The Regorous Methodology to Business Process Compliance

Guido Governatori

13 December 2017

www.data61.csiro.au

A Privacy Act

Section 1: (Prohibition to collect personal medical information)

Offence: It is an offence to collect personal medical information.

Defence: It is a defence to the prohibition of collecting personal medical information, if an entity immediately destroys the illegally collected personal medical information before making any use of the personal medical information

Section 2: An entity is permitted to collect personal medical information if the entity acts under a Court Order authorising the collection of personal medical information.

Section 3: (Prohibition to collect personal information) It is forbidden to collect personal information unless an entity is permitted to collect personal medical information.

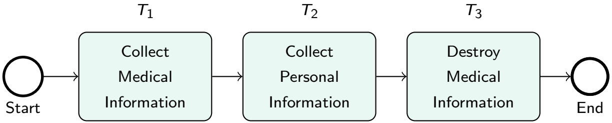
Offence: an entity collected personal information

Defence: an entity being permitted to collect personal medical information.

Making Sense of the Act

- Collection of medical information is forbidden.
- Destruction of the illegally collected medical information excuses the illegal collection.
- Collection of medical information is permitted if there is an authorising court order.
- Collection of personal information is forbidden.
- Collection of personal information is permitted if the collection of medical information is permitted

Are We Compliant?


T_1
T_2
T_3
Start
Collect Medical Information
Collect Personal Information
Destroy Medical Information
End

No Time for Compliance

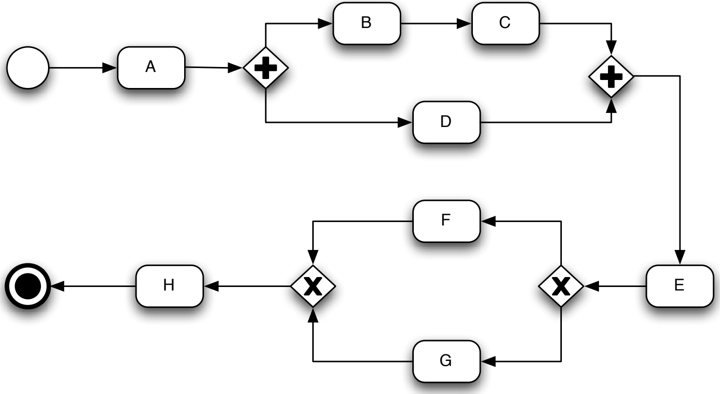
- Governatori "Thou Shalt is not You Will" showed that temporal logics are not suitable to represent norms (and the result extend to the vast majority of deontic logics)
- Governatori and Hashmi "No Time for Compliance" showed that compliance frameworks based on (linear) temporal logic are not able to handle the scenario correctly

The Regorous Approach

1. Annotated business process models
2. Proper representation of norms based on PCL (Process Compliance Logic)
3. Simulate execution of traces and round trips to PCL reasoner
    1. Determine what are the obligations in force for each state
    2. Determine which obligations have been fulfilled, violated, or pending
    3. Determine which violations have been compensated for

`http://www.regorous.com`

Modelling Processes



t_1 : A, B, C, D, E, F, H
t_2 : A, B, D, C, E, F, H
t_3 : A, D, B, C, E, F, H

t_4 : A, B, C, D, E, G, H
t_5 : A, B, D, C, E, G, H
t_6 : A, D, B, C, E, G, H

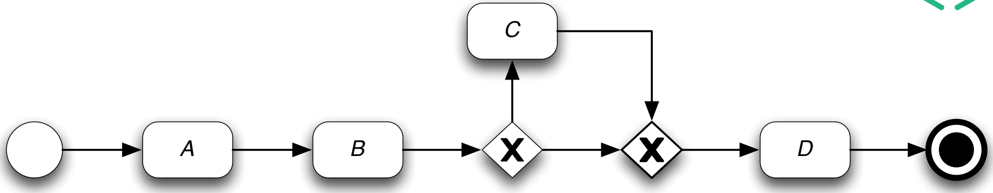
Annotated Traces

Let *Lit* be a set of literals, T be the set of traces of a process and $\mathbb{N}$ be the set of natural numbers

$$State\colon T \times \mathbb{N} \mapsto 2^{Lit}$$

The function *State* returns the set of literals describing "what's going on in a trace t after the execution of the n-th task in the process".

