FIDI ACCREDITED INTERNATIONAL MOVER

Version 3.1

Annex 01: FAIM Data (Privacy) Protection

FAQ

September 2016

Annex 01 FAIM Data (Privacy) Protection – FAQ

The purpose of this document is to prepare our communication to FIDI Affiliates on this topic. The list is non-exhaustive and can be amended based on specific questions from Affiliates.

1. *Is Data (Privacy) Protection Management addressed in FAIM 3.1?*

Yes; Data (Privacy) Protection Management has been incorporated in the FAIM 3.1 Standard.

2. *Why did FIDI introduce Data (Privacy) Protection Management in FAIM 3.1?*

Good privacy is good business. Good privacy practices are a key part of corporate governance and accountability. One of today's key business imperatives is maintaining the privacy of personal information. As business systems and processes become increasingly complex and sophisticated, organizations are collecting growing amounts of personal information. As a result, personal information is vulnerable to a variety of risks, including loss, misuse, unauthorized access, and unauthorized disclosure.

FIDI-FAIM Applicants are trying to strike a balance between the proper collection and use of their customers' personal information as individuals expect their privacy to be respected and their personal information to be protected by the organizations with which they do business. Customers are no longer willing to overlook an organization's failure to protect their privacy.

3. *What is Data (Privacy) Management Protection about?*

Data (Privacy) Protection Management is the systematic application of management policies, procedures and practices with respect to the collection, use, retention, disclosure, and disposal of personal information in conformity with the commitments described in the Applicant's privacy notice.

4. *What is a Privacy Notice?*

A privacy notice is a statement of the overall intentions and direction of a company describing its commitment how personal information is collected, used, retained, disclosed, and disposed.

By privacy we mean the rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure, and disposal of personal information.

5. *What do you mean by Personal Information?*

Personal information (sometimes referred to as personally identifiable information) is information that concerns, or can be related to, an identifiable individual. Some examples of personal information are as follows:

- Name
- Home or e-mail address
- Date of Birth
- Identification number (for example, a Social Security or Social Insurance Number)
- Physical characteristics

6. *What are the specific risks of having inadequate privacy policies and procedures related to Data (Privacy) Protection Management?*

The following are specific risks of having inadequate privacy policies and procedures:

- Damage to the organization's reputation, brand, or business relationships
- Legal liability and industry or regulatory sanctions
- Charges of deceptive business practices
- Customer or employee distrust
- Denial of consent by individuals to have their personal information used for business purposes
- Lost business and consequential reduction in revenue and market share
- Disruption of international business operations
- Liability resulting from identity theft

7. *What exactly does the FAIM 3.1 Standard cover and what does it requires from the Applicant?*

The FAIM 3.1 Standard covers topics related to personal information only. Personal information (also sometimes referred to as personally identifiable information) is information that concerns, or can be related to, an identifiable individual.

FAIM 3.1 requests that the Applicant must have a documented process in place ensuring that personal information is collected, used, retained, disclosed, and disposed of in conformity with the commitments described in the Applicant's privacy notice.

8. *What are the FAIM 3.1 audit evidence requirements?*

The Applicant needs to demonstrate that it has a documented data (privacy) protection procedure in place ensuring that personal information is collected, used, retained, disclosed, and disposed of in conformity with the commitments described in your company's privacy notice.

The Applicant's data (privacy) protection procedure needs to address the following 10 minimum privacy principles:

1. Management:
   The Applicant defines, documents, communicates, and assigns accountability for its privacy policies and procedures.

2. Notice:
   The Applicant provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.

3. Choice and consent:
   The Applicant describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.

4. Collection:

   The Applicants collects personal information only for the purposes identified in the notice.

5. Use, retention, and disposal:

   The Applicant limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The Applicant retains personal information for only as long as necessary to fulfil the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.

6. Access:

   The Applicant provides individuals with access to their personal information for review and update.

7. Disclosure to third parties:

   The Applicant discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.

8. Security for privacy:

   The Applicant protects personal information against unauthorized access (both physical and logical).

9. Quality:

   The Applicant maintains accurate, complete, and relevant personal information for the purposes identified in the notice.

10. Monitoring and enforcement:

    The Applicant monitors compliance with its privacy policies and procedures and has procedures to address privacy related complaints and disputes.

The above mentioned data (privacy) protection procedure needs to be monitored and reviewed.

Furthermore, the Applicant needs to demonstrate that its privacy notice has been communicated to internal personnel (staff).

9. Is the data we hold on our own Staff included as part of FAIM requirements for Data Protection?

The data (related to personal information) concerning your own staff has also to be addressed in your procedures however the focus during the onsite visit will be on your end-customers (private and corporate customers) and your supply chain.

