APPENDIX

BINDING CORPORATE RULES (BCR)

LEGRAND GROUP

CONTENTS

1. INTRODUCTION

The subsidiaries of the LEGRAND Group that carry out the personal data processings described in Annex 1 transfer personal data between one another; Some of the subsidiaries are located in countries which do not guarantee a level of protection equivalent to that in the European Union within the meaning of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 ("GDPR").

The LEGRAND Group has therefore drawn up these binding corporate rules ("BCR") so that data transfers made between its different subsidiaries comply with the GDPR.

The Management of LEGRAND FRANCE SA undertakes to ensure that its subsidiaries and employees comply with the rules set forth in these binding corporate rules.

2. DEFINITIONS

The terms used in these binding corporate rules have the same meaning as in the GDPR.

Within the meaning of clauses :

'controller' shall mean the natural or legal person, public authority, agency or 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 such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

'data importer' shall mean the subsidiary of the LEGRAND Group located outside the European Union which receives personal data from the data exporter and which is not subject to the mechanism of a third country ensuring adequate protection within the meaning of the GDPR.

'data protection representatives' or **'field service managers'** are the Group Data Protection Officer's local correspondents, who act as relays, at a local level, for the Group Data Protection Officer. The role of the data protection representatives is specified in the annex "Setting-up of a network of data protection officers" of the binding corporate rules.

'data subject' shall mean the person whose personal data is collected and processed.

'Group Data Protection Officer' is the natural person appointed by name at LEGRAND FRANCE SA who is in charge, at a global level, of handling complaints, monitoring and auditing compliance with the binding corporate rules and, more generally, with the rules on data protection. The role of the Group Data Protection Officer is specified in the annex "Setting-up of a network of data protection officers" of the binding corporate rules.

'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical,

physiological, genetic, mental, economic, cultural or social identity of that natural person.

'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

'processing' shall mean any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

'sensitive data' are personal data subject to Article 9 ("Processing of special categories of personal data") and/or Article 10 ("Processing of personal data relating to criminal convictions and offences") of the GDPR.

'subsidiaries' shall mean the entities linked to the LEGRAND Group legally, whether that entity is a subsidiary as in within the meaning of article L.233-1 of the French Commercial Code (an entity in which LEGRAND owns more than half the capital), or sister company, etc. Any entity that does not transfer personal data in the conditions described in Annex 1shall not be qualified of "subsidiary".

'supervisory authorities' shall mean the authorities within each country of the European Union charged with ensuring compliance with the GDPR.'LEGRAND European headquarters' shall mean the head office of LEGRAND FRANCE SA.

'**data exporter'** shall mean the subsidiary or LEGRAND FRANCE SA located in the European Union which transfers the personal data.

'third party' shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients.

This article reproduces a lot of definition that are in the GDPR.

Perhaps the most important one is "personal data", which means any information relating to an identified or identifiable individual. It should be noted that the definition of personal data goes beyond identification data, such as surname and first name. Indeed, the employer number of an identified individual, although it does not allow directly the identification of the person, is still personal data. The scope of this definition is particularly broad.

Another important word is "processing". A processing means any operation, such as access, copy, deletion, collection, etc. It is therefore, once again, a broad definition.

3. ENFORCEABILITY OF THE BINDING CORPORATE RULES

LEGRAND FRANCE SA and all subsidiaries of the LEGRAND Group that transfer personal data in the conditions stated by Annex 1are bound to comply with these binding corporate rules. Subsidiaries that does not transfer personal data in the condition stated by Article 4 are not parties to this BCR and shall be excluded from the term "subsidiary" in these BCR.

LEGRAND FRANCE SA and its subsidiaries undertake to comply with the binding corporate rules via a unilateral declaration of consent signed by the legal representative of LEGRAND FRANCE SA and of each of the subsidiaries to comply with the binding corporate rules.

LE GRAND FRANCE SA and the subsidiaries of the LEGRAND Group must ensure that their own employees comply with these binding corporate rules.

Regarding the enforceability of the binding corporate rules against employees, the binding corporate rules are appended to the "information system acceptable use policy" which is part of the LEGRAND Group Rules of Procedure.

The binding corporate rules are accordingly enforceable against employees of the LEGRAND Group.

If the employees of the LEGRAND Group do not comply with the binding corporate rules, they may be subject to disciplinary sanctions.

The GDPR sets out rules for the processing of personal data and, among other things, regulates transfers of personal data to countries outside the EU/EEA. Indeed, the philosophy of the GDPR is that the personal data should be protected even when they are transferred outside the field of application of the GDPR. "Transfer" should be understood broadly here, as mere remote access to personal data located in the EU/EEA, from outside the EU/EEA, is a transfer.

One way to make these transfers of personal data comply with the GDPR, when they occur within a group of companies, is to have the exporters and the recipients of the personal data sign a document called "BCR" (Binding Corporate Rules) stating that they will process the personal data in compliance main rules and principles of the GDPR.

This also means that the companies that are parties to these BCR must ensure that their employees will comply with these BCR when they process personal data.

It shall be noted that most of the provisions of these BCR are mandatory under the GDPR.

4. SCOPE

These binding corporate rules are intended to apply to all transfers of personal data made within the Group, to the extent that such transfers are described in Annex 1.

The nature and purpose of the processing concerned, the nature of the data transferred, the purposes of the transfers, the importers and exporters of data within the European Union and outside the European Union, are described in annexes which are an integral part of these binding corporate rules.

These BCR only apply to the transfers of personal data listed in the Annex 1. Moreover, as stated in Article 3, only the subsidiaries that transfer personal data in the conditions described in Annex 1are party to the BCR.

*In consequence, these BCR **do not** apply:*

- to any company that is not a subsidiary of the LEGRAND Group;

- to subsidiaries that do not process personal data as described in Annex 1;

- to any subsidiaries of the LEGRAND Group, where they transfer personal data outside the scope of Annex 1.

5. DATA PROTECTION PRINCIPLES

Personal data must be:

- transferred and processed for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes (purpose limitation);
- transferred and processed lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness, fairness and transparency);
- adequate, relevant and limited to what is necessary to the purposes for which they are transferred and processed (data minimisation);
- accurate and, if needs be, up to date (accuracy);
- transferred and processed for no longer than is necessary for the purposes for which the personal data are processed (storage limitation);
- transferred and processed in a manner that ensures appropriate security of the personal data (integrity and confidentiality).

