LINKBYNET.COM

LINKBYNET

Binding Corporate Rules | BCR Linkbynet

Controller and Processor BCR

CONTENTS

1. Preliminary Remarks 5
2. Definitions 5
3. Scope of the binding corporate rules 6
   3.1. Geographical scope 6
   3.2. Linkbynet's entities concerned by the BCR 6
   3.3. Datas concerned by the BCR and purposes 7
4. Description of operations 7
5. Obligations of the entities involved in the transfer of data 7
   5.1. As regards the compliance with regulation and BCR 7
   5.2. With regards to data quality and purpose of transfer 8
   5.3. As regards Sensitive Data and automated individual decisions 9
   5.4. Sub-processing 9
6. Data subjects 10
   6.1. Data subject's rights 10
7. Confidentiality with regards to Personal Data 11
   7.1. For Internal and Hosted Data 11
   7.2. For Hosted Data 12
   7.3. Limited right of disclosure 12
8. Security with regards to Personal Data 12
9. Linkbynet's internal organization to ensure effectiveness of the BCR 12
   9.1. Data Protection management and follow-up of the BCR 12
   9.2. Complaint handling 13
   9.3. Applicable terms to Linkbynet's employees 14
   9.4. Data Protection Training 14
10. Right to Audit of the Controller 15
11. Data protection authority 15
12. Access to binding corporate rules 15
13. Review of Binding Corporate Rules 16
14. Disputes, JURISDICTION AND applicable law 16
   14.1. Applicable law and national legislation 16
   14.2. Burden of proof and data protection abilities within Linkbynet 16
   14.3. Disputes between Importer, Exporter and/or Sub-processor 17
15. Effective date 17

16. Appendices to the BCR 17

APPENDIX A - LIST OF LINKBYNET'S ENTITIES BOUND BY THE BCR 18

APPENDIX B - ROLES AND POSITION OF THE ENTITIES INVOLVED IN A DATA TRANSFER 19

APPENDIX C - LIST OF PROCESSED OPERATIONS 20

APPENDIX D - EXTRACT OF THE INFORMATION SYSTEM SECURITY POLICY 21

APPENDIX E - EXTRACTS OF STANDARD COMPLIANCE CHECK PROCEDURE 23

(TRANSLATED FROM FRENCH) 23

APPENDIX F - EXTRACTS OF COMPLAINT HANDLING PROCEDURE 24

(TRANSLATED FROM FRENCH) 24

APPENDIX G - EXTRACTS OF TRAINING PROGRAM FOR LINKBYNET INDIAN OCEAN 26

(TRANSLATED FROM FRENCH) 26

Log book
In order to facilitate the communication between teams, respective contact details have been inserted in the header of this document.

	LINKBYNET
Contact	**Ramakrishna MADOO**
Position	**Quality assistant**
Landline	+33 (0)1.48.13.29.94
Email	r.madoo@linkbynet.com
Fax	n/a
Address	8th Floor, Orbis Court, 132 Route St Jean
Zip code - City	Quatre Bornes, Mauritius

REVISION & VALIDATION
In order to control the document review, a revision and follow up table has been inserted below.

Date	Version	Object		
		Création	Confirmation	Approval
29/04/2014	3	Isabelle ANDRICQUE Sollicitor	Solange LEMAIRE Quality Manager	Pôle BCR - CNIL *(en lien avec les DPA Espagnoles et Irlandaises)*
17/01/2014	2	Ramakrishna MADOO Quality assistant	Isabelle ANDRICQUE Solicitor	Responsable département international CNIL
11/09/2012	1	Document Creation		
		Ramakrishna MADOO Quality assistant	Isabelle ANDRICQUE Solicitor Solange LEMAIRE Quality Manager	

Preamble
This document is strictly confidential.
It cannot be disclosed in whole or in part to a third party, by any means and for any purpose whatsoever, without prior written consent of LINKBYNET.

1. PRELIMINARY REMARKS

Always vigilant on ensuring trusting relationships with its partners, customers and employees, Linkbynet is constantly striving to improve the quality of the services it offers. This is clearly put in light with its governance policy aiming at settling a fairer and safer company. As actions speak louder than words, Linkbynet has decided to adopt the Binding Corporate Rules (BCR) in order to guarantee an adequate and effective protection to the personal data it has to deal with in the framework of its operations.

The quality of service that Linkbynet offers to its customers is based on a follow-the-sun workflow relying on its international entities and specially the possibility for all its entities to have access to the data hosted on behalf of its customers. For this purpose, Linkbynet has to perform transfers of data outside the European Economic Area (EEA) within the meaning of the applicable law.

The purpose of these BCR is to cover and regulate such transfer of data between Linkbynet's entities, in accordance with data protection laws specially European Union Directive 95/46/EC dated 24 October 1995 and European Union Directive 2002/58/EC dated 12 July 2002.

The rules contained in these BCR allows customers, employees and any concerned person, to be sure that their rights as regards to their "personal information" (any information that relates to them, such as a name, contact details, shopping habits, preferences, etc.) are respected and that they have the right to control their use.

2. DEFINITIONS

The terms mentioned in the binding corporate rules of Linkbynet have the following meaning. Some of these definitions are based on the terms (personal data, data processor and data controller) defined in the directive 95/46/EC dated 24 October 1995 and Directive 2002/58/EC dated 12 July 2002. For a better understanding of the terms Controller, Processor, Sub-Processor, Exporter and Importer, some diagrams describing the situations are inserted in Appendix B - of the BCRs.

"Controller", the natural person or legal person, public authority, agency or any other body which alone or jointly with others, determines the purposes and means of the processing of Personal data. Where the purposes and means of processing are determined by national or Community laws or regulations the Controller or the specific criteria for his nomination may be designated by National or Community law. In the light of Linkbynet's activities, the Controller is:

- The concerned Linkbynet's entity, for Internal data.
- Linkbynet's concerned customer, for Hosted data.

"Data subject" is the identified or identifiable natural person to whom the personal data relates.

"Exporter" is the entity transferring its data from the European Union to an entity based in a country that does not possess an adequate level of protection. The Exporter is the Controller, regardless of the situation (Hosted or Internal Data).

"Hosted data" means data controlled by Linkbynet's customers and hosted by Linkbynet on their behalf (acting as a Processor as explained in Appendix B).

"Internal data" means data controlled by one of Linkbynet's entities (acting as a Controller as explained in Appendix B).

"Importer" is a Linkbynet's entity based outside the European Union in a country that does not provide an acceptable level of protection. The Importer will be the recipient of transfers from the Exporter. Depending on the situations, the Importer is either the Processor or the Sub-processor (as further explained in Appendix B -).

"Linkbynet" is the group of entities which consists of LBN and its affiliates as defined by Articles L.233-1 to L.233-3 and L.233-16 of the French Commercial code. It may be used to designate either one entity of the group or the entire group; depending on the context where it is used.

