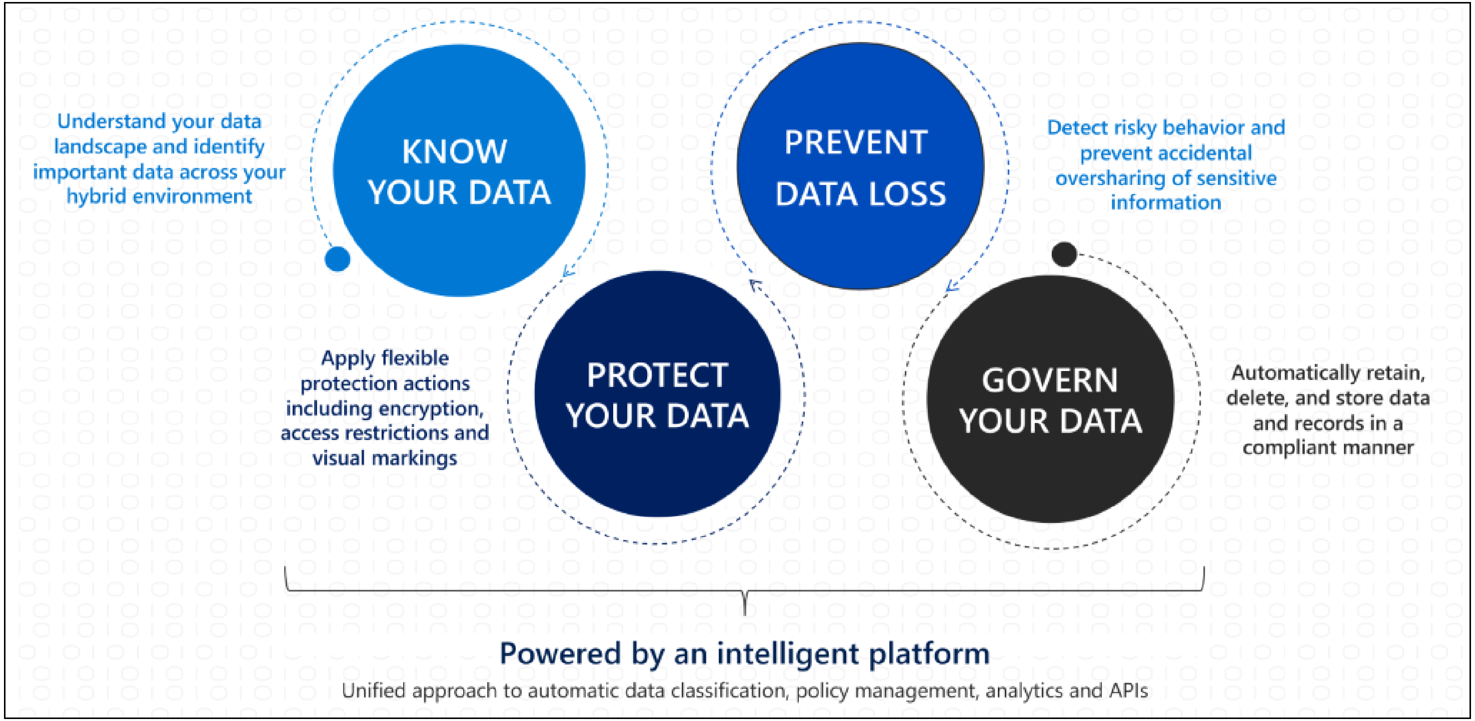
TOREON

Information Protection – Data Classification & Labelling

◆ CREATING TRUST FOR A SAFER DIGITAL SOCIETY ◆

The Microsoft Approach



Understand your data landscape and identify important data across your hybrid environment

Detect risky behavior and prevent accidental oversharing of sensitive information

Apply flexible protection actions including encryption, access restrictions and visual markings