10. *Is Outsourcing & Supply Chain addressed in FAIM 3.1 in relation to Data (Privacy) Protection Management?*

Yes; Outsourcing increases the complexity for dealing with privacy. A FIDI-FAIM Applicant may outsource a part of its business process and, with it, some responsibility for privacy; however, the Applicant cannot outsource its ultimate responsibility for privacy for its business processes. Complexity increases when the entity that performs the outsourced service is in a different country and may be subject to different privacy laws or perhaps no privacy requirements at all. In such circumstances, the Applicant that outsources a business process will need to ensure it manages its privacy responsibilities appropriately.

11. *What are the FAIM 3.1 audit requirements regarding Supply Chain?*

The Applicant must demonstrate the process to control Data Protection (privacy) in its Supply Chain.

12. *Are our move files being checked during the on-site visit and how exactly?*

Yes; during the on-site audit the Auditor will check mainly for compliance in move files where you were acting as the booker of the move and you outsourced the origin services and/or the destination services to non-FIDI agents. The Auditor will randomly select files among the Applicant's active or complete files.

The auditor will verify following:

- The Applicant needs to demonstrate that its move files are compliant where its company was acting as the booker of the move and the Applicant communicated its company's privacy notice to its Supply Chain.

- The Applicant needs to demonstrate that its move files are compliant where its company was acting as the booker of the move and the Applicant communicated its company's privacy notice to its private customers and corporate accounts.

  At least 80% of files must meet the Standard.

13. *What in case our company has its own Data (privacy) Protection Policy?*

In case your company has its own Data (Privacy) Protection Policy you need to indicate where on your existing documents the core elements as described above are included.

14. *We store all our customer data on a password protected XL sheet, is this OK?*

In case this solution is aligned with your procedure as described under principle 8 (see question 8 above, which states: "Security for privacy - the Applicant protects personal information against unauthorized access"), it meets the FAIM 3.1 minimum requirements.

15. Definitions used in Data (Privacy) Protection Management.

Privacy: The rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure, and disposal of personal information.

Data (Privacy) Protection Management: Systematic application of management policies, procedures and practices with respect to the collection, use, retention, disclosure, and disposal of personal information in conformity with the commitments described in the Applicant's Privacy Notice.

Privacy Notice: Statement of the overall intentions and direction of a company describing its commitment how Personal Information is collected, used, retained, disclosed, and disposed.

Principles: set of statements generally accepted in data (privacy) protection management.

Personal information: (sometimes referred to as personally identifiable information) information that concerns, or can be related to, an identifiable individual.

Individuals, for this purpose, include prospective, current, and former customers, employees, and others with whom the entity has a relationship. Most information collected by an organization about an individual is likely to be considered personal information if it can be attributed to an identified individual. Some examples of personal information are as follows:

- Name
- Home or e-mail address
- Date of Birth
- Identification number (for example, a Social Security or Social Insurance Number)
- Physical characteristics

Sensitive information: Some personal information is considered sensitive. Some laws and regulations define the following to be sensitive personal information:

- Information on medical or health conditions
- Financial information
- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Sexual preferences
- Information related to offenses or criminal convictions

Non-personal information: information about or related to people that cannot be associated with specific individuals. This includes statistical or summarized personal information for which the identity of the individual is unknown or linkage to the individual has been removed. In such cases, the individual's identity cannot be determined from the information that remains because the information is de-identified or anonymized. Non-personal information ordinarily is not subject to privacy protection because it cannot be linked to an individual. However, some organizations may still have obligations over non-personal information due to other regulations and agreements

Privacy or Confidentiality?

Unlike personal information, which is often defined by law or regulation, no single definition of confidential information exists that is widely recognized. In the course of communicating and transacting business, partners often exchange information or data that one or the other party requires be maintained on a "need to know" basis. Examples of the kinds of information that may be subject to a confidentiality requirement include the following:

- Transaction details
- Engineering drawings
- Business plans
- Banking information about businesses
- Inventory availability
- Bid or ask prices
- Price lists
- Legal documents
- Revenue by client and industry

Also, unlike personal information, rights of access to confidential information to ensure its accuracy and completeness are not clearly defined. As a result, interpretations of what is considered to be confidential information can vary significantly from organisation to organisation and, in most cases, are driven by contractual arrangements.