Above are the main principles of the GDPR.

These principles are as follow:

*- **Purpose limitation**: the principle of limitation of the purpose, as stated in the GDPR, is a 3 in 1.*

First of all, the purpose of the processing must be specified, which means that the purpose of every processing must be determined and expressly defined prior to the collection of personal data. No personal data can be collected if there is no defined purpose; no personal data can be collected "just in case". Moreover, personal data cannot be processed in a way incompatible with the purpose for which they were originally collected.

Secondly, the purpose of the processing (marketing, HR, accountability, etc.) must be explicit, which means that it must be brought to the attention of the data subject (the person whose personal data is processed), for instance through a privacy policy.

Finally, the purpose of the processing must be legitimate, which means that the purpose of the processing must be legal and shall not be too invasive of privacy.

*- **Lawfulness, fairness and transparency**: the processing of personal data must comply with the applicable law, and must be fair and transparent for the data subject, which means that the data subject must be informed of the processing, and his/her personal data shall not be processed in a manner he/she does not expect.*

The GDPR prohibits unlawful processing. For instance, an employee cannot be recorded by video on a continuous basis by its employer, unless its function requires it, as this processing would infringe the employee's right to privacy.

*- **Data minimisation**: only the personal data that is useful for the processing shall be processed. If a personal data is not useful, it shall not be processed. If a personal data is useful for the processing but not essential, the data subject shall have the choice to provide the personal data or to refuse.*

*- **Accuracy**: when informed of a personal data that is incorrect or not up to date, the LEGRAND entity processing the personal data shall correct, update (or, where applicable, delete) the personal data.*

*- **Storage limitation**: Data shall be stored for a limited period, first in "active base", then in archive. The personal data shall be stored in active base only for the duration of the processing. Once the personal data is no longer useful for the processing, it shall be deleted or archived.*

Once the "active base" duration is expired, the personal data can be archived if they are useful for the concerned subsidiary, for instance in order to comply with a legal requirement, in order to take a legal action or to defend itself in court.

These durations shall be determined in advance.

*- **Integrity and confidentiality**: The personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.*

The personal data must also be protected against breach of confidentiality committed by the subsidiaries staff or by third parties.

6. LEGAL BASIS FOR PROCESSING PERSONAL DATA

All processing of personal data must meet at least one of the following conditions:

- 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;
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- 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;
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
- the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

All personal data processing must rely on at least one of the above legal basis.

Regarding staff personal data, most of the time, the processing of this kind of data can rely on the performance of the contract between the employee and the concerned subsidiary, as long as the processing is needed for the performance of the contract. For instance, this is the case regarding the processing of the personal data for e-mail exchanges for work purposes.

Otherwise, if the processing of personal data of an employee is not necessary for the performance of the employment contract, the processing could rely on the legitimate interest of the employer. This, for instance, is the case where the personal data of the employee is processed for the purpose of optional internal communication.

7. LEGAL BASIS FOR PROCESSING SPECIAL CATEGORIES OF PERSONAL DATA

All processing of special categories of personal data is prohibited with the exception of cases where:

- the data subject has given his/her explicit consent to the processing of the special categories of personal data, except in cases where the legislation prohibits it, or

- processing is necessary for the purposes of complying with the obligations and specific rights of the controller in the field of employment law and social protection law in so far as it is authorized by EU or national law or a collective agreement pursuant national law providing for adequate safeguards for the fundamental rights and the interests of the data subjects, or

- 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/her consent, or

- processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects, or

- processing relates to special categories of personal data which are manifestly made public by the data subject in question, or

- processing of the special categories of personal data is necessary for the establishment, exercise or defence of legal claims, or

- processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject, or

- processing of the special categories of personal data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, to the extent that the said data are processed by a health professional subject, under EU or national law or rules established by national competent bodies, to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy, or

- processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy, or

- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the GDPR, based on EU or national law, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

The GDPR prohibit the processing of "special categories of personal data": personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

These special categories of personal data can however be processed when one or more of the above conditions is met.

For instance, a subsidiary can process information regarding the union membership of its employees if the processing is necessary for the purposes of complying with its obligations in the field of employment law or social protection law.

8. TRANSPARENCY AND RIGHT TO INFORMATION

The binding corporate rules will be published on the LEGRAND Group intranet and each Data subject may request a copy of them, at no cost.

Data subjects are informed by a notice published on the LEGRAND Group intranet prior to the processing and transfer of their personal data:

- of the identity of the controller;
- of the contact details of the data protection representatives and of the Group Data protection officer;
- of the purposes of the processing for which the data are intended and the legal basis for the processing;
- of the legitimate interest pursued, when the processing is based on the legitimate interests;
- of the existence of a right of access, correction, limitation, opposition and removal of the data relating to them as well as the contact details of the department competent to receive their requests;
- of the right to lodge a complaint with the supervisory authority;
- of the period for which the personal data will be stored, or the criteria used to determine that period;
- of the nature of the data transferred outside the European Union;
- of the purposes of the transfer of their data outside the European Union;
- of the recipients or categories of recipients of their data;
- of the existence of binding corporate rules ensuring a level of protection of the transfers made to subsidiaries outside the European Union.

Where the personal data are gathered through indirect collection, the Data subjects must also be informed of the source of the personal data and whether the personal data came from publicly accessible sources.

Each Data subject will be informed of the publication of the information notice on the LEGRAND Group intranet.

The external providers who are Data subjects have access to the LEGRAND Group intranet where the information notice on the BCR and the binding corporate rules are published and may request a copy of them, at no cost.

The external providers who are data subjects are also informed about the binding corporate rules through the “Liability commitment of suppliers”, which is a document that each legal representative of external provider has to sign. In this document, the legal representative of external provider undertakes that prior to the start of the service, he will provide each of his employees involved in the execution of the service at LEGRAND Group (external providers who are Data subjects) with the

BCR, and the notice of information of the BCR, which are annexed to the document "Liability commitment of suppliers". He will also inform them that they can have access on the LEGRAND Group intranet, where they can exercise their rights, to the BCR and to the notice of information of the BCR.

Where there is a processing of personal data, there is also a requirement to inform the data subjects of the main characteristics of this processing (purpose, retention period, rights of the data subjects, etc.).

This information can be delivered through a privacy policy on a website (or, more specifically, regarding employees, on the intranet).