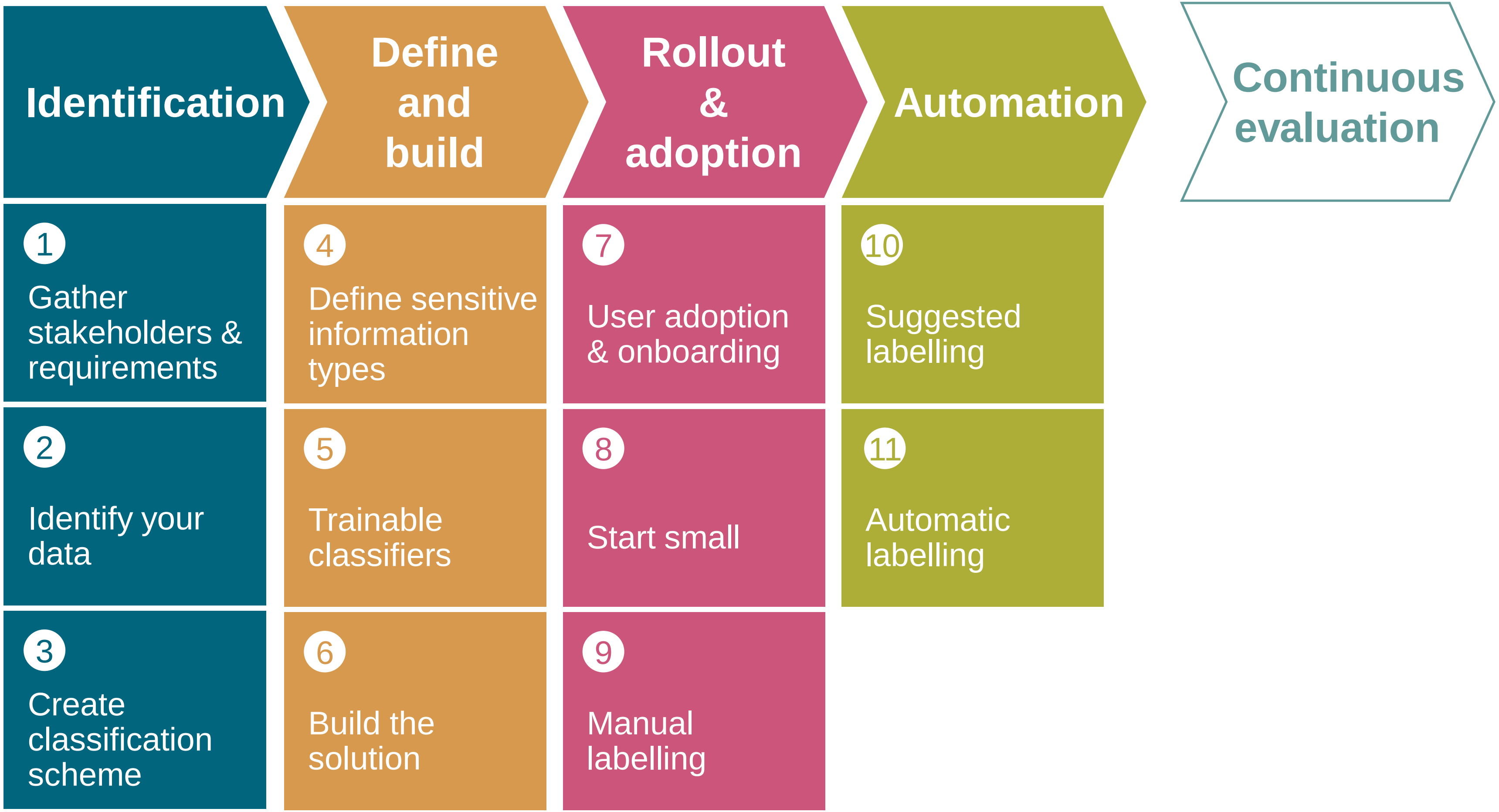
Automatically retain, delete, and store data and records in a compliant manner

Powered by an intelligent platform

Unified approach to automatic data classification, policy management, analytics and APIs