Example



Tasks

- A: "turn the light on"
- B: "check if glass is empty"
- C: "fill glass with water"
- D: "turn glass upside-down"

Propositions

- p: "the light is on"
- q: "the glass is full"

Trace 1: $\langle A, B, D \rangle$
Trace 2: $\langle A, B, C, D \rangle$

- $State(i, 1) = \{ p \}, \; i \in \{ 1, 2 \}$
- $State(1, 2) = \{ p, q \}$
- $State(2, 2) = \{ p, \neg q \}$
- $State(2, 3) = \{ p, q \}$
- $State(1, 3) = \{ p, \neg q \}$
- $State(2, 4) = \{ p, \neg q \}$

Modelling Norms

Norms are modelled as **if** . . . **then** . . . rules

- norms are defeasible (handling exceptions)
- two types of norms
  - constitutive rules: defining terms used in a legal context

$$A_1, \ldots, A_n \Rightarrow C$$

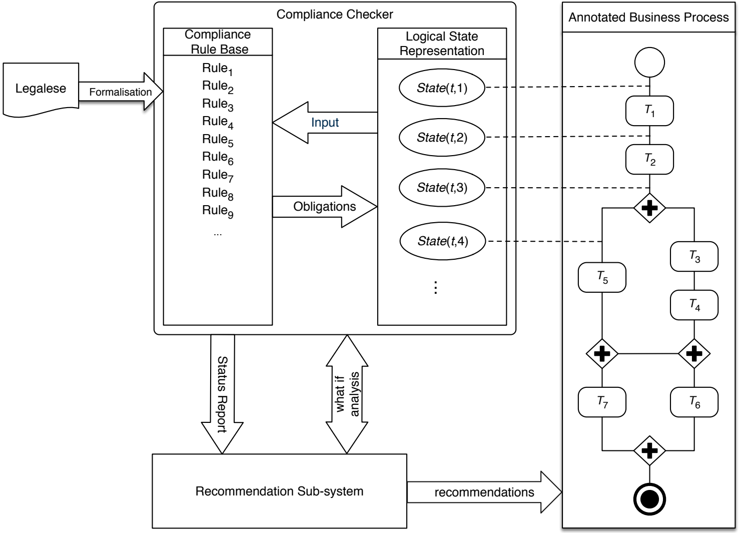
  - prescriptive rules: defining "normative effects" (i.e., obligations, permissions, prohibitions . . .)

$$A_1, \ldots, A_n \Rightarrow [\mathrm{O}]C_1 \otimes [\mathrm{O}]C_2 \otimes \cdots \otimes [\mathrm{O}]C_m$$
$$A_1, \ldots, A_n \Rightarrow [\mathrm{P}]C$$

Reasoning with Norms

1. A is a fact; or
2. there is an applicable rule for A, and either
    1. all the rules for $\neg A$ are discarded (i.e., not applicable) or
    2. every applicable rule for $\neg A$ is weaker than an applicable rule for A.

The Regorous Architecture



Privacy Regorously

- collection of medical information is forbidden
  - c destruction of medical information compensates the illegal collection

$$r_1 : \Rightarrow [\mathrm{O}]\neg \mathit{medicalInfo} \otimes [\mathrm{O}]\mathit{destroy}$$

- collection of medical information is permitted if acting under a court order

$$r_2 : \mathit{courtOrder} \Rightarrow [\mathrm{P}]\mathit{medicalInfo}$$

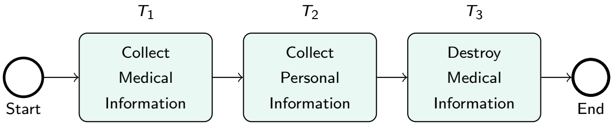
- collection of personal information is forbidden

$$r_3 : \Rightarrow [\mathrm{O}]\neg \mathit{personalInfo}$$

- collection personal information is permitted if collection of medical information is permitted

$$r_4 : [\mathrm{P}]\mathit{medicalInfo} \Rightarrow [\mathrm{P}]\mathit{personalInfo}$$

Are We Regorously Compliant?