"LBN" is the headquarter of Linkbynet's group, Linkbynet SAS, a Simplified Joint Stock Company, having its head office at 5-9 rue de l'Industrie, 93200 SAINT-DENIS, registered on the Trade Register of Bobigny under Trade Register number 430 359 927.

"Personal data" is any information relating to an identified or identifiable natural person (the data subject); an identifiable person is one who can be identified directly or indirectly , in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, psychological, mental, economic, cultural or social identity.

"Processing of personal data" is any operation or set of correlated operations, which is performed upon Personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

"Processor" is the entity which processes personal data on behalf of the Controller in the frame of a contractual relationship.

"Purpose of processing" is the aim of an application that processes personal data, irrespective of the medium used.

"Sensitive data" is any information concerning racial or ethnic origin, political, philosophical or religious views, health, or sexual orientation.

"Service agreement" is the agreement between an entity of Linkbynet and one of its customers for hosting and/or outsourcing services that implies hosting of Hosted Data by Linkbynet.

"Sub-processor" is the entity of Linkbynet which processes personal data on behalf of the Controller as a processor of the Processor.

"Transfer" is any disclosure of Personal data via a network or any disclosure from one medium to another, irrespective of the type of medium, in so far as such data is intended for processing in the recipient country, other than situations in which the data merely crosses the European Union territory.

3. SCOPE OF THE BINDING CORPORATE RULES

3.1. Geographical scope

The objective of the Binding Corporate rules is to set up an appropriate level of protection on the flow of Personal data from the European Union. The Importer, the Exporter, and the Processor (depending on the case), ought to abide by these internal rules.

These BCR shall apply at minimum to all personal data processed for processor activities on behalf of the Controller and that are submitted to EU.

3.2. Linkbynet's entities concerned by the BCR

These rules will bind all the Linkbynet's entities and any of their employees. The BCR will have a binding effect at:

- the effective date mentioned in article "Effective date" of the BCR, for Linkbynet's entities,
- the signing of their employment contract for any new Linkbynet's employee in accordance with article 9.3.1 of the BCR,
- the signing of a specific agreement for any current Linkbynet's employee at the time of effectiveness of the BCR's in accordance with article 9.3.1 of the BCR.

In case of transfers of data to non-group entities, the Exporter and the Importer shall agree on the terms of this transfer in a separate agreement. The Controller's suppliers that do not belong to Linkbynet and are duly authorized by the Controller to access and process the Personal data; are not concerned by these rules and such processes remain on the sole liability of the Controller.

3.3. Datas concerned by the BCR and purposes

The BCR apply both to Internal data and to Hosted data that are of the following nature:

- Internal data: database of clients, suppliers and employees, human resources, accounting, recordings of video monitoring system,
- Hosted data: might be of any nature, depending on the activity of the Linkbynet's customer and the content it makes hosted by Linkbynet (such as banking data, mailing addresses, database of clients etc.).

Processings of Internal Data within Linkbynet are carried out for the purposes of Linkbynet's activities. Linkbynet's business activities include notably:

- to manage business activities (offers, services, products etc.), sales prospection
- to manage purchases and contracts, approve and validate payments,
- to develop and manage human resources (administration, carreer management, etc.), to manage social partners and personnel delegates..
- to manage the financial aspects of service delivery (assets, financial analysis, tax compliance, etc.)
- Recordings of video monitoring system to ensure security

For Hosted Data, the purposes of the data processing are determined by the Controller and might be for instance: to manage business activities, purchases and contracts, to develop clients and prospects databases etc.

4. DESCRIPTION OF OPERATIONS

The Binding Corporate Rules entail all processed operations that are listed in Appendix C - .

It is aforementioned that all members of Linkbynet and all their employees will access the Hosted data only in the framework of the Service agreement agreed with one of its customer, on request of this customer and for the purpose authorized by it.

In case of Hosted data, LBN warrants that if it cannot provide compliance with the Controller's instructions for whatever reasons, it agrees to inform promptly the Controller of its inability to comply, in which case the Controller is entitled to suspend the transfer of data. The Controller and Linkbynet will meet in order to find an amicable settlement to such difficulty. In case an agreement cannot be found, the Controller will be able to terminate the Service Agreement.

5. OBLIGATIONS OF THE ENTITIES INVOLVED IN THE TRANSFER OF DATA

5.1. As regards the compliance with regulation and BCR

Each Importer and Exporter complies with local regulation as well as the Binding Corporate rules. Binding Corporate Rules will be binding to the Controller through a specific reference to it in the Service Agreement.

In case of Hosted data, the Controller, as stipulated in its Service agreement, ought to inform the Processor of any impact on Linkbynet or Linkbynet's activities due to the nature of the concerned Hosted data or to the Controller's activities.

In case of Hosted data, Linkbynet has a general duty to help and assist the Controller to comply with the law. As such, Linkbynet undertakes:

- To be transparent about sub-processor activities in order to allow the Controller to correctly inform the Data subject ;
- To immediately inform the Controller of any recorded security breach that might impact its Hosted data ;
- To provide to the Controller any information he might need to comply with its legal obligations (e.g., notifications and/or authorizations with DPAs) and/or in case of an audit by a DPA or any other authority ;
- To execute any necessary measures when asked by the Controller, in order to have the data updated, corrected, deleted or anonymised from the moment the identification form is not necessary anymore provided that it has received the request in an appropriate and timely manner.

Being stated that Linkbynet is not a professional as regards data protection law and is not sized to be proactive and/or to analyze and understand specific activities of Controllers, this general duty does not include, in particular, any obligation for Linkbynet:

- To carry out , on behalf of the Controller, the notifications and authorizations the latter shall ask or send to its competent DPA ;
- To give any legal advice, for which it might be held liable ;
- To control the completeness and consistency of information transmitted by Customer to Linkbynet, of the steps taken with any authority, and any other action that rests with the Controller pursuant to applicable law ;
- More generally, to control or investigate how the Controller deals with its Hosted data processings. Linkbynet has no duty to be proactive and/or anticipate such requests.

This general duty does not imply any transfer of responsibility from the Controller to the Processor or the Sub-processor. Except in case of breach of the BCR by Linkbynet, the Controller remains exclusively liable for any non-compliance with the applicable law as regards its Hosted data.

5.2. With regards to data quality and purpose of transfer

The Exporters of personal data guarantee that they have completed the formalities by law with the national jurisdiction for the original processing as regards to the transfer of personal data that is sought. The Exporters of personal data undertake that the processing of Personal data carried out under their control, including data transfers at their initiative, will continue to be carried out in accordance with the provisions of these Binding Corporate Rules and in particular the following:

5.2.1. Quality of Personal data collected

The Exporters must warrant that Personal data which is transferred is

- Collected and processed in a fair and lawful manner as further specified herein
- Collected for specified, explicit and legitimate purposes and not further processed for a purpose that is incompatible.
- Adequate and relevant for the purpose for which they are to be processed.
- Concise, complete and updated where applicable.
- Only stored for a specific period of time as necessary with regards to the purposes of the processing when such data permit identification of the data subjet. Any personal information relating to individuals should only be kept where there is a business or legal need to do so.