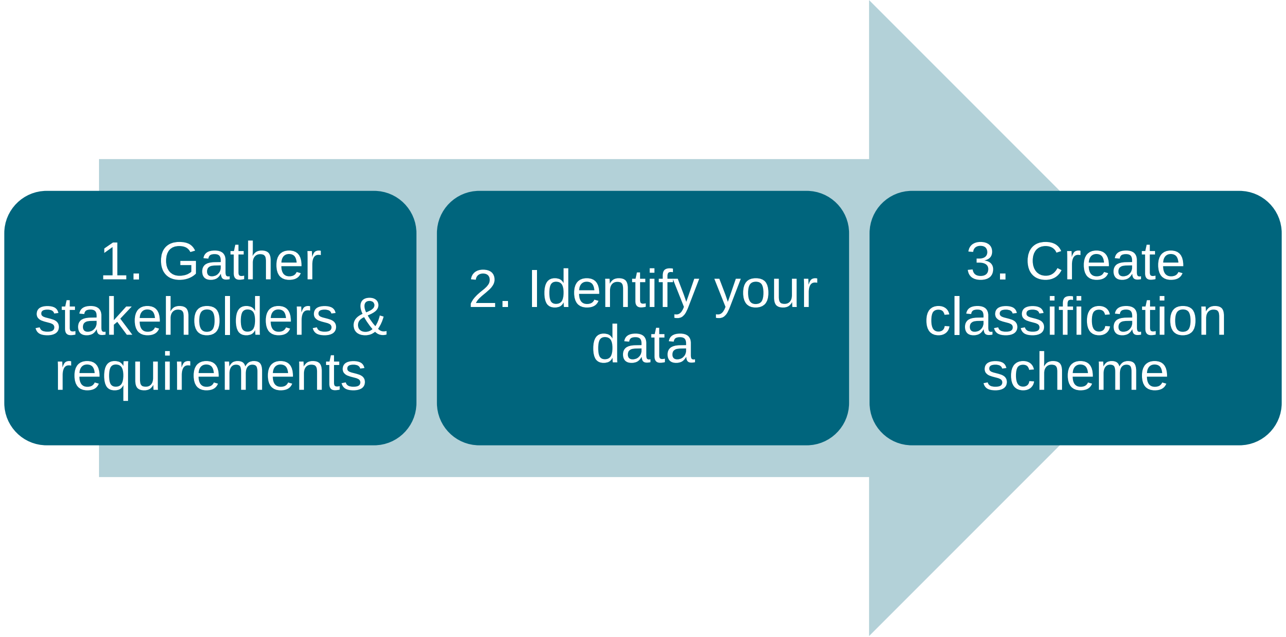
Our Approach: Information Protection – 12 Step approach

- Forms the basis of our Information Protection guidance
- Approach is proven & tested with Microsoft
- Based on practical experience
- Relies on Azure Information Protection
- Works close together with our customer for optimal success. Dedication required from both teams!



Identification	Define and build	Rollout & adoption	Automation	Continuous evaluation
1 Gather stakeholders & requirements	4 Define sensitive information types	7 User adoption & onboarding	10 Suggested labelling	
2 Identify your data	5 Trainable classifiers	8 Start small	11 Automatic labelling	
3 Create classification scheme	6 Build the solution	9 Manual labelling		

