FAIM 2022

FAQ 01

FAIM Data (Privacy) Protection

FIDI ACCREDITED INTERNATIONAL MOVER

September 2022

INDEX OF QUESTIONS

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?

Yes; Data (Privacy) Protection Management has been incorporated in the FAIM Standard since version 3.1, as approved at the FIDI Cape Town conference in March 2015.

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

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, organisations are collecting growing amounts of personal information. As a result, personal information is vulnerable to a variety of risks, including loss, misuse, unauthorised access and unauthorised 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 organisations with which they do business. Customers are no longer willing to overlook an organisation's failure to protect their privacy.

Furthermore, FAIM has recognised the concept of increased and more stringent privacy regulations since its 3.1 version, giving FIDI Affiliates an important advantage in preparation for the General Data Protection Regulation (GDPR), which came into force in May 2018. The main data privacy elements incorporated in the current FAIM Standard reinforce the previous FAIM 3.1 data protection requirements.

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 your company'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 to the collection, use, retention, disclosure and disposal of personal information.

By privacy, we mean the rights and obligations of individuals and organisations 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 inadequate privacy policies and procedures related to Data (Privacy) Protection Management?

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

- Damage to the organisation'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 Standard cover and what does it require from my company?

The FAIM 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 requests that your company 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 your privacy notice.

8. What are the FAIM audit evidence requirements?

You need to demonstrate that your company 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 privacy notice.

Your data (privacy) protection procedure needs to address the following 10 minimum privacy principles:

1. Management:

   You clearly define, document, communicate and assign accountability for your company's privacy policies and procedures.

   You create an overview of all data processing activities, documenting which personal data is processed, where it comes from and with whom it has been shared.

2. Notice:

   You provide notice about your privacy policies and procedures and identify the purposes for which personal information is collected, used, retained and disclosed.

3. Choice and consent:

   You describe the choices available to the individual and obtain implicit or explicit consent with respect to the collection, use and disclosure of personal information.

   Consent must be verifiable, i.e. you must have a record indicating how and when consent was given.

4. Collection:

   You collect personal information only for the purposes identified in the notice.

5. Use, retention and disposal:

   You limit the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. You retain personal information only for as long as necessary to fulfil the stated purposes or as required by law or regulations, and thereafter appropriately dispose of such information.

6. Access:

   You provide individuals with access to their personal information for review and update.

7. Disclosure to third parties:

   You disclose 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:

   You protect personal information against unauthorized access (both physical and logical).

   You must have a documented procedure in place, explaining how to handle a potential data breach, i.e. a breach of security leading to the destruction, loss, alteration or unauthorised disclosure of, or access to personal data.

9. Quality:

   You maintain accurate, complete and relevant personal information for the purposes identified in the notice.

10. Monitoring and enforcement:

    You monitor compliance with your company's privacy policies and procedures, and you have procedures in place to address privacy related complaints and disputes.

You need to review all policies, procedures, controls and the documents that are an integral part of it.

The above-mentioned data (privacy) protection procedure needs to be monitored and reviewed on a regular basis.

Furthermore, you need to demonstrate that your company's privacy notice has been communicated to internal 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 also has to be addressed in the procedures. However, the focus during the third party audit will be on your end-customers (private and corporate customers) and supply chain.

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

Yes; outsourcing increases the complexity for dealing with privacy. A FIDI-FAIM Applicant may outsource part of its business process and with it some responsibility for privacy. However, you cannot outsource the ultimate responsibility for privacy for your 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, you will need to ensure it manages its privacy responsibilities appropriately.

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

You must demonstrate that you have a process in place to control data (privacy) protection in your supply chain.

12. Are our move files being checked during the third party audit and how exactly?

Yes; during the audit the Auditor will check mainly for compliance in move files where you were acting as the booker and/or Origin/Destination Agent of the move. The Auditor will randomly select files among your active or complete files and at least 80% of your files must meet the below stated requirements:

- You need to demonstrate that your move files are compliant where your company was acting as the booker and/or Origin/ Destination Agent of the move, and that you communicated your company's privacy notice to your supply chain.

