

Privacy by Design Workshop

Privacy Use Case Template – Example Use Case

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. **Use Case Title**

*[A short descriptive title for the use case]*

“Acme Insurance Company Vehicle Data Tracking for Reduced Premiums”

2. **Category of Use Case**

*[To be established as Used Cases are submitted - may be Application categories such as “Online Banking” or Model categories such as “Two Domain”. Where no pre-defined category exists, define a category that you believe is appropriate]*

Application Type: “Mobile – Vehicular”

Model Type: “Seven Domain”

2.5 **Associated Use Cases**

3. **Provide a general description of the Use Case**

*[High-level synopsis of use case]*

The Acme Insurance Company in Toronto, Canada, offers customers the opportunity to enroll in a program to have specific vehicular data automatically transmitted from their vehicle to the company. With data subject consent and agreement with the privacy policies associated with this program, Acme will establish a communication link to the vehicle manufacturer, located in Bruges, and receive specific vehicle data relevant to driving behaviors, including speed, location, trip frequency and duration, miles driven, and safety function deployments such as ABS activation. These data flows are integrated with Acme’s backend systems, which include algorithms for calculating driving patterns related to driving behaviors and risk of accidents. In exchange, the Acme Insurance Company offers a program of increasing reductions in the customer’s premiums for driving patterns indicative of good driving behaviors and reduced accident risk. Local insurance agents have access to summary information related to their customer driving patterns.

**Provide a summary inventory for the Use Case, including:**

4. **Business Processes and Systems associated with Use Case**

*[Relevant business processes and systems where personal information is communicated, created, processed, stored or deleted]*

* 1. Vehicle’s Internal Communications Application (Vehicle Data Collection and Communication to Vehicle Manufacturer)
	2. Vehicle Owner’s Web Portal into Hudson Motors
	3. Vehicle Manufacturer Backend Data Collection Application
	4. Insurance Company’s Data Collection and Analysis App
	5. Insurance Company’s Customer Facing Web Portal
	6. Insurance Company’s Agent Portal
	7. Sales of the Mobile-Vehicular Program by Hudson Motors and optionally Acme Insurance
	8. Initializing the Mobile-Vehicular Program by Hudson Motors and optionally Acme Insurance
	9. Receiving Mobile-Vehicular Program Information & Preferences from Hudson Motors and optionally Acme Insurance
	10. Receiving the Associated Insurance Rate Adjustment Information from Acme Insurance
	11. Maintaining Mobile-Vehicular Program Information & Preferences from Hudson Motors and optionally Acme Insurance
	12. Understanding driving trends by country, region, type of vehicle, ages of drivers and…by Hudson Motors and optionally Acme Insurance

5. **Data subject(s) associated with Use Case**

*[Include any data subject associated with any of the applications in the use case]*

* 1. The registered Insured person associated with the vehicle VIN
	2. Other drivers designated by the vehicle owner that will drive the vehicle

6. **Domain Owners, Domains, and Roles associated with Use Case**

 *[A “Domain Owner” is the Participant responsible for ensuring that privacy controls and PMRM services are managed in business processes and technical systems within a given Domain. A “Domain” includes both physical areas (such as a customer site or home) and logical areas (such as a wide-area network or cloud computing environment) that are subject to the control of a particular domain owner. “Role” includes the responsibilities assigned to specific Domain Owners within a privacy domain.]*

* **Domain 1:** Hudson Motor Company’s Vehicle Communications Data Center, Vehicle Owner’s Web Portal and Backend Data Collection Application
	+ **Domain 1 Owner:** VP, Vehicle Manufacturer’s Vehicle Communication and Data Division
	+ **Role:** Application design, development, content, testing, integration testing with external systems, communication with vehicle owners, communication with additional designated drivers, communications with external systems and adherence to corporate security and privacy policies; management and reporting of raw datasets of vehicle information associated with operation of the vehicle, including date/time of operation, location, speed, braking data, airbag deployment, etc to management and the vehicles’ associated vehicle owner and designated drivers.