Phase 1: Identification

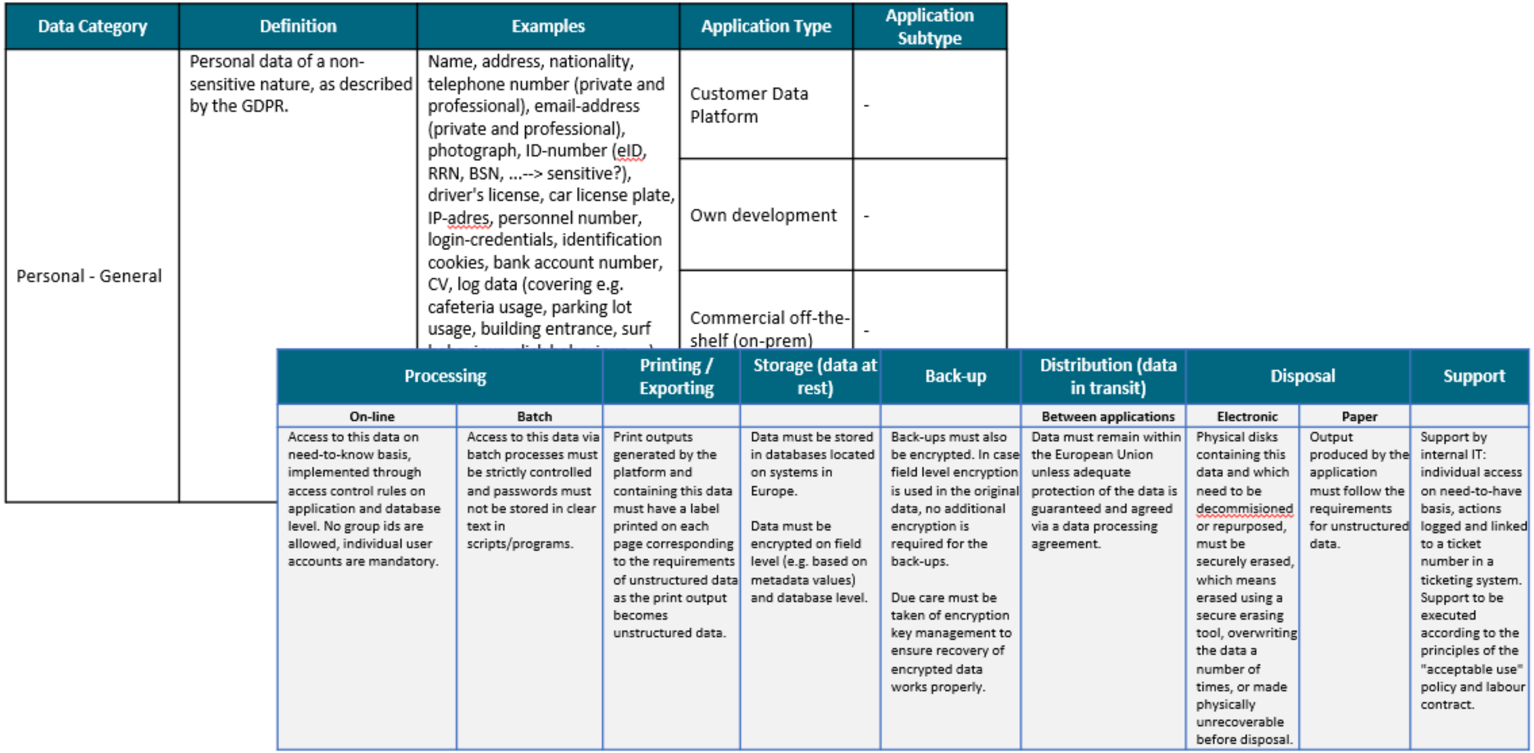


1. Gather stakeholders & requirements

2. Identify your data

3. Create classification scheme

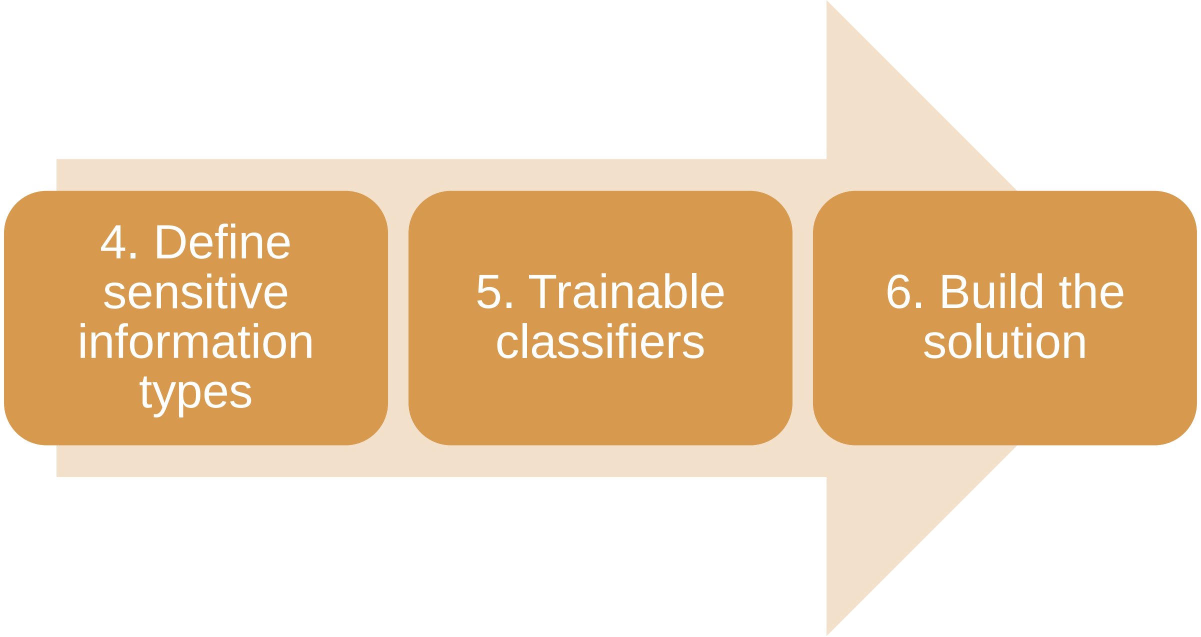
Classification Scheme example



Data Category	Definition	Examples	Application Type	Application Subtype
Personal - General	Personal data of a non-sensitive nature, as described by the GDPR.	Name, address, nationality, telephone number (private and professional), email-address (private and professional), photograph, ID-number (eID, RRN, BSN, ...--> sensitive?), driver's license, car license plate, IP-adres, personnel number, login-credentials, identification cookies, bank account number, CV, log data (covering e.g. cafeteria usage, parking lot usage, building entrance, surf	Customer Data Platform	-
			Own development	-
			Commercial off-the-shelf (on-prem)	-

Processing		Printing / Exporting	Storage (data at rest)	Back-up	Distribution (data in transit)	Disposal		Support
On-line	Batch				Between applications	Electronic	Paper	
Access to this data on need-to-know basis, implemented through access control rules on application and database level. No group ids are allowed, individual user accounts are mandatory.	Access to this data via batch processes must be strictly controlled and passwords must not be stored in clear text in scripts/programs.	Print outputs generated by the platform and containing this data must have a label printed on each page corresponding to the requirements of unstructured data as the print output becomes unstructured data.	Data must be stored in databases located on systems in Europe. Data must be encrypted on field level (e.g. based on metadata values) and database level.	Back-ups must also be encrypted. In case field level encryption is used in the original data, no additional encryption is required for the back-ups. Due care must be taken of encryption key management to ensure recovery of encrypted data works properly.	Data must remain within the European Union unless adequate protection of the data is guaranteed and agreed via a data processing agreement.	Physical disks containing this data and which need to be decommisioned or repurposed, must be securely erased, which means erased using a secure erasing tool, overwriting the data a number of times, or made physically unrecoverable before disposal.	Output produced by the application must follow the requirements for unstructured data.	Support by internal IT: individual access on need-to-have basis, actions logged and linked to a ticket number in a ticketing system. Support to be executed according to the principles of the "acceptable use" policy and labour contract.