T_1
T_2
T_3
Start
Collect Medical Information
Collect Personal Information
Destroy Medical Information
End

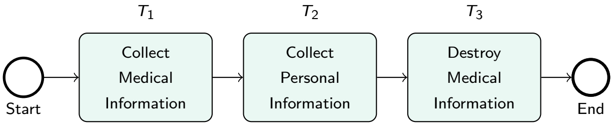
$r_1:\ \Rightarrow [\mathrm{O}]\neg \mathit{medicalInfo} \otimes [\mathrm{O}]\mathit{destroy}$

$r_2:\ \mathit{courtOrder} \Rightarrow [\mathrm{P}]\mathit{medicalInfo}$

$r_3:\ \Rightarrow [\mathrm{O}]\neg \mathit{personalInfo}$

$r_4:\ [\mathrm{P}]\mathit{medicalInfo} \Rightarrow [\mathrm{P}]\mathit{personalInfo}$

Are We Regorously Compliant?


T_1
T_2
T_3
Start
Collect Medical Information
Collect Personal Information
Destroy Medical Information
End

$$State(start) : \neg courtOrder$$

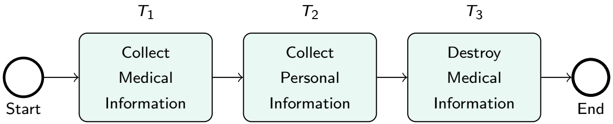
$$r_1 : \ \Rightarrow [\mathrm{O}]\neg medicalInfo \otimes [\mathrm{O}]destroy$$

$$r_2 : courtOrder \Rightarrow [\mathrm{P}]medicalInfo$$

$$r_3 : \ \Rightarrow [\mathrm{O}]\neg personalInfo$$

$$r_4 : [\mathrm{P}]medicalInfo \Rightarrow [\mathrm{P}]personalInfo$$

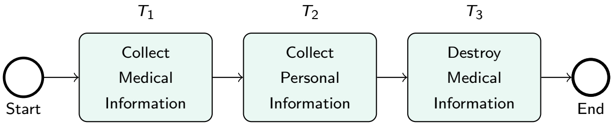
Are We Regorously Compliant?


T_1
T_2
T_3
Start
Collect Medical Information
Collect Personal Information
Destroy Medical Information
End

$$State(start): \neg courtOrder$$
$$Force(T_1): \quad [O]\neg medicalInfo$$
$$\quad [O]\neg personalInfo$$

$$r_1: \ \Rightarrow [O]\neg medicalInfo \otimes [O]destroy$$
$$r_2: courtOrder \Rightarrow [P]medicalInfo$$
$$r_3: \ \Rightarrow [O]\neg personalInfo$$
$$r_4: [P]medicalInfo \Rightarrow [P]personalInfo$$

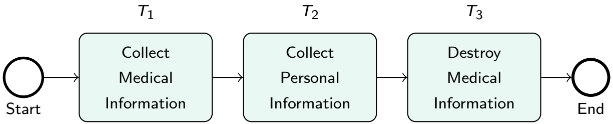
Are We Regorously Compliant?


T_1
T_2
T_3
Start
Collect Medical Information
Collect Personal Information
Destroy Medical Information
End

$$r_1: \Rightarrow [O]\neg medicalInfo \otimes [O]destroy$$
$$r_2: courtOrder \Rightarrow [P]medicalInfo$$
$$r_3: \Rightarrow [O]\neg personalInfo$$
$$r_4: [P]medicalInfo \Rightarrow [P]personalInfo$$

$$\begin{aligned} State(start) &: \neg courtOrder \\ Force(T_1) &: [O]\neg medicalInfo \\ & [O]\neg personalInfo \\ State(T_1) &: medicalInfo \end{aligned}$$

Are We Regorously Compliant?