**Note that having given Hudson Motors similar responsibilities as Acme, their Domain Owners would parallel Acme’s up unto the Insurance Rate setting**

* **Domain 2**: Acme Insurance Customer Vehicle Data Communications and Processing Application
	+ **Domain Owner:** VP for Customer Vehicle Support Programs
	+ **Role:** Application concept and specifications, content, production certification, communication with external systems, and adherence to corporate security and privacy policies; management of sub-sets of vehicle information associated with operation of the vehicle, including date/time of operation, location, speed, braking data, airbag deployment, including the vehicle driving patterns of each driver of the vehicle, for the purpose of providing safe driving guidance to the various drivers of the vehicle.
* **Domain 3**: Acme Insurance Software Development Group
	+ **Domain Owner:** CTO
	+ **Role:** Application design, software development, testing, integration testing, production certification, communication with external systems, and adherence to corporate security and privacy policies; management of live test data associated with operation of the vehicle, including date/time of operation, location, speed, braking data, airbag deployment for the purpose of assessing the driving skills of the various drivers and adjusting their insurance rates accordingly.
* **Domain 4**: Acme Insurance Company Customer Portal
	+ **Domain Owner:** VP for Customer Vehicle Support Programs
	+ **Role:** Application concept and specifications, content, production certification, communication with external systems, and adherence to corporate security and privacy policies; management of individual customer preferences, consent information, additional vehicle operators, and driving information
* **Domain 5**: Acme Insurance Company Analytics Processing System for Vehicle Data
	+ **Domain Owner**: VP for Advanced Analytics
	+ **Role:** Schema and analytics design, software development and testing, data processing, data storage, data disposition, reports and files output to Customer Profile Department; management of driving evaluation assessment data derived from system-based algorithms
* **Domain 6**: Acme Insurance Customer Profile Department
	+ **Domain Owner**: Director, Customer Profile Department
	+ **Role**: Review of files and driving profiles received from Analytics, interface with insurance agents servicing customers, review of automated decision recommendations requiring further analysis’ management of summary assessment information
* **Domain 7**: Local Insurance Agent
	+ **Domain Owner**: EVP for Regional Sales
	+ **Role**: Review of files and summary driving profiles received from Analytics, interface with Registered Vehicle Owner, explanation of summary assessment information
* **Domain 8**: Registered Vehicle Owner
	+ **Domain Owner**: Vehicle Owner
	+ **Role**: Drives and receives the summary assessments from Hudson Motors and the Local Insurance Agent
* **Domain 9**: Other Drivers Designated by Registered Vehicle Owner
	+ **Domain Owner**: Other Driver
	+ **Role**: Drives and receives summary assessments from the Registered Vehicle Owner [unless there is an option for this driver to receive direct feedback from either Hudson Motors or Acme Insurance].

7. **Systems supporting the Use Case applications**

*[System is a collection of components organized to accomplish a specific function or set of functions having a relationship to operational privacy management]*

* + Hudson Vehicle Manufacturer Data Management/Communication System (“Up-Star”)
	+ Hudson Vehicle Customer Web Portal (customer interface)
	+ Acme Insurance Customer Web Portal (customer interface)
	+ Acme Insurance Vehicle Data Processing System (“VDPS”)
		- Analytics
		- Summary Assessment and Insurance Rate Adjustments
		- Insurance Agent Portal
	+ ….

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Note: Not included in workshop Exercise: Products Having PI or PII in Use Case**

*[Categories of outputs or files containing PI or PII within the use case]..what is this? Has it excluded these data? If so, I think we might bundles most of what is below into the use case.]*

* + Domain 1: Raw datasets of vehicle information
	+ Domain 2: Sub-sets of vehicle information associated with operation of the vehicle, including date/time of operation, location, speed, braking data, airbag deployment….
	+ Domain 3: test sub-sets of vehicle information associated with operation of the vehicle, including date/time of operation, location, speed, braking data, airbag deployment….
	+ Domain 4: Customer preferences, consent information, additional vehicle operators, and driving information
	+ Domain 5: Driving evaluation assessment data derived from insurance company algorithms
	+ Domain 6: Summary assessment information