Phase 2: Define and build

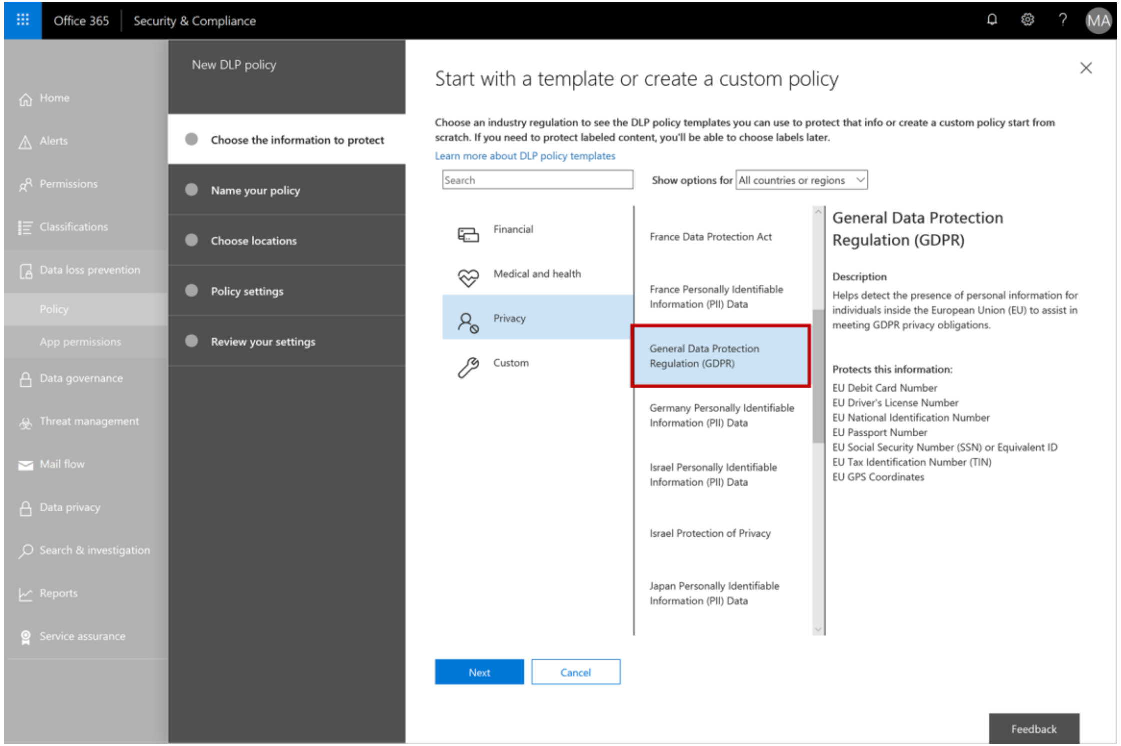


4. Define sensitive information types

5. Trainable classifiers

6. Build the solution

Sensitive information types - examples



Start with a template or create a custom policy

Choose an industry regulation to see the DLP policy templates you can use to protect that info or create a custom policy start from scratch. If you need to protect labeled content, you'll be able to choose labels later.

Learn more about DLP policy templates

Show options for: All countries or regions

General Data Protection Regulation (GDPR)

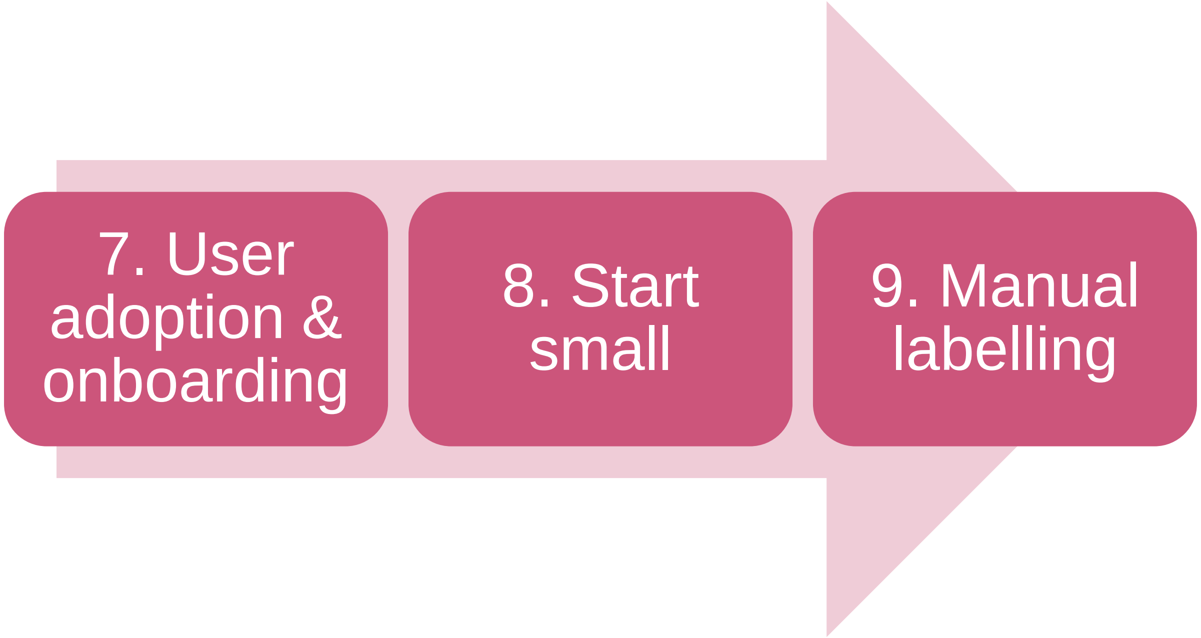
Description

Helps detect the presence of personal information for individuals inside the European Union (EU) to assist in meeting GDPR privacy obligations.