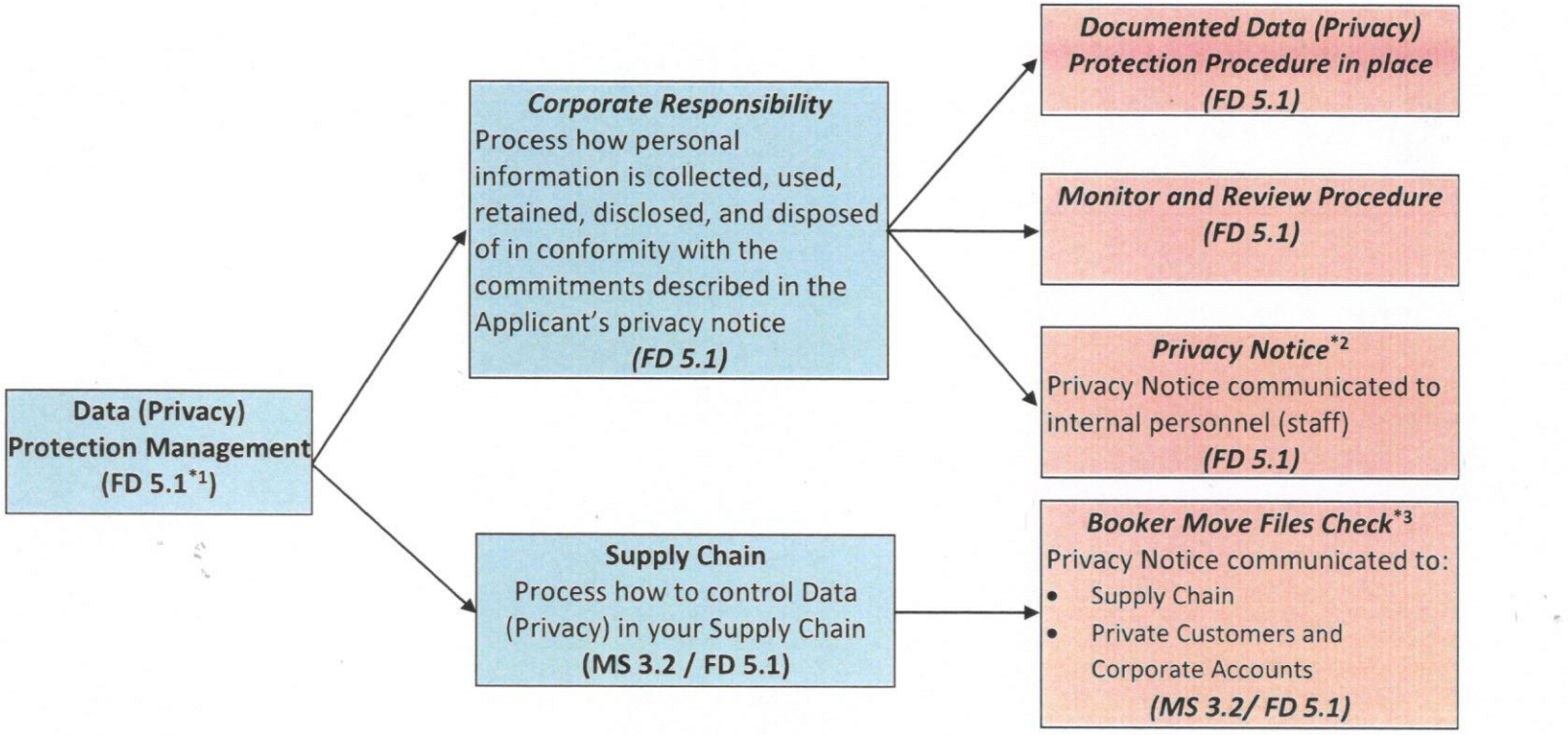
Explicit consent: "Explicit" in the data protection world generally means "specific". In other words the consent must specify the particular types of data, the specific purposes for which they may be used and/or the countries to which they may be disclosed.

Implicit consent: "Implicit" refers to "not specific" It is consent which is not expressly granted by a person or company, but rather inferred from a person or company's actions and the facts and circumstances of a particular situation.

Supply Chain: A Supply Chain is a system of organisations, companies, people, activities, information, and resources involved in moving a product or service from supplier to customer.

Supply Chain Management: The network created amongst different companies producing, handling and/or distributing a specific product or service. Specifically, the supply chain encompasses the steps it takes to get a good or service from the supplier to the customer. Supply chain management is a crucial process for many companies, and many companies strive to have the most optimized supply chain because it usually translates to being able to deliver a higher overall quality performance resulting in lower costs for the company.

16. Graphical overview of Data (Privacy) Protection Management in FAIM 3.1 and the related Audit Requirements.



**1 Please find the detailed explanation of the above mentioned topics in the FAIM 3.1 Pre-Audit Assessment Checklist.*
**2 Privacy Notice: Statement of the overall intentions and direction of a company describing its commitment how Personal Information is collected, used, retained, disclosed, and disposed.*
**3 During the on-site audit the Auditor will focus on core outsourced infrastructure services (operative labour, drivers, vehicles and warehousing) and will check mainly for compliance in move files where you were acting as the booker of the move and you outsourced the origin services and/or the destination services to non-FIDI agents.*

Agreement

I confirm that I have read and understood the FIDI Data (Privacy) Protection .

I accept and agree to abide by this Character, and the code of Conduct which is included in the FAIM pre- requirements. Non-compliance with FAIM pre-requirements will result in expulsion from the FIDI organization.

Date: **3rd May,2017**

Individual: **Ehsan Ul Haq**

Title: **CEO**

For and on the behalf of (Affiliate Company)**Express Movers (Pvt) Ltd.**