module.
- If successful, goal would to be target additional sites to manage the cookie compliance needs.

THE VALUE OF 168

ANY QUESTIONS?