9. RIGHTS OF THE DATA SUBJECT

The LEGRAND Group undertakes that:

- any data subject has the right to obtain a copy of all the data processed concerning him/her, without restriction, at reasonable intervals and within a reasonable time frame and without excessive costs;
- all data subjects have the right to obtain correction, removal or the blocking of data, in particular on the grounds that such data are incomplete or incorrect;
- any data subject has the right to object at any time on compelling legitimate grounds relating to his/her particular situation, to the processing of data relating to him/her, save where otherwise provided by national legislation. If the objection is justified, processing must be stopped;
- any data subject has the right to object to the processing of data relating to him/her for purposes of direct marketing, on simple request and at no cost;
- any data subject has the right to restrict the processing of data relating to him/her, where the conditions for such restrictions apply;
- any data subject has the right to receive the personal data concerning him/her which he/she has provide to he LEGRAND Group, where the processing (i) is based on consent or on a contract and (ii) is carried out by automated means

Data subjects are informed by means of a publication on the LEGRAND Group intranet, prior to any processing and transfer of their data, of the contact details of the competent department charged with responding to their requests for access rights.

The competent department to deal with requests for access rights is the data protection representative (also known as DPR) competent at local level.

The procedure put in place by the LEGRAND Group for enabling data subjects to lay complaints that a subsidiary of the group is not complying with the binding corporate rules is described in the annex "Complaints handling procedure" of the binding corporate rules.

Data subjects have the right to lodge a complaint, either (i) before the supervisory authority of their place of work, of their habitual place of residence or of the place where the alleged breach would have occurred or (ii) before the competent jurisdiction of the member state of the European Union in which the data exporter has an establishment or where the data subject has his/her habitual place of residence.

The GDPR grants rights to the data subjects. The mains rights are the followings:

- the right to rectify inaccurate personal data concerning him/her or to complete incomplete personal data;

- in certain circumstances (such as when the personal data is no longer necessary for the entity processing it), the right to erase the personal data concerning him/her;

- the right to object to processing of personal data concerning him/her, for instance where the personal data are used for direct marketing purposes;

- the right to obtain a copy of their personal data, so long as the deliverance of this copy does not affect the rights and freedom of others.

The data controller has a maximum of one month (three months for a "complex" request) from the date of receipt of the request to proceed to the request

10. AUTOMATED INDIVIDUAL DECISIONS

The LEGRAND Group undertakes that no appraisal or decision relating to the data subject of a nature to impact on him/her significantly will be based solely on the automated processing of his/her data except if the decision in question:

- is taken with a view to 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/her legitimate interests, such as arrangements allowing him/her to put his/her point of view, or
- is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

11. SECURITY AND CONFIDENTIALITY

The LEGRAND Group undertakes to 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.

These measures must provide a level of security adapted to the risks connected with processing and with the nature of the data to be protected, having regard to the level of technology and the cost of implementation.

Enhanced security measures will be applied in the case of processing sensitive data.

The measures taken by the LEGRAND Group to ensure security and confidentiality are described in the annex "security and confidentiality policy" of the binding corporate rules.

Pursuant to the GDPR, the LEGRAND Group shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

In doing so, the LEGRAND Group must take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor.

The security measures are listed in Annex 5 of these BCR. The employees can also consult the document entitled "Legrand Information Security Policy" ("LISP") which is the shared cybersecurity framework within the Group.

12. RELATIONS WITH PROCESSORS

Where the data are transferred to a processor (whether this processor is a subsidiary or not) the Group controller must choose a processor providing sufficient guarantees in terms of the technical security measures and organizational measures governing the processing to be carried out, and must ensure those measures are complied with.

A contract will be entered into with the processor by which the processor must undertake to act only on the instructions of the Group controller in question and that obligations in terms of security and confidentiality of the data are incumbent on the processor. This contract must also include all the other mandatory information listed by Article 28 paragraph 3 of the GDPR.

A processor is an entity processing personal data on behalf of the data controller, for instance by providing services such as data hosting, maintenance, payroll management, etc.

***1.** When engaging a data processor, a LEGRAND subsidiary must always first ensure that this data processor provides "sufficient guarantees".*

The guarantees "provided" by the processor are those that the processor is able to demonstrate to the satisfaction of the LEGRAND subsidiary, as those are the only ones that can effectively be taken into account by the LEGRAND subsidiary when assessing compliance with its obligations. Often this will require an exchange of relevant documentation (e.g. privacy policy, terms of service, record of processing activities, records management policy, information security policy, reports of external data protection audits, recognised international certifications, like ISO 27000 series).

The LEGRAND subsidiary's assessment of whether the guarantees are sufficient is a form of risk assessment, which will greatly depend on the type of processing entrusted to the processor and needs to be made on a case-by-case basis, taking into account the nature, scope, context and purposes of processing as well as the risks for the rights and freedoms of natural persons.

The following elements should be taken into account by the LEGRAND subsidiary in order to assess the sufficiency of the guarantees: the processor's expert knowledge (e.g. technical expertise with regard to security measures and data breaches); the processor's reliability; the processor's resources. The reputation of the processor on the market may also be a relevant factor for controllers to consider.

***2.** When engaging a data processor, the GDPR requires that an agreement is signed between the processor and the concerned LEGRAND subsidiary. This agreement must include mandatory*

information, such as a description of the processing, or a statement that the processor will only process the personal data according to the "documented instruction" of the controller.

13. RESTRICTIONS ON TRANSFERS TO EXTERNAL CONTROLLERS OR PROCESSORS

The LEGRAND Group undertakes to restrict transfers outside the Group.

If data are transferred to entities not belonging to the Group, the LEGRAND Group undertakes that:

- External processors established in the European Union or in a country recognised by the European Commission as guaranteeing an adequate level of protection will be bound by a written contract specifying that the processor acts only on the sole instructions of the controller and is responsible for implementing adequate security and confidentiality measures;
- All transfers of data to external controllers established outside the European Union are compliant with the European rules on the transfers of personal data, in accordance with articles 44 and seq. of the GDPR;
- All transfers of data to external processors established outside the European Union must abide by the rules relating to processors (article 28 of the GDPR) in addition to the rules on the cross-border flows of data (articles 44 and seq. of the GDPR).