According to article 7 of Directive 95/46/EC, 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 (fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data).

5.3. As regards Sensitive Data and automated individual decisions

Subject to compliance with the national provisions made under Community Directive 95/46/EC dated 24 October 1995, Sensitive data may only be processed if:

- the Data Subject has given its explicit consent to the Processing of those Sensitive Data, and such consent is considered as valid pursuant to the applicable law and regulation; or
- the Processing is necessary for the purpose(s) of carrying out the obligations and specific rights of the Data Controller in the field of employment law in so far as it is authorized by applicable law providing for adequate safeguards; or
- the Processing is necessary to protect the vital interests of the Data Subject or of another person where the Data Subject is physically or legally incapable of giving his consent; or
- The Processing is carried out in the course of legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the Processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purpose(s) and that the Personal Data is not disclosed to a third party without the consent of the Data Subjects; or
- The Processing relates to Sensitive Data which has been made public by the Data Subject; or
- The Processing of Sensitive Data is necessary for the establishment, exercise or defence of legal claims; or
- The Processing of the Sensitive Data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those Sensitive Data are processed:
  - by a healthcare professional under applicable laws or rules by national competent bodies to the obligation of professional secrecy, or
  - by another person also subject to an equivalent obligation of secrecy; or
- The Processing is otherwise permitted under the applicable law of the country of establishment of the Data Exporter.

Importer and Exporter warrant that no evaluation of or decision about the Data subject which significantly affects them will be based solely on automated processing of their data unless that decision:

- is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or
- is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests

5.4. Sub-processing

5.4.1. Restrictions on onward transfers to external sub-processors

For Internal and Hosted data, in case of onward transfers to external sub-contractors located outside of the EU Linkbynet commits to ensure that concerned sub-contractors are bound by a written agreement according to Article 16 and 17 of the Directive 95/46/EC and provide sufficient guarantees pursuant to Articles 25 and 26 of the Directive 95/46/EC (eg by using EU Standard Contractual Clauses).

For Hosted Data, Linkbynet undertakes to perform onward transfers to sub-contractors only with prior information to the Controller and its prior written consent.

Where the Service Agreement provides for a general consent, Hosted data may be sub-processed to external sub-processors only with the prior information to the Controller in accordance with Article 13 last paragraph of these BCR. Controller will be entitled to refuse such sub-processing by exercising a veto right (opt-out).

5.4.2. Sub-processing within the group

Hosted data may be sub-processed by other Linkbynet entities only with the prior information to the Controller. Controller will be entitled to refuse sub-processing to a new Linkbynet's affiliate by exercising a veto right (opt-out). Where the Service Agreement provides for a general consent, Linkbynet shall make sure that Article 13 last paragraph of these BCR is complied with.

In case of Hosted data a list of the sub-processors involved in the data processing activities for the Controller is to be made available to the latter upon request.

6. DATA SUBJECTS

6.1. Data subject's rights

The Controller must ensure that individuals are always told in a concise manner about the uses, disclosures and other processing activities performed on their information when such information is obtained unless otherwise stated by law.

Data subject must have access to processed Personal data with regards to them and must be able to request their amendments or deletion. Data subjects have the right to oppose to the processing of relative Personal data on legitimate grounds (notably to oppose direct marketing on request and free of charge).

6.1.1. As regards Internal Data

Data subjects are entitled to enforce any breach of the following BCR principles:

- Purpose limitation (Article 5.2.1)
- Data quality and proportionality (Article 5.2.1)
- Criteria for making the processing legitimate (Article 5.2.1)
- Transparency and easy access to BCR (Article 12)
- Rights of access, rectification, erasure, blocking of data and object to the processing (Article 6.1)
- Rights in case individual automated decisions are taken (Article 5.3)
- Security and confidentiality (Article 8 and 7)
- Restrictions on onward transfers outside of the group of companies (Article 5.4)
- National legislation preventing respect of BCR (Article 5.1)
- Right to complain (Article 9.2)
- Cooperation duties with DPA (Article 11)
- Liability and jurisdiction provisions (Articles 6.2 and 14)

Data subjects' rights shall cover the judicial remedies for any breach of the rights guaranteed and the right to receive compensation for any damage (material harm but also any distress). In accordance with Articles 9.2 and 14, LBN accepts responsibility for any damages resulting from the violation of the BCR by any Linkbynet's entity.

For the application of these rights and in case of a breach by an importer outside the EU, Data subjects might choose to lodge a complaint in front of:

- The jurisdiction of the European Union member state where LBN is established, France ; or
- The competent authority as regards data protection (CNIL).

The process implemented by Linkbynet to ensure theses rights to Data subjects are further detailed in article "9.2Complaint handling".

In any case, amicable settlement ought to be emphasized prior to the matter is referred to the court.

6.1.2. As regards Hosted Data

In case of Hosted Data, Data subjects are entitled to enforce the principles provided by Article 6.1.1 as well as the following principles:

- Duty to respect BCR (Article 3)
- Cooperation with the Controller (Article 5.1)
- List of Linkbynet's entities bound by the BCR (Appendix A)

Data subjects' rights shall cover the judicial remedies for any breach of the rights guaranteed and the right to receive compensation for any damage (material harm but also any distress). In accordance with Articles 9.2 and 14, LBN accepts responsibility for any damages resulting from the violation of the BCR by any Linkbynet's entity.

Data subject might refer their grievances directly to the Controller and to the Data Protection Authority or Courts competent for the data Controller.

If such action is not possible because the Controller has factually disappeared or ceased to exist in law or become insolvent, (unless any successor entity has assumed the entire legal obligations of the Controller by contract of the operation of law, in which case the Data subject can enforce this right against), then the Data subject may take action before Linkbynet or the data protection authority or Courts competent for the Processor (LBN).

If more favorable solutions for the Data subject exist according to national law, then they would be applicable.
In any case, amicable settlement ought to be emphasized prior to the matter is referred to the court.

7. CONFIDENTIALITY WITH REGARDS TO PERSONAL DATA

7.1. For Internal and Hosted Data

Access to Personal data will be granted only to people who have been predefined. The Personal data ought to be used for the initial purpose that it has been agreed for and compatible with a specific way of processing.

For Linkbynet's employees, such access is restricted by the implementation of controlled access, via the use of logins and passwords.

For any person having access to Personal data, personal usage or transmission in any way is prohibited. In case of breach, the employer of the breaching person will be liable towards the other parties involved in the Personal data processing while taking action against its concerned employee if appropriate.

Linkbynet's employees have been informed and alerted on the fact that, in case of non-compliance with this confidentiality obligation, they might be legally pursued, especially on the basis of insider dealing or breach of professional secrecy as the case may be, and might be sentenced to financial sanctions and imprisonment.

