Company Focused Case Study – Legally Compliant Case

A) Descriptions

As mentioned earlier, the Banana Inc. aims to work in Europe and Canada. Since the company is collecting personal information from the users, they need to comply with EU and Canadian regulations related to collect, use and disclosure of personal information.

In Canada, Personal Information Protection and Electronic Documents Act (PIPEDA) (http://laws-lois.justice.gc.ca/eng/acts/p-8.6/) is the federal regulation for protecting the privacy of the users. In Europe, European Union (EU) has passed a new regulation, which is based on the EU Data Protection Directive 1995 and it is called EU Data Protection regulation (http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:31995L0046).

In order to be compliant to the regulations and not get financial penalties and reputation loss, company x needs to comply with these two regulations. Since, the company deals with the collect, use and disclosure of personal data, the articles specifically related to these actions need to be considered as the starting point.

Here, we provide few of the articles the company needs to be compliant with:

- EU Data Protection Directive –

Article 6. Member States shall provide that personal data must be:

- ✓ (a) processed fairly and lawfully;
- ✓ (b) collected for specified , explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
- ✓ (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed ;
- ✓ (d) accurate and, where necessary, kept up to date ; every reasonable step must be taken to ensure that data which are inaccurate or incomplete , having regard to the purposes for which they were collected or for which they are further processed , are erased or rectified;
- ✓ (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed . Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

Article 7. Member States shall provide that personal data may be processed only if:

- ✓ (a) the data subject has unambiguously given his consent; or
- ✓ (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

- ✓ (c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
- ✓ (d) processing is necessary in order to protect the vital interests of the data subject; or
- ✓ (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
- ✓ (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed , except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 d).

Article 10. Information in cases of collection of data from the data subject Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information , except where he already has it:

- ✓ (a) the identity of the controller and of his representative, if any;
- ✓ (b) the purposes of the processing for which the data are intended;
- ✓ (c) any further information such as — the recipients or categories of recipients of the data , — whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply, — the existence of the right of access to and the right to rectify the data concerning him in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

Article 17. Security of processing –

1 . Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

2 . The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

3 . The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that: — the processor shall act only on instructions from the controller, — the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.

4 . For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.

Article 19. Contents of notification –
1 . Member States shall specify the information to be given in the notification. It shall include at least:

- ✓ (a) the name and address of the controller and of his representative , if any;
- ✓ (b) the purpose or purposes of the 'processing;
- ✓ (c) a description of the category or categories of data subject and of the data or categories of data relating to them;
- ✓ (d) the recipients or categories of recipient to whom the data might be disclosed ; (e) proposed transfers of data to third countries;
- ✓ (f) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 17 to ensure security of processing.

2. Member States shall specify the procedures under which any change affecting the information referred to in paragraph 1 must be notified to the supervisory authority.

- PIPEDA

Article 6.1 – Valid Consent - For the purposes of clause 4.3 of Schedule 1, the consent of an individual is only valid if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting.

Article 7. (1) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may collect personal information without the knowledge or consent of the individual only if

- ✓ (a) the collection is clearly in the interests of the individual and consent cannot be obtained in a timely way;
- ✓ (b) it is reasonable to expect that the collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province; (b.1) it is contained in a witness statement and the collection is necessary to assess, process or settle an insurance claim; (b.2) it was produced by the individual in the course of their employment, business or profession and the collection is consistent with the purposes for which the information was produced;
- ✓ (c) the collection is solely for journalistic, artistic or literary purposes;
- ✓ (d) the information is publicly available and is specified by the regulations; or
- ✓ (e) the collection is made for the purpose of making a disclosure (i) under subparagraph (3)(c.1)(i) or (d) (ii), or (ii) that is required by law

Article 7.2 (1) In addition to the circumstances set out in subsections 7(2) and (3), for the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, organizations that are parties to a prospective business transaction may use and disclose personal information without the knowledge or consent of the individual if:

- ✓ (a) the organizations have entered into an agreement that requires the organization that receives the personal information
    - (i) to use and disclose that information solely for purposes related to the transaction,
    - (ii) to protect that information by security safeguards appropriate to the sensitivity of the information, and
    - (iii) if the transaction does not proceed, to return that information to the organization that disclosed it, or destroy it, within a reasonable time; and
- ✓ (b) the personal information is necessary
    - (i) to determine whether to proceed with the transaction, and
    - (ii) if the determination is made to proceed with the transaction, to complete it.

Article 7.4 (1) Use without consent - Despite clause 4.5 of Schedule 1, an organization may use personal information for purposes other than those for which it was collected in any of the circumstances set out in subsection 7.2(1) or (2) or section 7.3.

Article 7.4 (2) Disclosure without consent Despite clause 4.5 of Schedule 1, an organization may disclose personal information for purposes other than those for which it was collected in any of the circumstances set out in subsection 7.2(1) or (2) or section 7.3. 2015, c. 32, s. 7.

B) Questions

1) Select some of the relevant legal statements.
2) Identify legal actors in the selected legal statements.
3) Develop a Hohfeldian model of the selected legal statements. Note that for start some of the models have been done.
4) Identify the legal Intentional Elements (i.e. softgoals, goals, tasks, resources, ..) for each of the actors and for each article.
5) Create GRL models for each of the actors and provide the links between them
6) Analyze the compliance of Banana Inc. and Bonzo with the legal documents.