When personal data are transferred outside the EU/EEA, the expedient of the personal data must ensure that the transfer complies with articles 44 and seq. of the GDPR.

It means that the expedient and the recipient shall, for instance, sign "standard contractual clauses" that will requires the recipients to process the personal data in compliance with the European standard, similarly to these BCR.

Implementing the measures listed by articles 44 and seq. is not necessary where the personal data are transferred to a country that has been recognized by the EU Commission as "guaranteeing an adequate level of protection". It is also not necessary for transfers of personal data to LEGRAND subsidiaries where such transfers are already covered by these BCR (see Annex 1).

14. TRAINING PROGRAMME

The LEGRAND Group undertakes to put an appropriate mechanism in place to enable adequate training on personal data protection to be delivered:

- To the data protection representatives;
- To personnel of each subsidiary who have permanent or regular access to personal data;
- To personnel in charge of developing tools for processing personal data.

Information tools enabling personnel in the LEGRAND Group to be made aware of the binding corporate rules are accessible on the intranet.

The procedure put in place by the LEGRAND Group for training programme is described in the annex "training programme" of the binding corporate rules.

In order to comply with the requirements of the GDPR and/or these BCR, it is crucial that the LEGRAND subsidiaries train their personnel.

Indeed, these BCR won't be fully enforced unless the personnel in charge of processing of personal data is familiar with the rules set out in these BCR. The training can be on-site, distance training, e-learning, etc. It can be done by third party, at the group level and followed-up by the subsidiary itself.

15. AUDIT PROGRAMME

The LEGRAND Group undertakes to conduct compliance audits on the binding corporate rules within the Group and more particularly:

- to audit all aspects covered by these binding corporate rules, including the methods intended to ensure that corrective measures will be implemented;
- that these audits are carried out regularly by LEGRAND Group internal auditors or at the express request of the Group Data Protection Officer;
- that the results of all audits are forwarded to the Group Data Protection Officer as well as to the Group Chief Information Officer of LEGRAND FRANCE SA;
- that the supervisory authorities may receive a copy of these audits, on request;
- that the audit schedule enables the supervisory authorities to conduct audits themselves on data protection, if needs be;
- that each of the subsidiaries in the group agrees to undergo the audits carried out by the LEGRAND Group internal auditors or by the Supervisory authorities and undertakes to follow their advice on everything that relates to these rules.

The procedure put in place by the LEGRAND Group for conducting compliance audits is described in the annex "Audit procedure" of the binding corporate rules.

In order for the BCR to be fully enforced, and to improve the level of compliance by identifying the gaps, the GDPR requires audits to be conducted on a regular basis.

16. COMPLIANCE WITH THE RULES AND AUDIT OF THEIR APPLICATION

The LEGRAND Group undertakes to appoint the appropriate personnel to guarantee and monitor compliance with these rules.

The Group Data Protection Officer is thus assisted by data protection representatives.

The Group Data Protection Officer has an advisory role with regard to the Group Chief Information Officer at LEGRAND FRANCE SA, processes requests from the supervisory authorities, draws up annual reports on compliance with the rules and ensures the rules are complied with at global level.

The field service managers (data protection representatives) are charged with processing complaints originating from data subjects, submitting reports on important questions linked to data protection to the Group Data Protection Officer and with ensuring the rules are complied with at local level.

The roles of the Group Data Protection Officer and the data protection representatives are specified in the annex "Setting-up of a network of data protection officers" of the binding corporate rules.

In some circumstances, the GDPR requires to appoint a data protection officer (DPO), who can act for the whole group of companies and have representatives within the subsidiaries.

The DPO (at the Group level) and the representatives (at the local level) are responsible for implementing compliance with the European Data Protection Regulation within the organisation that has appointed him/her, for all processing operations carried out by that organisation.

17. ACTION IN THE CASE WHERE NATIONAL LEGISLATION HINDERS COMPLIANCE WITH THE BINDING CORPORATE RULES

Where a subsidiary of the LEGRAND Group has reason to believe that the legislation applying to it is likely to prevent the company from fulfilling its obligations under the binding corporate rules and to have a negative impact on the safeguards provided by this BCR, the said subsidiary will immediately inform the Group Data Protection Officer thereof (unless that is prohibited by a law enforcement authority charged with ensuring compliance with the law).

In the event of conflict between the national legislation and the undertakings by virtue of the rules, the data protection representative competent at local level will take a responsible decision on the action to undertake and, in case of doubt, will consult the Group Data Protection Officer.

The Group Data Protection Officer may, where appropriate, consult the Group Legal Department and report the situation to the competent supervisory authorities.

The report to the supervisory authorities must include, where applicable, the categories of personal data requested, the entity requesting the personal data, and the legal ground for the disclosure of the personal data. This information shall not be reported to the supervisory authorities where legal provisions (such as the obligation to keep the secret of investigations) forbid such report.

Ultimately, if the local legislation and or practices impinge on the effectiveness of the binding corporate rules, the Group Data Protection Officer may decide (i) to implement "*supplementary measures*" (as defined in the Schrems II decision of the Court of Justice of the European Union) necessary to bring the level of protection of the data transferred up to the EU standard, or (ii) to suspend the transfer.

The BCR is not always enough to have the personal data transfer comply with the GDPR. The GDPR also requires the data exporter to assess whether the domestic law and practices of the country of destination hinders compliance with the BCR.

Indeed, if the national law does not allow the data importer to comply with the BCR, the purpose of the BCR, which is to ensure the data is processed by the recipient in compliance with the main rules and principles of the GDPR, is nullified. If it is established that the domestic law of the country of destination hinders compliance with the BCR , "additional measures" need to be implemented. The purpose of these additional measures is to restore compliance with the BCR. These measures can, depending on the circumstances, be of technical, organizational or contractual nature

18. INTERNAL COMPLAINT MECHANISMS

The LEGRAND Group undertakes to instigate an internal complaint handling system in the context of which any data subject must be able to lay a complaint that a subsidiary of the group is not complying with the rules.

Complaints are dealt with at local level by the field service managers who forward them to the Group Data Protection Officer where they are founded.

The procedure put in place by LEGRAND Group for enabling data subjects to lay complaints that a subsidiary of the group is not complying with the binding corporate rules is described in the annex "Complaints handling procedure" of the binding corporate rules.

The purpose of this internal complaint mechanism is to ensure that each subsidiary complies with the GDPR.