Protects this information:

EU Debit Card Number
EU Driver's License Number
EU National Identification Number
EU Passport Number
EU Social Security Number (SSN) or Equivalent ID
EU Tax Identification Number (TIN)
EU GPS Coordinates

Phase 3: Rollout & adoption



Phase 4: Automation

10. Suggested labelling

11. Automatic labelling

Phase 5: Continuous evaluation

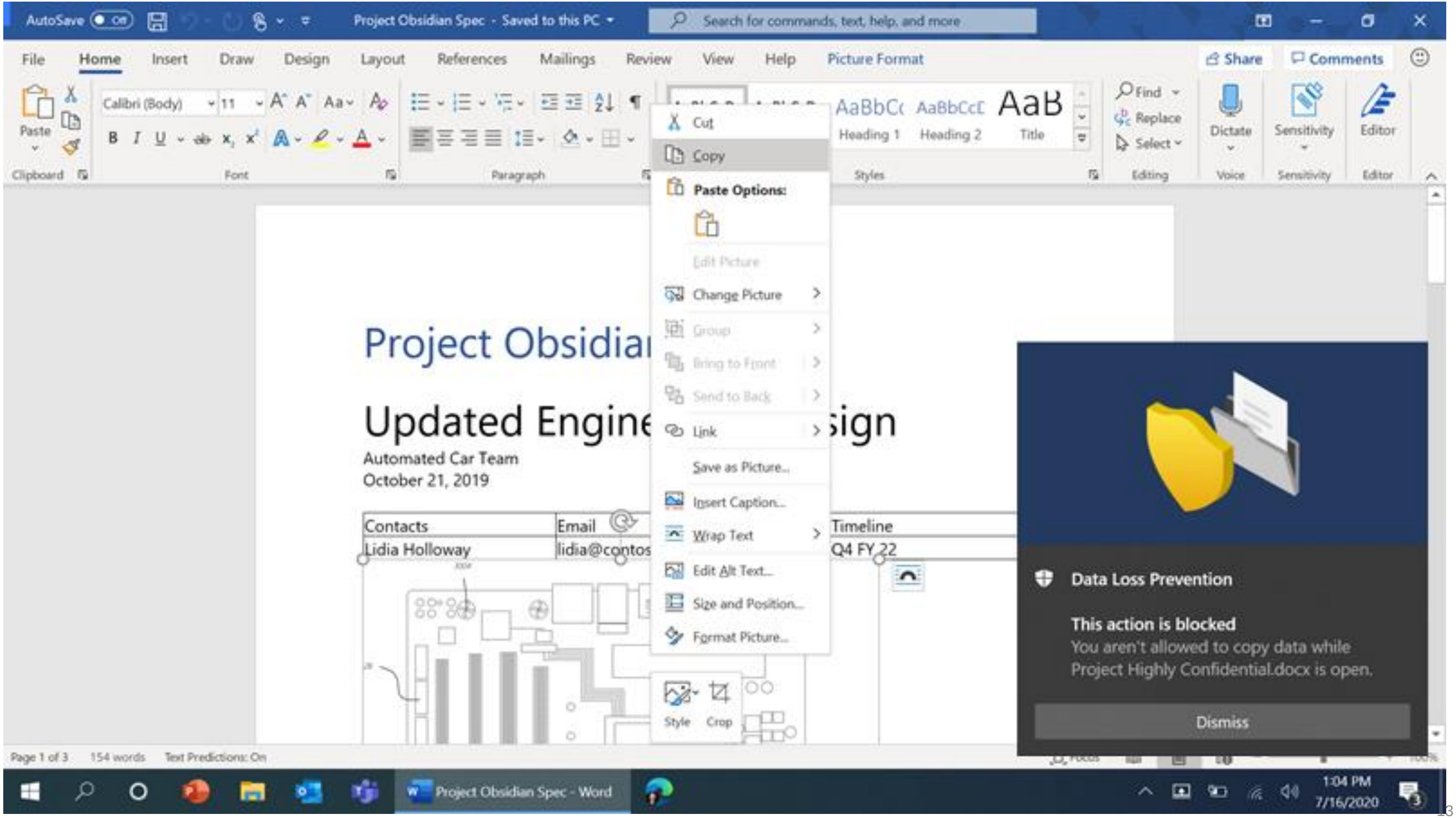
Continuous evaluation

And after?

Data Governance

Data Loss Prevention

Cloud app security



Project Obsidian

Updated Engine sign

Automated Car Team
October 21, 2019

Contacts	Email	Timeline
Lidia Holloway	lidia@contos	Q4 FY 22

Data Loss Prevention

This action is blocked

You aren't allowed to copy data while Project Highly Confidential.docx is open.