T_1
T_2
T_3
Collect Medical Information
Collect Personal Information
Destroy Medical Information
Start
End

$r_1 : \Rightarrow [O]\neg medicalInfo \otimes [O]destroy$

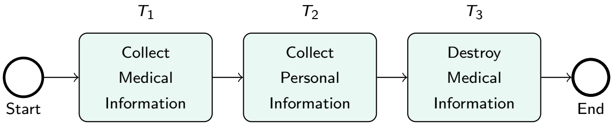
$r_2 : courtOrder \Rightarrow [P]medicalInfo$

$r_3 : \Rightarrow [O]\neg personalInfo$

$r_4 : [P]medicalInfo \Rightarrow [P]personalInfo$

$$\begin{aligned} &State(start) : \neg courtOrder \\ &Force(T_1) : \quad [O]\neg medicalInfo \\ &\qquad\qquad\quad [O]\neg personalInfo \\ &State(T_1) : medicalInfo \\ &Violated(T_1) : [O]\neg medicalInfo \end{aligned}$$

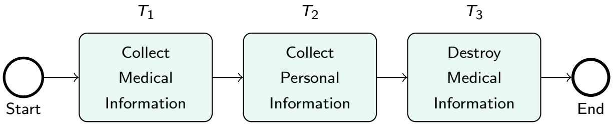
Are We Regorously Compliant?


T_1
T_2
T_3
Start
Collect Medical Information
Collect Personal Information
Destroy Medical Information
End

$$\begin{aligned}
r_1 &: \;\Rightarrow [O]\neg \mathit{medicalInfo} \otimes [O]\mathit{destroy}\\
r_2 &: \mathit{courtOrder} \Rightarrow [P]\mathit{medicalInfo}\\
r_3 &: \;\Rightarrow [O]\neg \mathit{personalInfo}\\
r_4 &: [P]\mathit{medicalInfo} \Rightarrow [P]\mathit{personalInfo}
\end{aligned}$$

$$\begin{aligned}
&\mathit{State}(\mathit{start}) : \neg \mathit{courtOrder}\\
&\mathit{Force}(T_1) : \; [O]\neg \mathit{medicalInfo}\\
&\qquad\qquad\;\; [O]\neg \mathit{personalInfo}\\
&\mathit{State}(T_1) : \mathit{medicalInfo}\\
&\mathit{Violated}(T_1) : [O]\neg \mathit{medicalInfo}\\
&\mathit{Force}(T_2) : [O]\mathit{destroy}
\end{aligned}$$

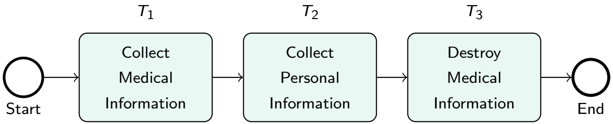
Are We Regorously Compliant?


T_1
T_2
T_3
Start
Collect Medical Information
Collect Personal Information
Destroy Medical Information
End

$$\begin{aligned}
r_1 &: \Rightarrow [O]\neg \mathit{medicalInfo} \otimes [O]\mathit{destroy}\\
r_2 &: \mathit{courtOrder} \Rightarrow [P]\mathit{medicalInfo}\\
r_3 &: \Rightarrow [O]\neg \mathit{personalInfo}\\
r_4 &: [P]\mathit{medicalInfo} \Rightarrow [P]\mathit{personalInfo}
\end{aligned}$$

$$\begin{aligned}
&\mathit{State}(\mathit{start}) : \neg \mathit{courtOrder}\\
&\mathit{Force}(T_1) : \; [O]\neg \mathit{medicalInfo}\\
&\qquad\qquad\;\; [O]\neg \mathit{personalInfo}\\
&\mathit{State}(T_1) : \mathit{medicalInfo}\\
&\mathit{Violated}(T_1) : [O]\neg \mathit{medicalInfo}\\
&\mathit{Force}(T_2) : [O]\mathit{destroy}\\
&\mathit{State}(T_2) : \mathit{personalInfo}
\end{aligned}$$

Are We Regorously Compliant?


T_1
T_2
T_3
Start
Collect Medical Information
Collect Personal Information
Destroy Medical Information
End

$r_1: \ \Rightarrow [\mathrm{O}]\neg medicalInfo \otimes [\mathrm{O}]destroy$

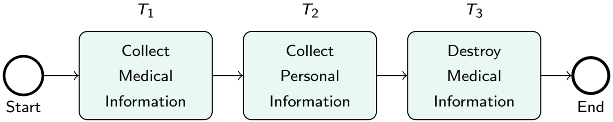
$r_2: courtOrder \Rightarrow [\mathrm{P}]medicalInfo$