19. RIGHTS OF THIRD-PARTY BENEFICIARIES

The binding corporate rules grant data subjects the right to enforce the following binding corporate rules principles before the appropriate supervisory authority or court in order to seek remedy and obtain compensation if a member of the group has not met the obligations and does not respect those principles, among which:

- the data protection principles (article 5 of these binding corporate rules);
- the lawfulness of the processing (article 6 of these binding corporate rules);
- the right to transparency and accessibility of the binding corporate rules (article 8 of these binding corporate rules);
- the rights of access, correction, erasure, opposition, restriction and portability of the data; the right to lodge a complaint with the competent supervisory authority (article 9 of these binding corporate rules);
- the rights to object automated individual decisions (article 10 of these binding corporate rules);
- the right to security and confidentiality of the data (articles 5 and 11 of these binding corporate rules);

- the restriction on subsequent transfers outside the Group (article 13 of these binding corporate rules);
- the actions required in case a national legislation hinders compliance with the binding corporate rules (article 17 of these binding corporate rules);
- the right to lay a complaint through the intermediary of the companies' internal complaints mechanism (article 18 of these binding corporate rules);
- the obligation for LEGRAND Group will comply with its duty to cooperate with the supervisory authorities (article 21 of these binding corporate rules).

The data subject registers a complaint at local level with the competent local data protection representative who forwards it to the Group Data Protection Officer.

This complaint will follow the complaints handling procedure.

The data subject may choose to enforce the above-mentioned principles before:

- the jurisdiction of the data exporter established in the European Union or of the place of work of the data subject or of the alleged infringement, or
- the jurisdiction of LEGRAND FRANCE SA or the jurisdiction of the usual place of residence of the data subject,
- or of the competent supervisory authority.

The data subject choosing to enforce these above-mentioned principles before a jurisdiction has the right to obtain compensation for the damage and, where applicable, to receive and indemnification in case of breach of one or more of the above-mentioned principles.

It is mandatory for the BCR to confer to the data subjects the ability to enforce the rights listed in this article. Once again, the purpose here is to give the BCR enforceability.

20. LIABILITY

LEGRAND FRANCE SA agrees to accept liability for and to take the measures necessary to redress acts committed by other subsidiaries in the Group established outside the European Union and to pay compensation for any proven harm arising from a violation of the binding corporate rules by the subsidiaries.

It falls to LEGRAND FRANCE SA to prove that the subsidiary established outside the European Union is not liable for the violation which led to the claim for redress.

If LEGRAND FRANCE SA is able to prove that the subsidiary established outside the European Union is not liable for the violation, the former's liability will not be incurred.

The BCR must explain the mechanism used to determine the liability when a subsidiary outside the EU breaches the GDPR or the BCR. LEGRAND FRANCE SA bears a large part of the liability, due to its role in the choice of the transfer tools.

21. MUTUAL ASSISTANCE AND COOPERATION WITH THE SUPERVISORY AUTHORITIES

The LEGRAND Group undertakes that the subsidiaries will cooperate and assist one another in the management of claims or complaints from individuals, or of inquiries or requests for information originating from the supervisory authorities.

LEGRAND FRANCE SA undertakes that the subsidiaries will apply the advice of the supervisory authorities on the interpretation of the binding corporate rules.

The subsidiaries must always cooperate with the supervisory authorities.

The supervisory authorities are the EU authorities in charge of personal data protection (for instance, in France, the CNIL or, in Belgium, the APD). Cooperation with these authorities is mandatory.

22. UPDATING THE RULES

The LEGRAND Group undertakes to forward to all subsidiaries in the Group and to the supervisory authorities any significant modification made to the binding corporate rules or the list of subsidiaries, aiming to take in account changes in the regulatory environment or in the company's structure, via the intranet.

Updates to the binding corporate rules or list of subsidiaries subject to the binding corporate rules are possible without it being necessary to file a new request for authorisation, provided the following conditions are met:

- the Group Data Protection Officer updates the list of subsidiaries subject to the binding corporate rules, records and consigns any updates to the rules and supplies the information required to the data subjects or supervisory authorities, at their request;
- no transfer is made to a new subsidiary so long as it is not genuinely bound by the binding corporate rules and so long as it is not in a position to ensure they are complied with;
- any modification to the rules or to the list of subsidiaries, accompanied by a short statement of the grounds justifying this update, must be once a year notified to the supervisory authorities issuing the authorisations.

Any substantial modification to the binding corporate rules will also be disclosed to the data subjects.

These BCR can be modified (for instance, in case of change of the characteristics of the transfers of personal data, or in case of change of the applicable legislation/regulation) but it is mandatory, under the GDPR, to report changes without undue delay to all LEGRAND subsidiaries and to the relevant supervisory authorities.

23. LINKS BETWEEN THE NATIONAL LEGISLATION AND THE BINDING CORPORATE RULES

Where the local legislation, for instance European Union legislation, requires a higher level of protection for personal data, it will take precedence over the binding corporate rules.

In all cases, the data will be processed in accordance with the relevant local legislation.

The philosophy behind this article is that in case of conflict between the provisions of these BCR and those of an applicable legislation, the text providing the higher level of personal data protection shall prevail.

24. FINAL PROVISIONS

The binding corporate rules come into effect on 31 / 05 / 2015

The binding corporate rules were last updated on XX / XX / XXXX

25. ANNEXES

Annex 1: Details of transfers and nature of the data transferred

Annex 2: List of Legrand Group companies affected by the binding corporate rules

Annex 3: Complaints handling procedure

Annex 4: Setting-up of a network of data protection officers

Annex 5: Security and confidentiality policy

Annex 6: Audit procedure

Annex 7: Training programme

Annex 8: Information system acceptable use policy.

ANNEX 1

DETAILS OF TRANSFERS AND NATURE OF THE DATA TRANSFERRED

LEGRAND GROUP

Data transfers outside the European Union liable to be made within the LEGRAND Group concern two principal stages of processing

1.1 Initial processing requiring transfer: internal directory

Purpose of the principal processing

The purpose of the processing is to create an internal directory of the LEGRAND Group.

The internal directory is made up of three systems:

- White Pages (WP) and Active Directory (AD)
- Lotus Notes (LN)
- Microsoft Office 365
- IT Department call duties

Processing has several additional purposes:

- To provide employees of the Legrand Group with employees' business contact numbers and details;
- To centralise authorisations for applications and technical infrastructure equipment (servers, networks);
- To provide the contact numbers (business and personal phone numbers) of persons on call duty in the IT Department.

