

Privacy by Design Workshop

Privacy Use Case Template v.20

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

1. **Use Case Title**

*[A short descriptive title for the Use Case]*

“**Hudson Motors** Vehicle Driving Analysis Program to improve the efficiency and safety of their driving and **Acme Insurance Co** Vehicle Data Tracking for Reduced Premiums”

2. **Category of Use Case**

*[To be established as Used Cases are defined - may be Use Case for specific Data Subject, Domain, System, Application, Business Process or Product category or a Model category that crosses Data Subjects, Domains, Systems, Applications, Business Processes or Products. As the Use Case is developed the category may not change, but the PMRM process will likely change the number of Domains, Systems, Applications, Business Processes or Products, needed to comply with the Privacy Policies via Privacy Controls and PMRM Services.]*

**Category:** Model for Driving Efficiency & Safety and Insurance Reductions

**Model Type:** High Level Privacy Architecture for Improving Driving Efficiency and Safety and Reducing Insurance Premiums

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

*[High-level synopsis of Use Case]*

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

*[an introduction, the context, objective, target audiences, specification summary and terminology]*

**Introduction and Objective:** Hudson Motors offers vehicle owners and registered drivers in CA, BE and Turkey the opportunity to enroll in a program that will improve the efficiency and safety of their driving by collecting specific vehicular data for each unique driver, analyzing the data and reporting it back to the vehicle owner and registered drivers on a regular basis so that they may track and improve their driving.

The Acme Insurance Co (**Acme**) in Toronto, Canada, offers vehicle owners and registered drivers in CA, BE and Turkey the opportunity to enroll in a program to reduce their insurance premiums by having specific vehicular data collected for each unique registered driver that signs up for the program to be automatically transmitted to Acme for premium reduction considerations. As part of this program, Acme may reduce the vehicle insurance premiums for vehicle owners and may provide better insurance quotes for registered drivers when they purchase a vehicle.

**Target Audiences:** Vehicle drivers and Insurance customers; City, Province and Country Officials responsible for maintaining safe roads, especially during bad weather conditions

**Context:** With vehicle owners and registered drivers consents and in agreement with the privacy policies associated with these programs, Hudson Motors, located in Bruges, Belgium will 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, for each unique driver. Drivers of the vehicle may include the vehicle owner and drivers that register themselves or they may be anonymous, identified only by their physical characteristics collected by the vehicle’s sensors.

Hudson Motors will seek the consent(s) of the vehicle owner and registered drivers to collect and use to the data for purpose of registering, providing the vehicle owner and each registered driver with relevant summaries of efficient and ‘good driving’ behaviors, up-selling new features and vehicle models and performing vehicle analysis by region, weather conditions, individual driver body types and so on. Driving and vehicle performance, will however be collected for all drivers of Hudson Motors vehicles for use by Hudson Motors and other third parties as described in the Privacy Policy.

Hudson Motors will also offer the option to vehicle owners and registered drivers to apply for reduced insurance from Acme.

Acme will establish a communication link with Hudson Motors to 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, for vehicle and all of its drivers and for each registered driver. Acme will consider increasing premium reductions for the vehicle and/or each registered driver, for driving patterns indicative of good driving behaviors and reduced accident risk.

The driving behaviors of all registered and anonymous drivers will be used in the premium analysis for the vehicle. The driving behaviors of registered drivers will affect future premiums when a registered driver becomes a vehicle owner.

Local insurance agents will have access to summary information related to the driving patterns of registered drivers that are current or prospective customers.