$r_3: \ \Rightarrow [\mathrm{O}]\neg personalInfo$

$r_4: [\mathrm{P}]medicalInfo \Rightarrow [\mathrm{P}]personalInfo$

$$\begin{aligned}
&State(start) : \neg courtOrder\\
&Force(T_1) : \quad [\mathrm{O}]\neg medicalInfo\\
&\qquad\qquad\quad [\mathrm{O}]\neg personalInfo\\
&State(T_1) : medicalInfo\\
&Violated(T_1) : [\mathrm{O}]\neg medicalInfo\\
&Force(T_2) : [\mathrm{O}]destroy\\
&State(T_2) : personalInfo\\
&Violated(T_2) : [\mathrm{O}]\neg persoanlInfo
\end{aligned}$$

Are We Regorously Compliant?


T_1
T_2
T_3
Start
Collect Medical Information
Collect Personal Information
Destroy Medical Information
End

$r_1: \ \Rightarrow [O]\neg \mathit{medicalInfo} \otimes [O]\mathit{destroy}$

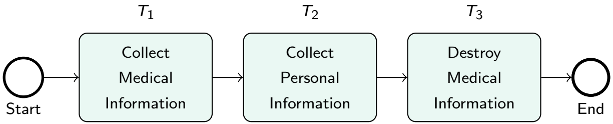
$r_2: \mathit{courtOrder} \Rightarrow [P]\mathit{medicalInfo}$

$r_3: \ \Rightarrow [O]\neg \mathit{personalInfo}$

$r_4: [P]\mathit{medicalInfo} \Rightarrow [P]\mathit{personalInfo}$

$$\begin{aligned}
&\mathit{State}(\mathit{start}) : \neg \mathit{courtOrder}\\
&\mathit{Force}(T_1) : \ [O]\neg \mathit{medicalInfo}\\
&\qquad\qquad\ \ [O]\neg \mathit{personalInfo}\\
&\mathit{State}(T_1) : \mathit{medicalInfo}\\
&\mathit{Violated}(T_1) : [O]\neg \mathit{medicalInfo}\\
&\mathit{Force}(T_2) : [O]\mathit{destroy}\\
&\mathit{State}(T_2) : \mathit{personalInfo}\\
&\mathit{Violated}(T_2) : [O]\neg \mathit{persoanlInfo}\\
&\mathit{State}(T_3) : \mathit{destroy}
\end{aligned}$$

Are We Regorously Compliant?


T_1
T_2
T_3
Start
Collect Medical Information
Collect Personal Information
Destroy Medical Information
End

$r_1 : \Rightarrow [O]\neg medicalInfo \otimes [O]destroy$

$r_2 : courtOrder \Rightarrow [P]medicalInfo$

$r_3 : \Rightarrow [O]\neg personalInfo$

$r_4 : [P]medicalInfo \Rightarrow [P]personalInfo$

$State(start) : \neg courtOrder$

$Force(T_1) : [O]\neg medicalInfo$

$\qquad [O]\neg personalInfo$

$State(T_1) : medicalInfo$

$Violated(T_1) : [O]\neg medicalInfo$

$Force(T_2) : [O]destroy$

$State(T_2) : personalInfo$

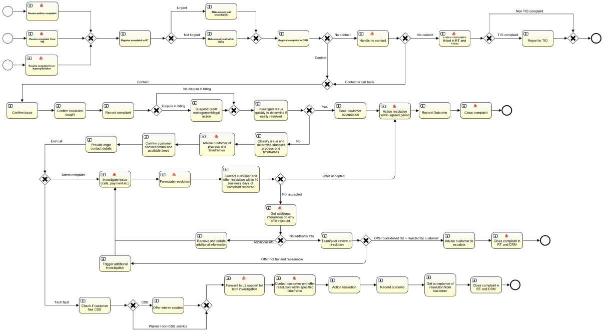
$Violated(T_2) : [O]\neg persoanlInfo$

$State(T_3) : destroy$

$Compensated(T_3) : [O]\neg medicalInfo$

The Regorous Evaluation

Formalised Chapter 8 (Complaints) of TCPC 2012. Modelled the compliant handling/management processes of an Australian telco.