Purpose of the transfers

The first purpose of the transfer is to enable all the particulars contained in the directory to be read from all the computer stations (fixed and mobile) deployed in the Group.

The objective of the transfer is also to enable automatic replication of the directory on the Group's servers (approx. 90 servers).

For the IT Department on-call duties, the purpose of the transfer is to enable employees with access to the Group's information systems, limited read-only access to particulars relating to people on call duty in the IT Department.

Nature of the data transferred

Last name, First name, job title, direct manager, department, employee no., telephone numbers, contact details of assistant(s) and direct manager, e-mail address(es), postal address(es), identity photo, professional competencies and experience, centres of interest.

Particular categories of data transferred (where applicable)

None

Data subjects

Personal data transferred relate to the following categories of data subjects:

All employees of the Legrand Group and its subsidiaries as well as certain providers under contract to Legrand (with confidentiality undertaking and access to the internal network).

For the IT Department call duties, restricted list of Legrand employees and external providers on call duty.

1.2 Secondary processing requiring transfer: talent management

Purpose of the principal processing

The purpose of the processing is to enable career management of the "talents" identified within the LEGRAND Group.

Purpose of the transfers

The purpose of the transfer is to enable exchanges within the LEGRAND Group of information on LEGRAND Group employees identified as "talents" and on their career.

The recipients of the data are human resources departments, managers and employees themselves of all LEGRAND Group subsidiaries.

Nature of the data transferred

The data transferred relates to identification, career and mobility management:

- pay, CV, job description, objectives, skills assessment, development action plans, mobility and promotion plans, training plans, comments regarding the annual reviews of the employee, direct manager and HR manager.

Particular categories of data transferred (where applicable)

None

Data subjects

Personal data transferred relate to all Group employees.

ANNEX 2

LIST OF LEGRAND GROUP COMPANIES AFFECTED BY THE BINDING CORPORATE RULES

LEGRAND GROUP

List of Legrand Group companies affected by the binding corporate rules. All new subsidiaries in accordance with article L233-3 of the French Commercial Code falling within the scope of the Legrand Group shall be added to this list.

ANNEX 3

COMPLAINTS HANDLING PROCEDURE

LEGRAND GROUP

The LEGRAND Group has put in place a procedure for handling complaints from data subjects where they consider that a subsidiary of the Group is not complying with the binding corporate rules.

Complaints are handled at local level by the competent data protection representative.

Complaints must be handled without undue delay and, at any rate, within one month of receipt of the request. Considering the complexity of the complaint and the number of requests, this period may be extended by two further months where necessary, taking into account the complexity and number of the complaints.

Accordingly, the data subjects should refer their complaint, by e-mail, to the competent data protection representative whose contact details are shown on the list of data protection representatives accessible on the Group's intranet site.

The data protection representative has a period of 15 days to handle the complaint. If, due to the complexity of the complaint and the number of requests, the data protection representative deems it necessary to extend the response period (by two months maximum), the data protection representative shall seek the Group Data Protection Officer before extending the period.

The data protection representative makes all the verifications necessary to ensure that the complaint is founded.

If the complaint is not founded, he/she informs the Data subject, explaining the reasons why the complaint is unfounded and that they have the possibility of addressing an appeal to the Group Data Protection Officer.

Where he/she considers the complaint is founded, he/she forwards it to the Group Data Protection Officer who will carry out the necessary verifications. The Group Data Protection Officer has a period of 15 days to investigate the complaint.

If the Group Data Protection Officer considers there are grounds for the complaint, he/she puts the subsidiary in question on notice to implement a corrective action plan, and determines if the complaint deserves payment of compensation to the Data subject. If such is the case, LEGRAND FRANCE SA undertakes to compensate the Data subject for any harm arising from the binding corporate rules being thus violated.

If the Data subject is not satisfied with the response given by the Group Data Protection Officer, they have the option of appealing to the Group General Management.

The Data subject may choose to bring a complaint before:

- The jurisdiction of the data exporter established in the European Union or of the place of work of the data subject or of the alleged infringement, or
- the jurisdiction of LEGRAND FRANCE SA or the jurisdiction of the usual place of residence of the data subject, or

- the competent data protection authority.

ANNEX 4
SETTING-UP OF A NETWORK OF DATA PROTECTION OFFICERS

LEGRAND GROUP

The LEGRAND Group has put in place a network of data protection officers in charge of handling complaints, monitoring and auditing compliance with the binding corporate rules and, more generally, with the rules on data protection.

A Group Data Protection Officer has been appointed at LEGRAND's European headquarters .

Data protection representatives have been appointed by area or country. They act as relays for the Group Data Protection Officer.

The role of the Group Data Protection Officer is to advise the Group Chief Information Officer, process requests from the data protection authorities, draw up annual reports on compliance with the rules and to ensure the rules are complied with at global level.

Documents for training personnel having access to the data-processing that is the subject of the binding corporate rules will be prepared by the Group Data Protection Officer.

The Group Data Protection Officer is also tasked with updating the list of subsidiaries, recording and consigning any updates to the binding corporate rules and with supplying the information required to the data subjects or data protection authorities, at their request.

The Group Data Protection Officer is bound to notify the data protection authorities charged with issuing authorisations, of any substantial modification to the binding corporate rules or to the list of subsidiaries, once a year, accompanied by a short statement of the grounds justifying this update.

The Group Data Protection Officer will be the recipient of all reports on audits carried out by the internal auditors and of all complaints made by data subjects on the implementation of the binding corporate rules which the data protection representatives will have deemed justified.

The Group Data Protection Officer may also request a data protection representative to carry out an audit for a particular given subsidiary.

The Group Data Protection Officer is also informed by the subsidiaries where the latter have reason to believe that the legislation applying to them is likely to prevent their fulfilling their obligations under the binding corporate rules.

The Group Data Protection Officer will take a responsible decision on the action to undertake.

The Group Data Protection Officer may, where appropriate, consult the Group Legal Department and the competent data protection authorities.

The data protection representatives are tasked with handling requests for access rights from the data subjects as well as the complaints originating from the data subjects.

The data protection representatives investigate any such complaints and determine if they are founded. If the complaints are founded, they forward them to the Group Data Protection Officer.