7.2. For Hosted Data

In addition to the rules defined in article 7.1 and as also provided in the Service agreement, all members of Linkbynet and their employees shall access Personal data only when it is needed and authorized by Linkbynet's customer. The persons that might have access to Personal data are from the Technical department (technical managers, experts, engineers, administrators) or the Project department (account managers, project managers, project assistants).

On the termination of the Service Agreement, the Processor and Sub-processors shall, at the choice of the Controller, return all the Personal data transferred and the copies thereof to the Controller or shall destroy all the Personal data and certify to the Controller that it has done so, unless legislation imposed upon them prevents it from returning or destroying all or part of the Personal data. In that case, the Processor and the Sub-processors will inform the Controller and warrant that it will guarantee the confidentiality of the Personal data and will not actively process the Personal data anymore.

7.3. Limited right of disclosure

Any legally binding request to Linkbynet for disclosure of the Personal data by a law enforcement authority shall be communicated to the Controller unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.

In any case, the request for disclosure should be put on hold and the DPA competent for the Controller and the lead DPA for the BCR should be clearly informed about it.

8. SECURITY WITH REGARDS TO PERSONAL DATA

Linkbynet has implemented a policy with regards to security of data in order to prevent any unplanned loss, disclosure or destruction as well as misuse. An extract of the Information System security policy is attached in o.

The IT management of changes is ensured through a range of physical, environmental and electronic measures in order to avoid loss, breaches in compliance and deterioration due to fire, power cut or backup.

For Hosted data, all members of Linkbynet and their employees shall respect the instructions regarding security measures as provided for in the Service Agreement.

9. LINKBYNET'S INTERNAL ORGANIZATION TO ENSURE EFFECTIVENESS OF THE BCR

LBN takes the responsibility to perform every necessary step that are required for the set up and effective implementation of the Binding Corporate Rules and of the data protection regulation. For this purpose, LBN commits to put in place the following organization within Linkbynet.

9.1. Data Protection management and follow-up of the BCR

The Linkbynet's parent company, LBN, has the responsibility to apply the BCR for the protection of data within the group of Linkbynet. LBN is governed by the French law and is therefore under the scope of the European Union.

LBN has designated a "Correspondant Informatique et Libertés" (CIL) (data protection officer) for the « Commission Nationale de l'Informatique et des Libertés » (CNIL): he is the Security Manager of Linkbynet's group. Thanks to its duties, the CIL is the guarantor of the respect of the data protection law and of the BCR within Linkbynet and is especially in charge of advising managing officers on this matter. The CIL has been nominated

by the president and the managing director of LBN, ensuring him the full support and trust of the company's board, without effect upon its independence towards management allowing him a total freedom of speech.

The CIL is part of a larger organization implemented in Linkbynet, as described herein:

Management of the data protection is structured to be chaired by a member of high level management, the Security Manager (who is CIL) and the Security group services in a periodical Security committee occurring at least once a year.

The Security committee is composed at least of a chief executive officer, the Security Manager, the Operational director, the technical director and a member of the quality department.

The Security committee is in charge of :

- Incidents review and analysis
- Follow-up and updates of actions plan defined after security audits
- Evolution of Linkbynet's security policy
- Defining global projects relating to security measures

One of the chapters of the committee is dedicated to Personal Data Protection.

The Security committee will designate privacy auditors, who will have the duty to perform periodic checks for compliance in order to ensure that the rules set (all aspects of the BCR) are effectively applied in accordance with the standard compliance check procedure applicable within Linkbynet. Extracts of this procedure are mentioned in Appendix E - .

Such audit might be requested by privacy officers (or any other competent function in the organization) at any time.

The reporting of such compliance check procedure will be directed towards the Security Manager and will be analyzed during a Security Committee meeting. Upon request, Linkbynet will also send this report to the lead DPA. The report will also be sent to the Controller (and to its competent DPA upon request) when its Hosted Data are concerned.

The Security Committee will determine evolutions of process and solutions that must be implemented as regards the conclusion of this report. It will also be in charge of the follow-up of the effective realization of the actions decided.

9.2. Complaint handling

In order to implement one of their rights as mentioned in article 6 or in case of a dispute about any unlawful and/or untimely processing of their personal data, Data subjects are entitled to lodge a complaint with Linkbynet.

These complaints can be addressed by filling an online form accessible on Linkbynet's website (by clicking on the link "Dataprotection") or by calling in person to closest Linkbynet office that will fill the required form on behalf of the Data subject.

When the complaint concerns Hosted Data, Linkbynet has the duty to communicate the claim or request without delay to the Controller without obligation to handle it. When the Controller has disappeared factually or has ceased to exist in law or became insolvent, Linkbynet ought to handle such claim or request.

When Linkbynet handle a complaint, it follows the rules applicable to such complaint handling process as set in an internal procedure. Some extracts of it are stipulated in Appendix F - .

There will usually be a period of investigation of these complaints of a month within their being lodged.

The Quality and Legal departments and the CIL will receive the completed form. One of them will be designated as the exclusive interlocutor of the Data subject. This person ought to be responsible for the identification, recording and listing the complaint. With regards to that, enquiries will be made in the light of alleged complaints.

They may also mediate in order to offer compensation with the prior approval of LBN's board. The interlocutor of the Data subject is bound to be neutral in its activities.

In case of such complaint, the burden of proof rests with the Headquarters based in the EU, LBN, regardless of where the claim originates.

However, this process does not negate the right of the Data subject to have a grievance and lodge a complaint to the lead Data Protection Authority and the competent Court pursuant to Articles 6.1.1 and 6.1.2 of these BCR.

9.3. Applicable terms to Linkbynet's employees

9.3.1. Undertaking to comply with BCR

LBN commits to make any current Linkbynet's employees at the date of effectiveness of the BCR, undertake to comply with the BCR by signing a specific agreement. For this purpose, LBN will prioritize the signature of those employees directly concerned by the processing of Personal data, within a two month-period after the effective date of the BCR. Then, LBN will ensure its signature by any other current Linkbynet's employees within a six-month period after the effective date of the BCR.

Any new Linkbynet's employee (employed after the effective date of the BCR) undertakes to comply with the BCR when signing its employment agreement. Each employee will be given a copy of the BCR and/or the place where it could be found in the internal network of Linkbynet.

At the time of their respective undertaking to comply with the BCR, the employees (current and new ones) will also be given, a résumé of the content of the BCR, consisting of the essential elements as regards data protection and especially the risks for them not to comply with these rules. This synthesis shall be updated freely by LBN as needed.

9.3.2. Disciplinary action

By undertaking to comply with the BCR in accordance with article 9.3.1, employees are informed of their personal risks in case of non-compliance. In addition to legal sanctions as the case may be when provided by law or regulation, employees will be subject to disciplinary sanction implemented by their employer.

Linkbynet's entities may take different disciplinary sanctions on their respective employees, graduated from a simple notification to dismissal, depending on the criticality of their misconduct.