4. **Products,** **Business Processes(s), System(s) and Application(s) associated with Use Case**

*[Relevant Products, Business Processes, Systems and Applications where personal information is collected, communicated, created, processed, stored, shared, transferred or deleted]*

**Products, External and Internal:**

* “Efficient and Safe Driving Practices Program” for Hudson Motors registered drivers
* Vehicle Performance Analysis for Hudson Motors to use to:
	+ improve vehicle design
	+ up-sell registered drivers
	+ respond to regulatory inquiries regarding vehicle safety matters and other regulatory inquiries
* Reduced Insurance Premiums for Acme customers based upon their “Good Driving Practices Program”
* Insurance Performance Analysis for Acme to use to:
	+ improve or refine their premiums
	+ up-sell to customers new insurance programs
	+ respond to regulatory inquiries regarding premium rates and other regulatory inquiries
* Safe Roads Program for Cities, Provinces and Countries
	+ Improve safety on roads with better road treatments during bad weather
	+ Create driver awareness programs for specific roads

**Relevant Business Processes:**

* Hudson Motors
	+ Enrolling, updating and retiring Vehicle Owners and Registered Drivers
	+ Collecting, analyzing and reporting to Vehicle Owners and Registered Drivers
	+ Improving vehicle performance and design
	+ Reporting to City, Province and Country officials on their effectiveness in keeping roads safer and drivers more aware
	+ Responding to regulatory inquiries (of all kinds)
	+ Responding to subpoenas and legal inquiries (of all kinds)
* Acme
	+ Enrolling, updating and retiring Customers in the “Good Driving Practice” program
	+ Receiving, analyzing and calculating premium changes, based upon the “Good Driving Practices” of the customer or potential Customer
	+ Improving Acme’s insurance program for the company and its Customers
	+ Responding to regulatory inquiries (of all kinds)
	+ Responding to subpoenas and legal inquiries (of all kinds)

**Relevant Systems and Applications within Systems**

* Hudson Motors
	+ Vehicle Sensory System
		- Driver Identification Application
		- “Up-Star” Collection Application
		- Time/Location Tracking Application
	+ Weather Tracking System
		- Weather Tracking by Time/Location Application
		- Vehicle Performance Weather Analysis
		- “Safe Roads” Weather Analysis Application
		- “Safe Roads Reporting Program Application for Cities, Provinces and Countries
	+ Vehicle Performance System
		- Driver Performance Analysis Application
			* integrating data from the three Vehicle Sensory applications and the Weather Tracking System applications
		- Vehicle Performance Analysis Application
			* integrating data from the three Vehicle Sensory applications and the Weather Tracking System applications
	+ Registered Driver System
		- Registration Application for Register Drivers via a Driver Web Portal
		- Registration Application for Register Drivers via a Sales Agent Portal
		- Reporting Application for Registered Drivers
		- Up-Sell and Marketing Application(s)for Sales Agents
		- “Good Driving Practices” Application interface with Insurance Companies, including Acme
	+ Adhoc Reporting System
		- Data collection, analysis and external reporting ‘applications’ as required for regulators, subpoenas and legal inquiries
* Acme
	+ “Good Driving Practices” System
		- Registration Application for Insurance Agents to register Customer via the Insurance Agent Portal
		- Registration Application for Insurance Customers and potential Customers via the Registered Drivers Web Portal
		- Insurance Agent Portal to search for and market the “Good Driver Practices Program” product to current and potential Customers
		- Data Interface Application from Motor Companies
		- Premium Analysis Application to calculate premiums
		- Reporting and Repository Application for Insurance Agents and Registered Drivers
	+ Insurance Analysis System
		- Premium ROI Analysis Application
		- “Good Driver Practice” Analysis Application
	+ Adhoc Reporting System
		- Data collection, analysis and external reporting ‘applications’ as required for regulators, subpoenas and legal inquiries

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

*[Include any data subject associated with any of the Products, Business Processes, Systems or Applications in the Use Case]*

*[This section of the Use Case will be refined, as needed, to ensure compliance with the Privacy Policies. This refinement will occur as the subsequent steps in the Use Case are performed. It may be necessary to add Data subjects or eliminate Data Subjects]*

* + - The vehicle owner (data subject)
		- The registered driver (data subject)
		- The non-registered “anonymous” driver (data subject)
		- Hudson Motors sales person
		- Hudson Motors customer service representative
		- Hudson Motors privacy officer
		- Acme insurance agent
		- Acme customer service representative
		- Acme privacy officer

***Note:*** *Here is where I would recommend the first matrix that associates these Data Subjects (and other individuals) with the* Products, Business Processes(s), System(s) and Application(s). The Data Subject to Products/Processes/Systems will result in new or updated entries on both sides of the matrices.