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

8. **PI and PII covered by the Use Case**

*[Specify the PI and PII bundles collected, created, communicated, processed or stored within Privacy Domains or Systems*

* + Hudson Motors Customer Data 1: Registered driver name, Registered driver contact information, VIN, Driver Number, privacy preferences and other preferences
	+ Hudson Motors’ Customer Additional Driver Data: Additional driver name, Additional Driver contact information, VIN, Additional Driver Number, privacy and other preferences
	+ Insurance Customer Data 1: Registered driver name, Registered driver contact information, Insurance Policy Account Number, VIN, Driver Number, privacy preferences and other preferences
	+ Insurance Customer Additional Driver Data: Insurance Policy Account Number, Additional driver name, Additional Driver contact information, VIN, Additional Driver Number, privacy and other preferences
	+ Insurance Agent Data: Insurance Agent name and contact information, Insurance Agent’s Customer Policy Account Numbers
	+ Hudson Motors Linked vehicle operational data: Specific vehicle data relevant to driving behaviors, time, date and location stamped, including speed, location, trip frequency and duration, miles driven, and safety function deployments such as ABS activation, by VIN and Driver Number, as permitted by policy
	+ Insurance Customer Information Analytics: Evaluation assessment and summary information by VIN and Driver Number for a given time period.
	+ Insurance Customer Information Rate Analysis: Rate assessment and summary information by VIN and Driver Number for a given time period

**[Note: per domain, system, application or product, depending on level of use case analysis**

9. **Data Flows and Touch Points Linking Domains or Systems**

*[Touch points are the points of intersection of data flows with privacy domains or systems within privacy domains. Data flows are data exchanges carrying PI and privacy policies among domains in the use case Provide a simple diagram showing the touch points applicable to the Use Case]*

*Identify the touch points and the direction(s) of the data flows and associate with each data exchange which bundles of information are flowing. If necessary change the bundles based upon the need for information.*

INSERT DIAGRAM HERE OR AS APPENDIX

10. **Legal, regulatory and /or business policies governing the Use Case**

*[Define and describe the source of policies and regulatory requirements governing privacy conformance within use case domains or systems]*

* + Government(s) regulations (BE, EU, CA and other country privacy regulations)
		- Required privacy permissions to collect, use and share PI/PII
		- Required retention and deletion requirements, established country by country
		- Required cross border flow requirements, established country by country
	+ Vehicle Manufacturer privacy policies
		- Registered driver must opt-in to the collection of said data and may opt-out at any time
		- Additional driver must opt-in to the collection of said data and may opt-out at any time and to what entities might see the driver’s vehicular operational data
	+ Telecom Carrier privacy policies
	+ Insurance Company privacy policies
		- Registered driver must opt-in to the collection of said data and may opt-out at any time
		- Additional driver must opt-in to the collection of said data and may opt-out at any time
	+ Data Subject(s) Consent preferences
		- Registered driver must opt-in to the collection of said data and may opt-out at any time
		- Additional driver must opt-in to the collection of said data and may opt-out at any time
	+ Specific Privacy Policies Associated with Each Application (e.g., “Data Communications to Manufacturer”)
		- Refer to the collection, use, sharing, cross-border transfers and retention of PI/PII

Provide or include link to a PIA if available

* [http://acmeinsurancegroupinc.biz/vehicle privacy/](http://acmeinsurancegroupinc.biz/vehicle%20privacy/)
* <http://HudsonCarCompany.biz/vehicle> privacy

<https://Registereddriverprivacypreferences> at Hudson Motor Cars and Acme Insurance Company

11. **Privacy controls required within the Use Case**

* *Control - a process designed to provide reasonable assurance regarding the achievement of stated objectives*

[Note: to be developed against specific domain, system, or applications as required by internal governance policies and regulations]

12.  **Functional Services Necessary to Support Privacy Controls**

* *Service - a collection of related functions and mechanisms that operate for a specified purpose*