9.4. Data Protection Training

Linkbynet engages to implement training programs with regards to Data Protection of Personal Data, so that any employee shall have followed at least one training session within a six-month period following effectiveness of the BCR. The emphasis will be more on the personnel who have access to Personal Data, IT personnel, security operating center personnel and Human Resources personnel.

An example of a procedure devised for an entity of Linkbynet situated outside the European Union is attached in Appendix G - .

Linkbynet undertakes to perform tests to its employees prior to and after the training session. Results of the tests are then kept in the employee's profile. In case where score are below expectations, training or refresher courses may be provided on a case to case basis.

As further needed, any employee involved in the processing of Personal data or in the development of tools used for such operations, will be provided appropriate training.

10. RIGHT TO AUDIT OF THE CONTROLLER

Any Linkbynet Processor or Sub-processor handling the Hosted Data of a particular Controller will accept, at the request of that Controller to submit their data processing facilities for audit of the processing activities relating to that Controller.

Such audit might occur at reasonable intervals for each Controller and Linkbynet shall prior be informed at least twelve business days before the beginning of the audit. It shall be carried out by the Controller or an inspection body composed of independent members selected by the Controller and where applicable, in agreement with the DPA. Linkbynet might refuse some inspectors if they are direct competitors of Linkbynet.

The auditors shall be in possession of the required professional qualifications bound by a strict duty of confidentiality by signing a specific agreement with Linkbynet in which they will specifically commit to comply with health and safety rules applicable in the audited premises.

The audit shall not interfere with Linkbynet's activity. As such, audit shall only be performed during the working hours corresponding to the auditee's premises and shall not last more than a reasonable period, in consideration of the context of the audit conducted by the Controller.

In any case, the occurrence of an audit shall not entail a risk for the quality or continuity of the services delivered by Linkbynet to its clients. Where the Controller would like to realize more than one audit per year, or the audit last more than fifteen (15) days, the time spent by Linkbynet's team will specifically be invoiced to the Controller.

A report audit shall be written by the auditors. This report (or at least relevant parts of it) shall be communicated to Linkbynet (and to the competent DPA upon request).

11. DATA PROTECTION AUTHORITY

The entities of Linkbynet engage to cooperate with the Data Protection Authorities (either LBN DPA or any Controller's DPA) during any enquiries or audits that the latter might conduct by responding to any requests that the Data Protection Authorities make, in a timely manner. Any Linkbynet's entity specifically undertakes to accept to be audited by the DPA.

The Data Protection Authorities will keep a copy of the Binding Corporate Rules in case of any requirement set by the national law. Entities of Linkbynet will follow the recommendations of these authorities with regards to the Binding Corporate Rules.

By considering the geographical position of LBN, the Data Protection Authority concerned by these BCR shall be the French "Commission Nationale de l'informatique et des Libertés" (CNIL).

12. ACCESS TO BINDING CORPORATE RULES

A read only copy of the Binding Corporate Rules will be available, for the internal staff, in electronic form (i) on Linkbynet's internal network, (ii) on the intranet and/or (iii) on request to the quality department, and will also be on the extranet for access by customers and suppliers. For customers, the corresponding URL of the page in the extranet will be indicated in the Service agreement.

A Data Subject may have access to the BCR by filling a form on the website of Linkbynet. An electronic version of the BCR will then be sent by email.

13. REVIEW OF BINDING CORPORATE RULES

The Security Committee (with the support of the legal and quality departments) will be responsible for the amendment of the Binding Corporate Rules and for keeping track and recording any updates to the BCR. Linkbynet ought to communicate the modifications once a year the information to the lead Data Protection Authority and to all members of Linkbynet. In case of Hosted data the information shall be communicated to the Controller in the same conditions through the extranet.

A list of entities that are bound by the rules is to be kept and maintained up to date by the Security Committee (cf appendix A). Transfers of Personal data to any new entity based outside the European Union and that does not provide an adequate level of data protection is unlawful until the headquarters based in the European Union, Linkbynet, confirms that the new entity is bound by the internal rules. The update list must be communicated to the lead Data Protection Authority.

In case of Hosted data and where a change affects the processing conditions, the information should be given to the Controller in such a timely fashion that the Controller has the possibility to object to the change. The Controller and Linkbynet will meet in order to find an amicable settlement to such objection. In case an agreement cannot be found, the Controller will be able to terminate the Service Agreement before the modification objected is made.

14. DISPUTES, JURISDICTION AND APPLICABLE LAW

14.1. Applicable law and national legislation

The Binding Corporate Rules are subject to French law in all its provisions, which is the European Union member state where LBN is based.

The BCR shall apply unless otherwise stated by the French law and/or a local regulation that shall apply prior to the BCR. Where a local legislation, for instance EU legislation, requires a higher level of protection for personal data it will take precedence over the BCR. In any event data shall be processed in accordance to the applicable law.

In case of Internal data, where there is a conflict between national law and the commitments of the BCR, LBN will decide to implement the appropriate solution and will consult the CNIL in case of doubt.

Where a legislation may prevent Linkbynet from fulfilling the instructions received from the Controller or its obligations under the BCR or Service agreement, it will promptly notify this:

- to the Controller which is entitled to suspend the transfer of Personal data and/or terminate the Service Agreement,
- to LBN and specifically to Linkbynet Privacy Officers and legal department,
- to the DPA competent for the Controller.

14.2. Burden of proof and data protection abilities within Linkbynet

The headquarters (LBN), located in France, have the data protection abilities as well as the sufficient assets to compensate for any damages resulting from breaches of the BCR. It will be in charge of paying said compensation to Data subject no matter which Linkbynet's entity is concerned, and will personally claim for a reimbursement to said entity internally.

The burden of proof for any alleged breach of rules will rest with LBN, (headquarters based in France), regardless of where the claim originates.

14.3. Disputes between Importer, Exporter and/or Sub-processor

In case a dispute occurs between the Importer, the Exporter or a Sub-processor as the case may be, failing amicable settlement, the competent jurisdiction shall be those mentioned in the contract binding the concerned entities.

The headquarters (LBN), located in France, have the delegated data protection abilities as well as the sufficient assets to compensate for any damages resulting from breaches of the BCR.

In case of breach by any Linkbynet's entity to the BCR or to the stipulations of the Service Agreement relating to data protection, the Controller might enforce it against LBN in accordance with Article 14.2.

15. EFFECTIVE DATE

The Binding Corporate Rules takes effect two months from the date of confirmation that the BCR of LBN has been approved.

16. APPENDICES TO THE BCR

The following appendices are added to the BCR as a part of them:

Appendix A - List of Linkbynet's entities bound by the BCR

Appendix B - Roles and position of the entities involved in a data transfer

Appendix C - List of processed operations

Appendix D - Extract of the Information **SYSTEM SECURITY POLICY**

Appendix E - Extracts of standard Compliance check procedure

Appendix F - Extracts of complaint handling procedure

Appendix G - Extracts of training program for Linkbynet Indian Ocean

APPENDIX A - LIST OF LINKBYNET'S ENTITIES BOUND BY THE BCR

This list shall be kept updated in accordance with article A Data Subject may have access to the BCR by filling a form on the website of Linkbynet. An electronic version of the BCR will then be sent by email.