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

 *[Relevant Domains, Owners and Roles associated with the Use Case and its specific Products, Business Processes, Systems and Applications they are responsible for that are to comply with Privacy Policies via Privacy Controls and PMRM Services.]*

 *[This section of the Use Case will be refined, as needed, to ensure compliance with the Privacy Policies. This refinement will occur as the subsequent steps in the Use Case are performed. It may be necessary to create new Domains, collapse Domains or revise Role(s).]*

 *[A “Domain and its Owner” is the responsible for ensuring that the Privacy Controls and PMRM Services that are required to satisfy the Privacy Policies are implemented in their Products, Business Processes, Systems and Applications. 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.]*

**Company, Domains, Domain Owner and Role:**

**Hudson Motors Domains:**

**1**. Product Development Division

The VP of Product Development is the domain owner and his/her role is to design and build better vehicles

2. Operation Division,

The VP of the Operations Division is the domain owner and his/her role is to design, implement and manage business processes and operational units for all other domains. Such operational units may include customer service centers

3. Automation Division

The VP of the Automation Division is the domain owner and his/her role is to build systems and applications and perform analytics for all other domains

4. Marketing Division

The VP of the Marketing Division is the domain owner and his/her role is to market vehicle and driver performance information to companies/entities such as Acme and City/Province/Country Official

 5. Sales Division

The VP of the Sales Division is the domain owner and his/her role is to sell vehicles and associated products, such as those offered by insurance companies and others

**Acme Domains:**

1. Product Development Division

The VP of Product Development is the domain owner and his/her role is to offer price competitive insurance programs

2. Operations Division

The VP of the Operations Division is the domain owner and his/her role is to design, implement and manage business processes and systems for all other domains

3. Automation Division

The VP of the Automation Division is the domain owner and his/her role is to build and maintain systems and applications and perform analytics for all other domains

4. Marketing Division

The VP of the Marketing Division is the domain owner and his/her role is to market insurance programs

**Service Providers:**

1. Telecommunications Company

 2. Offsite Storage Company

 3. Cloud Provider

 4. Others?

***Note:*** *that including Service Providers as a separate category may help to highlight their importance in compliance with Privacy Policies, Controls and Services*

**City/Province/Country Officials:**

1. Road Safety and Maintenance Division

The VPs of Road Safety and Maintenance Division are the domain owner and his/her role is to provide safe roads for their jurisdiction

***Note:*** *Here is where I would recommend the second set of matrices that associates these Data Subjects (and other individuals) and the* Products, Business Processes(s), System(s) and Application(s) with Domains. This will result in new or updated entries on both sides of the matrices.

7. **Applicable Privacy Policies**

*[Privacy Policies include a collection of legislative and company conformance criteria, which may be developed in general or assigned to Data Subjects, Domains, Systems, Applications, Business Processes and/or Products]*

*[Refine/define the Use Case as necessary to satisfy Applicable Privacy Polices by creating or modifying the Data Subjects, Domains, Systems, Applications, Business Processes or Products above. Update as necessary]*