Receive written complaint
Receive complaint from TIO
Receive complaint from Agency/Solicitor
Register complaint in RT
Urgent
Make enquiry call immediately
Not Urgent
Make enquiry call within 48hrs
Register complaint in CRM
No contact
Handle no contact
No contact
Close complaint ticket in RT and CRM
Non TIO complaint
TIO complaint
Report to TIO
Contact
Contact or call back
Contact
No dispute in billing
Confirm issue
Confirm resolution sought
Record complaint
Dispute in billing
Suspend credit management/legal action
Investigate issue quickly to determine if easily resolved
Yes
Seek customer acceptance
Action resolution within agreed period
Record Outcome
Close complaint
No
Classify issue and determine standard process and timeframes
Advise customer of process and timeframes
Confirm customer contact details and available times
Provide engin contact details
End call
Admin complaint
Investigate issue (calls, payment etc)
Formulate resolution
Contact customer and offer resolution within 10 business days of complaint received
Offer accepted
Not accepted
Get additional information on why offer rejected
Receive and collate additional information
Additional info
No additional info
Team/peer review of resolution
Offer considered fair + rejected by customer
Advise customer to escalate
Close complaint in RT and CRM
Trigger additional investigation
Offer not fair and reasonable
Forward to L2 support for tech investigation
Contact customer and offer resolution within specified timeframe
Action resolution
Record outcome
Get acceptance of resolution from customer
Close complaint in RT and CRM
Tech fault
Check if customer has CSG
CSG
Offer interim solution
Waiver / non-CSG service

41 tasks, 12 decision points (xor), 2 loops
shortest trace: 6 traces longest trace (loop): 33 tasks
longest trace (no loop): 22 tasks
over 1000 traces, over 25000 states

The Regorous Evaluation

TCPC 2012 Chapter 8. Contains over 100 commas, plus 120 terms (in Terms and Definitions Section).
Required 223 propositions, 176 rules.

Punctual Obligation	5	(5)
Achievement Obligation	90	(110)
Preemptive	41	(46)
Non preemptive	49	(64)
Non perdurant	5	(7)
Maintenance Obligation	11	(13)
Prohibition	7	(9)
Non perdurant	1	(4)
Permission	9	(16)
Compensation	2	(2)

Questions?

Guido Governatori

guido.governatori@data61.csiro.au

References

- Silvano Colombo Tosatto, Guido Governatori and Pierre Kelsen. “Business Process Regulatory Compliance is Hard”. In: *IEEE Transactions on Services Computing* 8.6 (2015), pp. 958–970. DOI: 10.1109/TSC.2014.2341236.
- Guido Governatori. “The Regorous approach to process compliance”. In: *2015 IEEE 19th International Enterprise Distributed Object Computing Workshop*. (Adelaide, Australia, 21 Sept. 2015). IEEE Press, 2015, pp. 33–40. DOI: 10.1109/EDOC.2015.28.
- Guido Governatori. “Thou Shalt is not You Will”. In: *Proceedings of the Fifteenth International Conference on Artificial Intelligence and Law*. (San Diego, 8–14 June 2015). Ed. by Katie Atkinson. New York: ACM, 2015, pp. 63–68. DOI: 10.1145/2746090.2746105.
- Guido Governatori and Mustafa Hashmi. “No Time for Compliance”. In: *2015 IEEE 19th Enterprise Distibuted Object Computing Conference*. (Adelaide, 21–25 Sept. 2015). Ed. by Sylvain Hallé and Wolfgang Mayer. IEEE, 2015, pp. 9–18. DOI: 10.1109/EDOC.2015.12.
- Guido Governatori and Shazia Sadiq. “The Journey to Business Process Compliance”. In: *Handbook of Research on BPM*. Ed. by Jorge Cardoso and Wil van der Aalst. IGI Global, 2009. Chap. 20, pp. 426–454. eprint: http://www.governatori.net/papers/2009/handbook09journey.pdf.
- Shazia Sadiq and Guido Governatori. “Managing Regulatory Compliance in Business Processes”. In: *Handbook of Business Process Management 2nd edition*. Ed. by Jan vom Brocke and Michael Rosemann. 2nd ed. Vol. 2. International Handbooks on Information Systems. Berlin-Heidelberg: Springer, 2015. Chap. 11, pp. 265–288. DOI: 10.1007/978-3-642-45103-4_11.