Review of Binding Corporate Rules.

Linkbynet SAS

A Simplified Joint Stock Company (société par actions simplifiées), having its head office at 5-9 rue de l'Industrie, 93200 SAINT-DENIS, France, registered on the Trade Register of Bobigny under Trade Register number 430 359 927 and European VAT number FR 93 430 359 927 000 34.

Linkbynet North America

LIEN PAR LE RESEAU INC, having its head office at 416 boulevard De Maisonneuve Ouest, Montréal, Québec, H3A1L2, registered as a business corporation (Loi sur les sociétés par actions), under the NEQ (Enterprise Quebec number) 1166872839.

Linkbynet Indian Ocean Ltd

It is incorporated as a private company limited by shares, having its head office at 8th Floor, Orbis Court, St Jean Road, Quatre Bornes, Mauritius, is registered on The Companies Act 2001 under register number C07049433.

Linkbynet East Asia Ltd

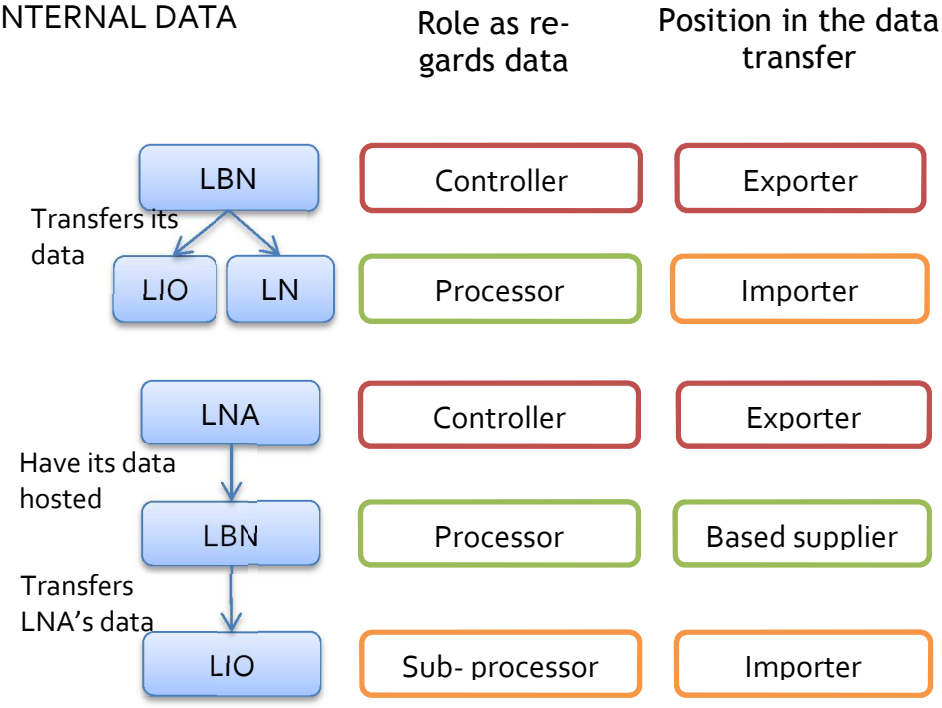
Private company limited by shares, having its head office at 21/F, On Hing Building, 1 On Hing Terrace, Central, Hong-Kong, constituted under « Companies ordinance – Chapter 32 of the laws of Hong-Kong » under certificate n°1993977.

Linkbynet VIETNAM Ltd

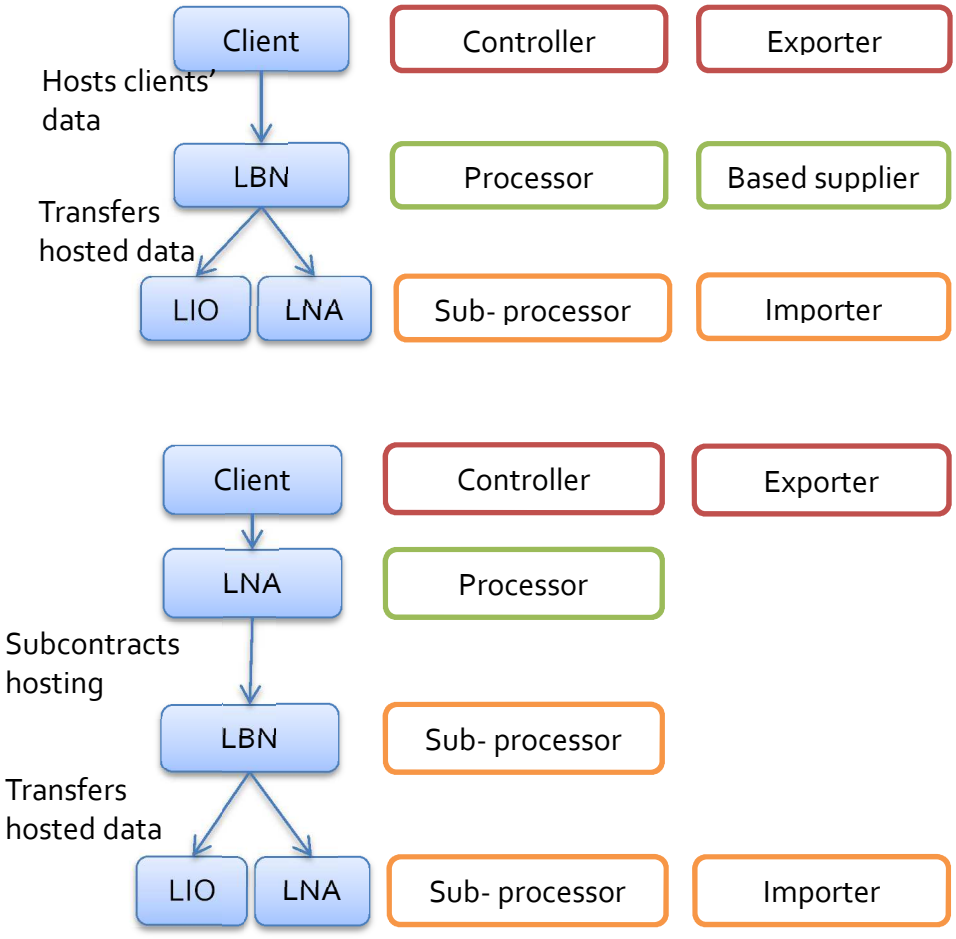
Private company limited constitued under Companies law of Vietnam, having its head office at 3rd floor, N°44 Nguyen Hue street, Ben Nghe Ward, District 1, Ho Chi Minh-Ville registered under number 411043002585 published by Ho Chi Minh City Peoples Committee, Vietnam.