* + Government(s) regulations (BE, EU, CA, Turkey)
		1. Require privacy permissions to collect, use, share, transport and retire PI/PII
		2. Require ability to turn off such permissions
		3. Require informing data subjects of the situations where they do not have the ability to opt-in/out, why and how the domain preserves their privacy
		4. Require statements regarding retention and deletion, and cross-border data flows, established country by country
	+ Hudson Motors privacy policies and statements
		1. Vehicle owner must opt-in to the collection of said personally identifiable data and may opt-out at any time. Hudson Motors has committed to a single internal privacy policy and, naturally country specific privacy statements written according to individual country requirements, however essentially making the same commitments in all jurisdictions
		2. Additional registered driver(s) that 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
		3. All drivers may register for more than one vehicle
		4. Drivers may decide not to register, however their driving information will be collected. These drivers of Hudson Motors vehicles will be identified by their physical characteristics (e.g. weight, height et. al) collected by sensory devices in the vehicle
		5. The vehicles may be driven anywhere around the world
		6. Vehicle owners and registered drivers may also opt-in to permit the sharing of their driving information with programs such as Acme offers. They may opt-out at any time
		7. Vehicle owners, registered drivers and other drivers will not have an opt-in or opt-out for the sharing of non-personally identified data and aggregated statistical vehicle performance information with entities such as Cities/Provinces/Countries or other entities using the information for analytics
	+ Insurance Co privacy policies and statements
		1. Registered vehicle owner must opt-in to participating in the Acme program and with Hudson Motors to permit the sharing of said data with Acme and may opt-out at any time
		2. Additional registered driver(s) must opt-in to participating in the Acme program and with Hudson Motors to permit the sharing of said data with Acme and may opt-out at any time
	+ Data Subject(s) Consent preferences
		1. For Hudson Motors, vehicle owners and registered driver(s) may opt-in/out of programs like the “Efficient and Safe Driving Program”
		2. For Acme, vehicle owners and registered driver(s) may opt-in/out of Hudson Motors providing driving information to Acme for the purpose of establishing insurance rated

***Note:*** *Here is where I would recommend the third set of matrices that associates the Privacy Policies with the Data Subjects (and other individuals) and the Products, Business Processes(s), System(s) and Application(s), Domains and Privacy Policies. This will result in new or updated entries on both sides of the matrices. This mapping will also facilitate the beginning of creation of the Privacy Controls.*

8. **Initial Privacy Impact (or other Assessments)**

*[Privacy Impact or other Assessments include a collection of current identified gaps in the current Systems, Business Processes and Products necessary to be closed to satisfy the Applicable Privacy Policies]*

*Refine/define the Use Case as necessary close the Privacy Impact or Assessments gaps by creating or modifying the Domains, Systems, Applications, Business Processes or Products. Update the above as necessary*

Summarize the initial PIA and link to its details

***Note:*** *I am not certain of the timing of doing a PIA in the ‘flow’ of this methodology. It seems that it best falls at the end of the PMRM cycle after a first iteration of the Use Case. It may be however better placed after the definition of the “PI/PII covered by the Use Case” or after the Data Flow step. This way all of the discovery and high level design processes are complete and the PIA becomes both a validation of the Use Case design and facilitates the identification of gaps that MUST/MIGHT be addressed.*

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

*[Specify the PI and PII collected, created, communicated, processed or stored by Data Subjects, Domains, within Domains, Systems, Applications, Business Processes or Products. Consider doing so by identifying PI/PII bundles of data rather individual data elements. Doing so will not only make this overall step more efficient, but will help one focus on who needs/or doesn’t need certain PI/PII. It will subsequently lead to significant changes in the elements of the Use Case defined above]*

*Refine/define the Use Case as necessary to satisfy Applicable Privacy Polices and close the Privacy Impact or Assessments by creating or modifying the Data Subjects, Domains, Systems, Applications, Business Processes or Products. Update the above as necessary]*

*[Note: per Data Subject, Domain, System, Application, Business Process or Product, depending on level of Use Case analysis: Define and describe the source of policies and regulatory requirements governing privacy conformance within Use Case]*

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

***Note:*** *From this point to the end, I have not revised the contents beyond their initial development. Typically, with the sections above, as I have completed a section, I have been able to refine the sections above with better design considerations.*