- You need to demonstrate that your move files are compliant where your company was acting as the booker and/or Origin/ Destination Agent of the move, and that you communicated your company's privacy notice to your private customers and corporate accounts.

For a graphical overview of the FAIM audit requirements, please refer to question 17.

For more information on move files' check in relation to the General Data Protection Regulation (GDPR), please refer to the following link in FIDINET:
http://portfolio.cpl.co.uk/FIDI-Focus/290/24/

13. What happens if our company has its own Data (privacy) Protection Policy?

If your company has its own Data (Privacy) Protection Policy, you need to indicate where in your existing documents you included the 10 minimum privacy principles, as described in question 8.

14. We store all our customer data on a password protected Excel 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 - you protect personal information against unauthorized access"), it meets the FAIM minimum requirements.

15. My company is FAIM compliant; does that guarantee that my company is automatically compliant with GDRP?

The previous FAIM 3.1 Quality Standard, approved at the FIDI Cape Town conference in March 2015, already recognised the concept of increased and more stringent privacy regulations, giving FIDI Affiliates an important advantage in preparation for the new GDPR, which came into force in May 2018. However, being FAIM compliant does not mean that your company is automatically GDPR compliant. You will have to go through the process of analysing and amending your internal procedures to be aligned with this particular European regulation, within the framework of your specific business setup.

It is important to understand that there is no direct relation between FAIM and the GDPR. Indirectly FAIM can be used as a stepping-stone towards demonstrating GDPR compliance, but the GDPR is a legal regulation with a different scope and objective than FAIM.

16. What are the definitions used in FAIM related to Data (Privacy) Protection Management?

Privacy: The rights and obligations of individuals and organisations 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 your privacy notice.

Privacy Notice: Statement of the overall intentions and direction of a company describing its commitment to the collection, use, retention, disclosure and disposal of personal information.

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 any other natural persons with whom the entity has a relationship. Most information collected by an organisation 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 any link 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 organisations may still have obligations over non-personal information due to other existing regulations and agreements.

Privacy or Confidentiality?

Unlike personal information, which is often defined by law or regulation, there is no widely recognized definition for confidential information. 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 types 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

In addition, 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 one organisation to another and generally 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 requested, the specific purposes for which they may be used and/or the countries to which they may be disclosed.