APPENDIX B - ROLES AND POSITION OF THE ENTITIES INVOLVED IN A DATA TRANSFER

FOR INTERNAL DATA



FOR HOSTED DATA



APPENDIX C - LIST OF PROCESSED OPERATIONS

- **Operations on Internal Data:**

Linkbynet's entity being respectively the Controller of its Internal Data, it might process any operation on the said data, provided that it respects applicable regulation especially French "Loi n° 78-17 Informatique et Libertés du 06 janvier 1978".

- **Operations on Hosted Data:**

The Importers participate in the outsourcing and hosting operations for the clients' portfolios of Linkbynet. The role of the Importer is essential as it allows Linkbynet to provide a high level of availability of the hosted environments on a 24h/7d follow the sun model. Below is a description of operations that the transferred data will be subject to only on the Client's request (no operation will be made at Linkbynet's initiative).

Operational requests can be made during opening and non-opening hours. These requests can be in the form of an incident, problem or service request with relations to maintenance updates, account modifications etc. Data is processed on web servers and databases of clients as well as production and preproduction servers. The departments involved are technical ranging from administrators to managers as well as account managers. Transmission of data runs through a secure protocol and backup is ensured by the Transversal activities' team. Upon the client's request, data may be extracted, deleted and/or destroyed. Proofs in the form of certificates are preserved in order to show that the data destruction has respected defined criteria.

Request of all types, as mentioned above, are handled as per the specific process that has been devised for its purpose. The incident, problems and service request processes are based on the Information Technology Infrastructure Library (ITIL) and the ISO 20 000. It ensures that processing is standardized in order to maintain the defined level of effectiveness, efficiency and compliance to security policies.

APPENDIX D - EXTRACT OF THE INFORMATION SYSTEM SECURITY POLICY

The Information System Security Policy defines the security framework and highlights the objectives, obligations and engagement of the Linkbynet group towards its clients and towards its own patrimony. It is based on ISO 27002 – Codes for good practices for security management. The scope of application of the ISSP is therefore as follows:

- All activities carried out by Linkbynet.
- All information systems of Linkbynet
- Every user accessing Linkbynet owned information, regardless of their status or hierarchy.

The ISSP defines the principles in order to protect information be it oral, on paper or electronic and to preserve:

- The confidentiality, which gives the right of information to the persons concerned.
- The integrity, which ensures that the information is not modified or altered
- And the non-repudiation, which guarantees an access or transaction, is given to one identified person.

This encloses the information system (the networks, the computers, the equipment in stock, the software, database, and the means of communication) but also the information exchanged orally, in written form and their physical protection from within or outside LINKBYNET.

The exchange of information among different sites must not compromise the security of data of the company. In order to control the exchange of information, the company must provide tools for sharing with a desired level of security. At the 4 sites of LINKBYNET, the collaborators perform the same task and exchange of necessary information to complete the projects. Different rights setup takes into consideration the site of the collaborator mainly by our internal IS. So, the local message servers, AD and folder server are accessible only to collaborators on the same site. The exchange of information is done by:

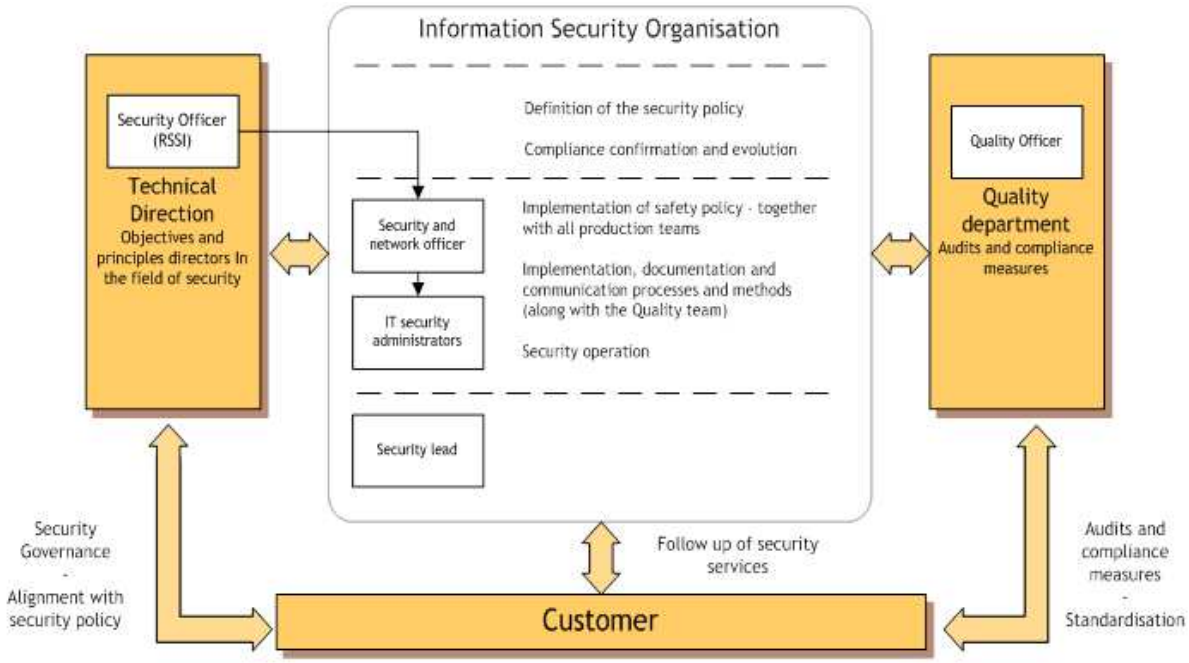
- The intranet for all client project
- Messenger for non-confidential information
- Phone
- Instantaneous messaging accessible to LBN collaborators only.

The same security rules apply to cloud computing as to a physical architecture:

- Access to data
- Segmentation of data and equipment
- Access rights to data
- Transfer of encrypted information
- Isolation of network flow and VM isolation
- Ensuring management of security update.

The security officer forms part of the Management. The different responsibilities regarding security are defined in the organization chart and diagram below:

Organizational Chart:



LINKBYNET must setup a committee responsible for the security of information.

A periodical analysis of security principles related to our activities must be realized. This will allow:

- The examination and validation of security policy
- The follow-up of initiated projects and readjust if necessary
- Start new projects

The technical management, network & security and quality department have a meeting every 3 months to have a global view on items present in the current ISSP and allow necessary actions.

APPENDIX E - EXTRACTS OF STANDARD COMPLIANCE CHECK PROCEDURE

(TRANSLATED FROM FRENCH)

Processes and services are audited at least once a year. This frequency shall also apply to data protection audit. Such audit will be planned by the Quality Department and validated by the Security Committee.

An audit shall be prepared and led by a lead auditor having enough independence as regards the matter audited. This includes that the auditor have not participate:

- To the process management,
- To the realization of the concerned services
- To the organization of the concerned activities.