* + Hudson Motors Vehicle Owner Data: Registered driver(s) name(s), physical identity as collected from sensors in the vehicle, driver contact information, VIN, Driver Number, product and privacy preferences for Hudson Motors “Driver/Vehicle Performance Program”, Acme “Good Driver Program” and other programs to be developed
	+ Hudson Motors Registered Driver Data: Registered driver name, physical identity as collected from sensors in the vehicle, driver contact information, VIN and Driver Number for each vehicle to be driven and product and privacy preferences for Hudson Motors “Driver Performance Program”, Acme “Good Driver Program” and other programs to be developed
	+ Acme “Good Driver” Customer Data: Customer or potential Customer’s name, contact information, Insurance Policy Account #, VIN, Driver Number, privacy preferences and other preferences
	+ Insurance Agent Data: Insurance Agent name and contact information,
	+ Insurance Agent’s Customer and Potential Customer Data: Policy Account Numbers
	+ Hudson Motors Driver Performance Data: By VIN and Driver Number, 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, weather factors, as permitted by policy
	+ Acme Customer Information Analytics: Evaluation assessment and summary information by VIN and Driver Number for a given time period.
	+ Acme Customer Information Rate Analysis: Rate assessment and summary information by VIN and Driver Number for a given time period

***Note:*** *Here is where I would recommend the fourth set of matrices that associates the PI/PII bundles with the Data Subjects (and other individuals) and the Products, Business Processes(s), System(s) and Application(s), Domains and Privacy Policies. This will result in new or updated entries on both sides of the matrices. Mapping PI/PII bundles against the Privacy Policy will add data elements to the bundles, change the PII identifiers and may split bundles into two or more. Mapping to Domains, et al will also verify that these sections are designed to accommodate privacy compliance.*

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

*[Touch Points are the points of intersection of Data Flows between Domains, Systems, Applications, Business Processes and Products. Data flows are data exchanges carrying PI and Privacy Policies among Domains, Systems, Applications, Business Processes and Products in the Use Case]*

*[Refine/define the Use Case as necessary to satisfy Applicable Privacy Polices and close the Privacy Impact or Assessments gaps by creating or modifying the Data Subjects, Domains, Systems, Business Processes or Products. Update the above as necessary]*

*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.*

*Note: I did not update this diagram, as I wanted to complete the above.*

INSERT DIAGRAM HERE OR AS APPENDIX

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

*[Control - a process designed to provide reasonable assurance regarding the achievement of stated Privacy Policies for each Data Subject, Domain, System, Application, Business Process or Product. Privacy Controls are either inherited, internally used and exported]*

*[The translation of Privacy Policies to Privacy Controls is* ***the*** *essential step in translating policy, to compliance to policy and then to integrating requirements into the design of what is required of Data Subjects, Domains, Systems, Applications, Business Processes and Products. It defines the requirements necessary to assure compliance by people, process and technology]*

*[Privacy Controls are to be developed for a specific Data Subject, Domain, System, Application, Business Process or Product as required by the Privacy Policies, e.g. internal governance policies and regulations]*

*Refine/define the Use Case sections as necessary to satisfy Applicable Privacy Polices and close the Privacy Impact or Assessments by creating or modifying the Domains, Systems, Applications, Business Processes or Products. Update the above as necessary]*

*Privacy Controls are grouped into the following categories of controls:*

* *Organizational Controls*
* *Preference Controls*
* *Collection Controls*
* *Use/Purpose Controls*
* *Sharing Controls*
* *Cross Border Controls*
* *Safeguard Controls*
* *Retention Controls*
* *Deletion Controls*
* *Access Controls*
* *Accuracy Controls*
* *Data Minimization Controls*

***Note:*** *What follows was material I put in last fall. I have not gotten to revise this section. I apologize. I do believe that by developing the controls by a framework it will be easier to develop specific controls for this use case.*