The data protection representative is also bound to submit reports on important questions linked to data protection to the Group Data Protection Officer and to ensure the rules are complied with at local level.

ANNEX 5
SECURITY AND CONFIDENTIALITY POLICY

LEGRAND GROUP

The LEGRAND Group has taken security and confidentiality measures in order to ensure that data will not be damaged or that unauthorised third parties gain access thereto.

White Pages: user interface = Calendra (https)

Data base = Adam (Idaps)

ACTIVE DIRECTORY: Windows directory

For ACTIVE DIRECTORY and WHITE PAGES:

Access via internal network requiring a Windows account

Read-only access for the whole set of files. Write access for the personal record (assistant also has this access).

The HR Department has a profile to delete or modify records.

For LOTUS NOTES

Lotus Notes IBM base on secure server. Local replications encrypted by proprietary protocol. Authenticated individual access to the system.

For Office 365

Office 365 servers for Legrand are hosted in the European Union.

The O365 system is certified ISO27001 and SSAE16 SOC1 type II,

For the IT DEPARTMENT CALL DUTIES system

Access limited to read-only for employees and providers with access to Group information systems. Write access is limited to the managers concerned.

These 4 systems (WHITE PAGES and ACTIVE DIRECTORY, LOTUS NOTES, 0365, IT DEPARTMENT CALL DUTIES) are accessible only from the Legrand network (specifically by firewall).

For the TOHM system (ex TALENTIS)

User interface = https. Access via individual login and password.

Tohm is an application from Technomedia (ISO 27001). The data are hosted in France.

All laptops, desktops and servers are protected by an anti-malware system.

ANNEX 6
AUDIT PROCEDURE

LEGRAND GROUP

The LEGRAND Group will carry out audits regularly once a year within the Group and within one or more subsidiaries.

The Group Data Protection Officer decides on the audit schedule within the LEGRAND Group.

The Group Data Protection Officer is therefore able to expressly request that an audit be conducted.

The audit may be carried out by LEGRAND Group internal auditors.

The purpose of these audits is to verify that subsidiaries located inside and outside the European Union comply with the binding corporate rules, in particular in terms of transparency, the right to information of the data subjects and the purpose limitation, quality and proportionality of the data.

The objective is also to verify how the subsidiaries are handling complaints from the data subjects and their requests to exercise their right of access to the data relating to them.

If necessary, an audit may also be conducted by the data protection authorities if they take the initiative to do so.

The subsidiaries are bound to cooperate and give all the elements of information necessary in order to enable the internal auditors to conduct their assignment.

At the end of the audit, an audit report is drawn up by the internal auditor who, where appropriate, may make recommendations and even request a time-driven corrective action plan to be put in place, if the results of the audit reveal serious breaches of the binding corporate rules or the regulations on data protection.

All subsidiaries are bound to implement the corrective action plans referred to in the audit report within the allotted time frame. If such were not the case, measures may be taken against them.

All the audit reports are addressed to the Group Data Protection Officer as well as to the Group Chief Information Officer. Copy of the audit report may also be sent to the data protection authorities, on request.

ANNEX 7
TRAINING PROGRAMME

LEGRAND GROUP

The LEGRAND Group provides its personnel with information tools explaining what “binding corporate rules” are and thus raising awareness of personnel to the major problems related to data protection (purpose limitation, proportionality of data, sensitivity of open comments areas, security and confidentiality of data) on the Group’s intranet.

FAQs on the recurrent queries about protecting personal data are also available on the Group’s intranet.

The LEGRAND Group has put a specific training programme in place for:

- Data protection representatives;
- Personnel of each subsidiary who have permanent or regular access to personal data;
- Personnel in charge of developing tools for processing personal data.

A specific information notice will be sent out to them by the Group Data Protection Officer which will be updated regularly. If needs be, training will be delivered by the Group Data Protection Officer on specific topics or by the Group’s external advisers.

Regularly and insofar as necessary, data protection representatives will run training for the personnel for whom they are competent locally, in order to remind them of the broad guidelines of the binding corporate rules and to raise awareness on the rules for protecting personal data.

Annex 8

legrand®	**INFORMATION SYSTEMS DEPARTMENT** **Information Systems Quality & Security** **INFORMATION SYSTEM** **ACCEPTABLE USE POLICY**

Introduction

The Legrand Group provides you with a full set of communication means and takes care to offer you high-quality services and equipment (internet access, computer networks, e-mail, etc.) at all times.

The Information Systems Department (ISD) aims to ensure information is secured against any harmful or illegal, deliberate or accidental operations contrary to the achievement of the Group's objectives and liable to endanger users of the information systems.

The ISD offers each user an efficient, reliable and accessible user area with daily data back-up.

The aim of this policy is to set out:

- the principles that contribute to protecting the Group against risks to which users expose themselves in the event of inappropriate or improper use of information systems.
- and the principles that contribute to protecting users' personal and even private information.

Article 1: Scope

The security policy put in place applies to all permanent or temporary users of Legrand Group information systems (Group hardware and data, internet, computer systems belonging to third parties, etc.). It also applies to all associates, providers, consultants and temporary staff and to all information systems owned, leased or operated by the Group.

Article 2: Access

A user's right of access to any computer system is subject to authorisation. This right of access, confirmed by the creation of an individual account, is personal, non-transferable and limited to activities necessary in order to do their job. Each user is therefore responsible for operations performed via their own account and must only use the account opened for them by the authorised administrator or for which they have received explicit delegation.

These provisions are without prejudice to a duty of loyalty, which may require the disclosure of their login details in order to ensure the continuity of the company's business (e.g.: user off work).

Article 3: Copyright

All the Legrand Group's information systems are Legrand Group property (physical hardware, network hardware, intranet and extranet networks, operating systems, software, storage media, access accounts as well as all the messages and data produced or processed on these information systems). They must be only used for the purpose of serving the interests of the Company, of its customers and of its users.

Before any software is installed, it is essential to firstly ensure that this is allowed under the licensing rights. Copying of software for personal reasons is strictly prohibited.

For all users, Legrand Group must give prior and specific approval for:

- Any connection to the computer hardware and software network.
- Any copying of software, databases or system configuration.
- Any system enabling access to Legrand Group data via an external network.
- Any data security practice involving access, acquisition, processing and storage of protected and confidential information.