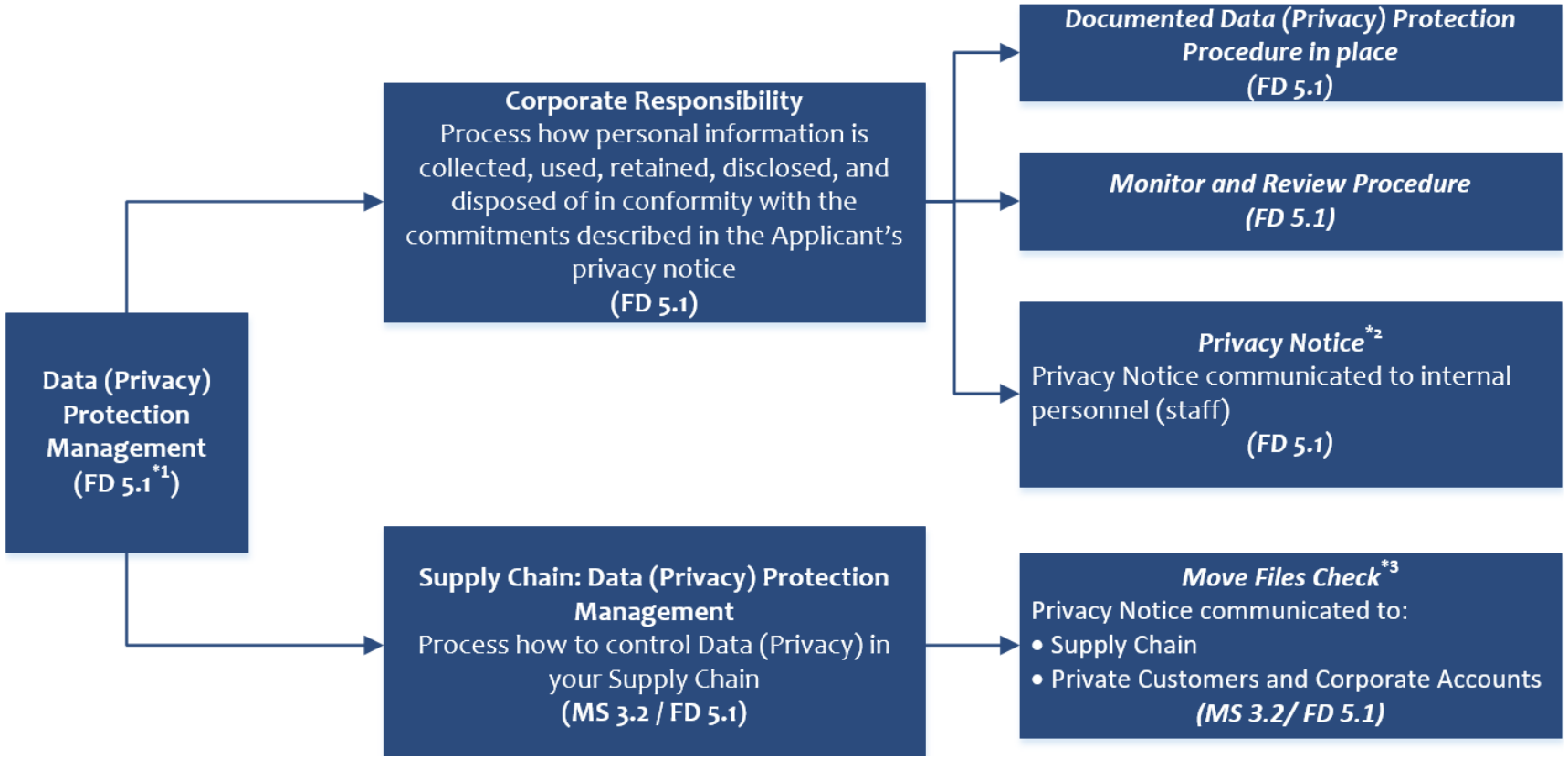
Implicit consent: "Implicit" refers to "not specific". In this case, consent is not expressly granted by a person or company, but rather inferred from a person or company's actions and the facts and circumstances of a particular situation.

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 a company. Many companies strive to have the most optimized supply chain, as this usually translates into being able to deliver a higher overall quality performance, resulting in lower costs for the company.

Logical security and physical security: Logical security protects computer software by discouraging user excess by implementing user identifications, passwords, authentication, biometrics and smart cards. Physical security prevents and discourages attackers from entering a building by installing fences, alarms, cameras, security guards and dogs, electronic access control, intrusion detection and administration access controls. The difference between logical security and physical security is that logical security protects access to computer systems whereas physical security protects the site and everything located within the site.

17. Graphical overview of Data (Privacy) Protection Management and the related FAIM audit requirements.



*1 Please find the detailed explanation of the above-mentioned topics in the FAIM 2022 Pre-Audit Assessment Checklist

*2 Privacy Notice: Statement of the overall intentions and direction of a company, describing its commitment to the collection, use, retention, disclosure and disposal of personal information.

*3 During the third party audit, the Auditor will focus on the requirement "MS 3.2 Supply Chain; Quality Management" on demonstrating compliance in move files, mainly depending on your business set-up. Furthermore, the emphasis will be on third-parties in your supply chain that are likely to be in direct contact with the end-customer.

Examples of moves files for assessment could be:

- 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 (I.e. booker moves & third-country moves).
- Where you were acting as the booker or Origin/ Destination Agent on behalf of an RMC or move management company.
- Where you were acting as the booker and you outsourced core infrastructure services. +
- Where you were acting as the Origin/ Destination Agent and you outsourced core infrastructure services. +

+ Core infrastructure services are operative labour, drivers, vehicles and warehousing.

The Auditor will randomly select files among your active or complete files. At least 80% of selected files must meet the Standard.