Data protection audits shall be based on the CNIL's best practices. (http://www.cnil.fr/fileadmin/documents/Guides_pratiques/Livrets/securite/index.html#/10/zoomed)

➢ Audit procedure

The auditor follows the following steps:

- **Interviews of the concerned persons,**
- **Gap analysis : the gaps might be :**
    - Non-compliance that leads to failure to partially or completely achieve the objectives,
    - Elements to be improved in order to limit the risk of non-compliance.

In accordance with European Union Directive 95/46/EC dated 24 October 1995, appropriate technical and organizational measures shall be implemented. The gap analysis above-mentioned will be used to establish an action plan.

➢ Audit report

The auditor will write a report of its audit, based on the key elements that shall be evaluated. Prior to this report, he/she will discuss the following points in the closing meeting.

- Background
- Strengths
- Weaknesses
- Non-compliance
- Improvement recommendations

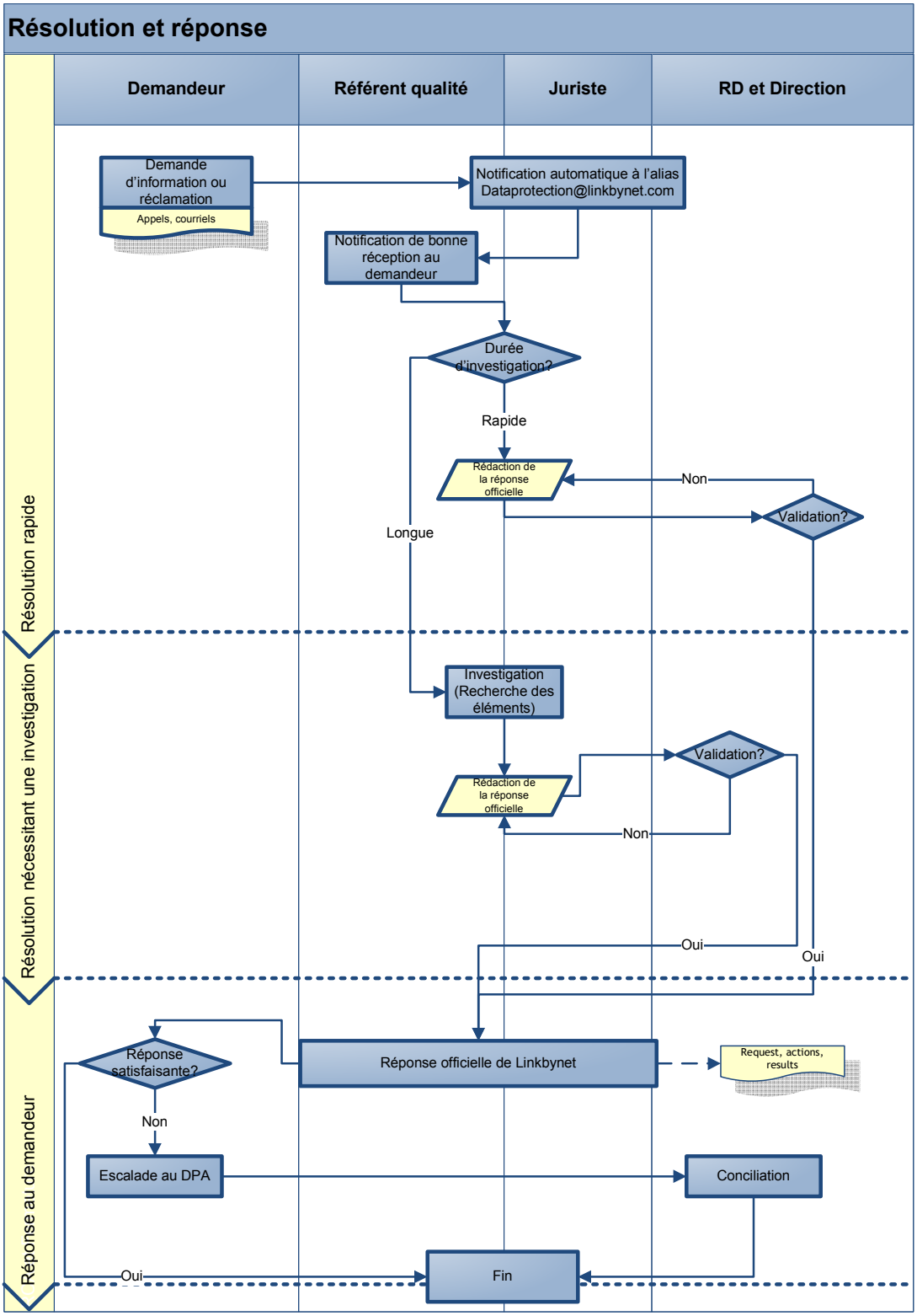
➢ Action plan and follow-up

Based on the report, an action plan is voted stating the deadlines, resources and priorities.
For data protection, the Security Committee will be in charge of the follow-up of the action plan.
The follow-up is documented in the 'Improvement control file'.

APPENDIX F - EXTRACTS OF COMPLAINT HANDLING PROCEDURE

(TRANSLATED FROM FRENCH)

After receiving a request, Linkbynet will qualify it as being a simple or a complex one. The Data subject have the right to ask for it complaint to be dealt as a complex one, without Linkbynet being able to refuse it.



Linkbynet will handle any request (simple or complex) with the same priority level and will make its best efforts to answer the Data subject in the shortest timing. Anyway, investigations might take some time. In order to ensure a trustful and transparent relation, the Linkbynet's interlocutor of the Data subject will keep him informed of the progress of the request's treatment. As such, he will transmit an approximate deadline to the Data subject for which he would have an answer, stating that in accordance with the BCR, being specified that in accordance with the BCR the investigations cannot exceed 1 month after the request has been lodged.

APPENDIX G - EXTRACTS OF TRAINING PROGRAM FOR LINKBYNET INDIAN OCEAN

(TRANSLATED FROM FRENCH)

By training its employees, Linkbynet makes sure that there is no gap between the expected skills' set required for a mission and the effective skills' set that this employee has.

Training might be asked for:

- In the frame of the arrival of a new employee ;
  Steps are defined with this new employee, determining the skills he must acquire to make his training valid.
- Each time a need is identified by the employee's manager.

In Linkbynet Indian Ocean, specific training sessions will be organized as regards security policy and especially data protection.

NB: In LBN and Linkbynet North America, these training will be organized:

- During the integration day for new employees,
- Within six months after the effective date of the BCRs for any current Linkbynet's employees, with an emphasis on the employees who have access to Personal Data, IT personnel, security operating center personnel and Human Resources personnel.

After the training session, the Human Resources Department will organize an evaluation in order to check if the knowledge has been acquired. This evaluation will be similar to the one realized before the training session by the trainees, so that the gap filled can be adequately appreciated.

A regular review will also be implemented by the Quality Department at intervals of four months.