Article 4: Use and protection

The Legrand Group's information systems are working tools. They must only be used for professional reasons. Nevertheless, personal use may be tolerated provided that it is outside working hours, within reason* and complies with legislation.

Access to the Legrand Group network supposes that users strictly comply with the rules of this information system acceptable use policy.

The ISD is concerned about personal privacy but it reserves the right to analyse users' traces in order to ensure compliance with this policy and confidentiality rules to which the information present on the network is subject. In particular, the ISD reserves the right to carry out routine audits on networks and information systems without prior notice.

* both in terms of time spent and use of computer resources.

Article 5: Confidentiality

Files produced by all users are considered as professional unless they are clearly labelled as private by their author. A file may only be modified with permission from its formal or implicit owner; this modification is clearly labelled. This rule also applies to e-mail exchanges. The case of multi-user workstations must be taken into account by each user in the event of such use.

Users must show discretion regarding any information on the internal working of the company that they have obtained using the computer systems.

System administrators may examine the content of files or inboxes if necessary in order to ensure the smooth running of the computer systems and to ensure proper compliance with the acceptable use policy. Administrators are however required to maintain the confidentiality of both private and professional data, of which they become aware under these circumstances.

Article 6: Data protection

Any personal information must be processed and transferred in accordance with current legislation. In the event that a user initiates or requests the modification of processing in accordance with the local regulations on the protection of personal data, they must firstly contact the competent local services. Personal information is information that enables the identification, in any form whatsoever, of a natural person (e.g.: their e-mail address).

Any person registered in a file must be informed of the nature of the data and the use made of it; they must be able to access all the data concerning them and have a right to modify incorrect data.

Case of the European Union, particularly France:

A Data Protection Officer has been appointed for Legrand Group France in order to establish how to comply with the law.

The Group has put in place an internal code of conduct to regulate all transfers of personal data made within the Group outside the European Union, thereby ensuring a high level of protection for personal data, regardless of the Group entity to which the personal data is transferred. This internal code of conduct, which defines Group policy on transferring personal data outside the European Union, is known as the “Binding Corporate Rules” (or “BCR”).

The Legrand Group and all employees are required to comply with these binding corporate rules (see annex).

Procedures have been put in place inside the Group to ensure that the BCR are complied with:

- A procedure for training personnel on the rules laid down in the BCR;
- An audit procedure;
- An internal complaints handling procedure;
- A network of data protection representatives to ensure the internal rules are observed.

The BCR also specify the principles to be abided by in the event of transferring personal data within the Group outside the European Union:

- Purpose limitation;
- Quality and proportionality of the personal data processed;
- Processing of personal data founded on a legal basis;
- Information provided to the data subjects concerned by the processing and easy access by them to the BCR;
- Rights of access, correction, erasure and blocking of the data subject’s data which is the subject of the processing;
- Rights in the event of automated individual decisions;
- Security and confidentiality;
- Restrictions in the event of subsequent transfers outside the Group;
- All member entities of the Group must inform the appointed Group data protection officer if there is any local legislation that might prevent this entity from complying with the BCR;
- The setting up of an internal complaints management mechanism for handling complaints from data subjects;
- Duty of the Group to co-operate with the competent personal data protection authorities.

Article 7: Code of conduct

Security is everybody's business. Each user contributes to it by using the computer systems with which they are provided in a responsible manner. Everyone must observe and abide by a certain number of common-sense recommendations and rules that ensure the continued smooth running of the information systems.

The lists below are not exhaustive, they are intended to set out guidelines for the use of computer services and user behaviour.

The user agrees:

In terms of use:

- not to harm the company's brand image when using the computer systems,
- to use all shared resources (computing power, disk space, etc.) in a reasonable manner and not unnecessarily overload the network by, for instance, streaming audio and video for personal reasons.

In terms of confidentiality:

- to only use their individual user account and accordingly remain identifiable at all times,
- to guarantee the confidentiality and integrity of data belonging to other users of the network,
- to only use and provide their Legrand e-mail for strictly professional reasons,
- not to leave any documents displayed on the monitor,
- not to leave their work space without logging out or placing their computer in sleep mode.

In terms of security:

- to regularly save their files,
- not to interrupt or endanger the smooth running of the network or systems connected to the network (unusual operations, introduction of viruses, etc.),
- to only use connection processes supplied by the Group's IT departments,
- to ensure that the development of tools does not deliberately endanger the integrity of the computer systems,
- to protect their own files, with help from IT specialists where applicable (the user being responsible for the rights they grant to third parties),
- to secure their passwords based on the recommendations of IT specialists (i.e. to keep them secret, not towrite them down on paper, not to disclose them to third parties and to change them regularly),
- to ensure insofar as possible restricted access to premises containing computer systems.

The following are considered as unacceptable use of computer systems:

- any connection to external sites featuring obscene or illegal content,
- any use of network and system analysis or surveillance tools,
- any installation or upgrading of systems (hardware or software) that is not approved by the ISD on the Legrand Group network,
- any connection of computer hardware not belonging to the Group without explicit permission from ISD,
- any deliberate introduction or introduction due to negligence of malicious programmes onto the information systems (viruses, worms, etc.).

Employee commitment

To conclude this document, each Group employee must comply with the principles specified above and agree to the following terms:

i) I have received and read a copy of this policy and I agree to abide by and comply with the information system acceptable use policy. I understand that failure to comply with this policy may result in disciplinary action and even be recognised as professional misconduct.

ii) I understand that any software and hardware provided to me by Legrand Group remain the property of the company (also including data stored on said equipment except for data clearly labelled as "private" or "personal" (see article 5).

iii) I agree not to modify or upgrade any programmes or computers provided by the Group without approval from the ISD.

iv) I agree not to duplicate any software, except for backup purposes as part of my job.

v) I agree that if I leave the company for any reason, I must immediately return to the Legrand Group the originals and copies of software, as well as any computer hardware, having removed then deleted from them the data clearly labelled as "private" or "personal" (see article 5).

vi) I agree I must pay special attention to protecting all software and hardware provided by the Legrand Group from theft and against any software and hardware damage.

vii) I understand that all email sent and received on the Legrand Group email system is the property of the Group and may be audited at any time, except for e-mails clearly labelled as private (see article 5).

viii) I have had an opportunity to ask questions about this policy and I am aware that additional information may be provided. (On Dialeg / ISD intranet).