* + A PbD step will be inserted in the design and testing stages of new modified Domains to confirm that the data is necessary
* Operational Controls
	+ Maintain an operational privacy and security policies and procedures
	+ Standard privacy and data protection legal language shall be inserted into all vendor, employees and customer terms of use
	+ Risk-based audit will be conducted annually and/or in conjunction with a regular Domain audit to verify that the legal language, the privacy policy and statements, the permissions, the PbD commitments, et al are being met
	+ Employees will be provided with annual training and education regarding the implementation of the legal language or at the time the terms change
	+ An inventory of PI/PII and its flows from Domain to Domain within and between organizations and countries
* Communication with Regulator(s) Controls
	+ Register, as required with regulators
	+ Respond, as required to regulator inquires

***Note:*** *Here is where I would recommend the next set of matrices that first maps the Controls to the Policies. Then I would recommend mapping the Controls to Data Subjects (and other individuals) and the Products, Business Processes(s), System(s) and Application(s), Domains and PI/PII bundles, and indicating whether they are inherited, internally generated, or exported. This exercise might be able to be done at the Domain level, reducing the time for the exercise. Again, there will be updates all throughout the design.*

12.  **Functional Privacy (PMRM) Services Necessary to Support the Privacy Controls**

*[Privacy Service(s) - a collection of related functions and mechanisms that operate together to comply with the stated Privacy Policies and implement the Privacy Controls for each Data Subject, Domain, System, Application, Business Process or Product]*

*[PMRM Services include, generically, the Core Policy Services of Agreement and Usage, the Privacy Assurance Services of Validation, Certification, Enforcement and Security, and the Presentation and Lifecycle Services of Interaction and Access. These PMRM Service classifications define the specific technical and business components needed to satisfy each Privacy Control for each Privacy Policy. They can easily be translated into technical specifications for implementation]*

*[****Note:*** *to be developed for Privacy Controls against a specific Domain, System, Application, Business Process as required by internal governance policies and regulations. Refine/define the Use Case as necessary to satisfy Applicable Privacy Polices and close the Privacy Impact or Assessments by creating or modifying the Domains, Systems, Applications, Business Processes or Products. Update the above as necessary]*

*[****Note:*** *I am recommending that we first map the Services at a high level to each control and as we do so we consider creating a mini-specification and an implementation example of how the Services might be implemented at a high level. Next I would validate the mapping and the mini-specification by reviewing the Privacy Controls Mapping to Data Subjects, Domains, Business Processes, Systems and Applications. During this process I would refine the mini-specification(s) looking for where the mini-specification might apply in multiple places. If it doesn’t apply I would create a second mini-specification for this instance. The result of this exercise would be a comprehensive (but minimum/standard) set of implementation specifications for the privacy controls that could be applied to business processes and systems/applications in each Domain.]*

*[****Note:*** *The result of this final step might achieve two things. First it would provide privacy compliance implementation for the Use Case. Second and more importantly it would provide a library of privacy compliance designs with mini-specifications and implementation examples.*

*I saw this technique employed by a tool that Barb Lawler presented that stream-lined privacy compliance at Intuit. While not exactly the same, Intuit has developed a set of (in my words) privacy controls/rules and has mapped them to implementation examples. Then by asking a developer a set of simplified questions, the Intuit tool applies these thousands of privacy rule/controls and returns to the developer examples of possible privacy compliance implementation examples. I think that the PMRM process might yield a similar effective outcome]*

13.  **Perform a Risk and/or Compliance Assessment**

*[The Risk and/or Compliance Assessment confirms that the Privacy Policies and Controls have been fully designed into the specific Data Subjects, Domains, Systems, Applications, Business Processes as required and the gaps identified in the initial Privacy Impact or other Assessments have been closed ]*

*[Identify the risks that require refining the Privacy Architecture as necessary to satisfy Applicable Privacy Polices and close the Privacy Impact or Assessments by creating or modifying the Domains, Systems, Applications, Business Processes or Products. Update the above as necessary]*