Data Protection Policy

Issued 24/05/2018

Document number HR1.1

CAUTION: The master of this document is held electronically: “xxx”

Therefore any printed version is ***NOT COPY CONTROLLED*** and will not be automatically updated.
Printed copies and uncontrolled electronic copies of this document may not be at the latest revision.

Table of Contents

1. Introduction **4**

2. Why this policy exists **4**

3. Definitions **5**

4. Scope **7**

4.1 Rights of data subjects *8*

5. Data protection risk **8**

6. Our procedures **8**

6.1 Data inventory and data flow *8*

6.2 Fair and lawful processing *8*

6.3 Responsibility: *9*

6.4 Sensitive personal data *10*

6.5 Accuracy and relevance *10*

6.6 Your personal data *10*

6.7 Data security *11*

6.8 Data retention *11*

6.9 Transferring data internationally *11*

6.10 Compliance with Rights of Data Subjects *11*

6.11 Training *15*

6.12 CCTV and Voice recordings *15*

6.13 Sub-contractors *15*

6.14 Breach notification under GDPR *16*

7. GDPR provisions **16**

8. Appendix A Notification requirements **19**

9. Appendix B Sample Web Privacy Notice **20**

Data Protection Policy

1. Introduction

Raritan Inc. and its subsidiaries process personal data about employees, clients, suppliers and another natural person ('data subject') for a variety of business purposes.

This policy sets out Raritan Inc. commitments and rules governing the processing and protection of personal data.

The objective of this policy is to provide to all persons involved in personal data processing with a framework for understanding and acting; it also sets out how data subjects can exercise their rights.

This policy is based on the obligations of the European regulation 2016/679 on the protection and freedoms of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR) and other applicable national provisions. Raritan Inc. will ensure personal information is processed lawfully, fairly and in a transparent manner in relation to the data subject.

Legrand including Raritan has appointed a Data Protection Officer (DPO) supported by local Data Protection Representatives (DPR) in key regions. The DPO will inform and advise Raritan and its employees about their obligations to comply with the GDPR and other data protection laws.

The DPO has overall responsibility to monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conducts internal audits.

The regional DPR and the DPO are the first point of contact for supervisory authorities and for individuals whose data is processed.

IDENTITY OF THE DATA CONTROLLER

The processing of personal data collected is carried out under the responsibility of Raritan Inc. and its subsidiaries as defined in this policy.

2. Why this policy exists

This data protection policy states Raritan Inc. commitment to compliance with data protection requirements and good practice, including:

1. processing personal information only where this is strictly necessary for legal and regulatory purposes, or for legitimate organizational purposes
2. maintaining an inventory of all processing activities and data flows. Clearly documenting the purpose and legal basis for said processing of personal information.
3. processing only the minimum personal information required for these purposes
4. providing clear information to natural persons about how their personal information can be used and by whom. Including details of data storage and processing.
5. only processing relevant and adequate personal information
6. processing personal information fairly and lawfully
7. Protecting the rights of employees, clients, suppliers and another natural person ('data subject')
8. Protecting both Raritan and the data subjects from the risk of data breach

This policy will be communicated throughout Raritan and Legrand and will be available to interested parties, as appropriate.

3. Definitions

Legrand	Legrand Group (parent company)
Raritan Inc.	Raritan Inc.; Raritan Europe BV; Raritan Computer UK ltd.; Raritan Deutschland GmbH; and its subsidiaries
Lawful processing	Lawful bases available for processing personal data and special categories of data include the following: 1. *Consent of the data subject* 2. *Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract* 3. *Processing is necessary for compliance with a legal obligation* 4. *Processing is necessary to protect the vital interests of a data subject or another person* 5. *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* 6. *Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject* *[For special categories of data]* 7. *Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law* 8. *Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement* 9. *Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent* 10. *Processing relates to personal data manifestly made public by the data subject* 11. *Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity* 12. *Processing is necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards* 13. *Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional* 14. *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 healthcare and of medicinal products or medical devices* 15. *Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)*
Business purposes	The purposes for which personal data may be used by us: Personnel, administrative, financial, regulatory, payroll and business

	development purposes. *Business purposes include the following:* 16. *Compliance with our legal, regulatory and corporate governance obligations and good practice* 17. *Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests* 18. *Ensuring business policies are adhered to (such as policies covering email and internet use)* 19. *Operational reasons, such as recording transactions, financial Controls, training and quality control, ensuring the confidentiality of commercially sensitive information, suppliers account management: contracts, orders, receipts, invoices, settlements, accounting, security vetting, credit scoring and checking* 20. *Management of safety, working conditions including legal documents, management, declaration and prevention of accidents and occupational diseases, management of occupational health activities, management of employees with disabilities* 21. *Travel administration and expense management, Management of company cars, including management and declaration of material accidents and incidents, Geolocation of professional vehicle* 22. *Management and monitoring of IT Infrastructure security, including identifications and authorizations for infrastructure applications and equipment. Control of Internet use, control of the use of messaging, logging of internet access, VoIP and email traffic.* 23. *Clients account management: contracts, orders, deliveries, Billing, settlements, accounting, financial information, legal documentation (auditors, tax authorities), trade statistics, portfolio tracking, dashboards, reporting, business statistics tool* 24. *Product development, administration and project management* 25. *The delivery of managed services on the behalf of other organization.* 26. *Investigating complaints* 27. *Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments* 28. *Usual staff administration, including recruitment files, monitoring staff conduct, disciplinary matters* 29. *Marketing our business* 30. *Improving services* 31. *Customer technical support* 32. *Security and protection of physical facilities and assets.*
Personal data	"Personal Data" means 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; Examples include information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, clients, suppliers and marketing contacts. Pseudonymised personal data (e.g. key-coded) – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

	Personal data Raritan gathers may include: • *Civil status, identity, identification data, images* • *Professional life (CV, schooling, vocational training, distinction ...)* • *Personal life (lifestyle, family situation, etc.)* • *Pay details* • *Educational (details of certificates and diplomas, education and skills)* • *Economic and financial information (income, financial situation, tax situation, etc.)* • *Connection data (IP address, logs, etc.)* • *Location data (travel, GPS data, GSM, etc.)* • *CCTV and Voice recordings* • *Data revealing racial or ethnic origin* • *Data revealing political opinions* • *Data revealing religious or philosophical beliefs* • *Data showing trade union membership* • *Genetic data* • *Biometric data for the purpose of uniquely identifying a natural person* • *Health data* • *Well-being data including daily habit monitoring* • *Data on sex life or sexual orientation* • *Data relating to criminal convictions or offences* • *National insurance number / Social security number* • *Passport details / National ID card* • *Driver's license details*
Sensitive personal data	*Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings—any use of sensitive personal data should be strictly controlled in accordance with this policy and the regulation*
Binding Corporate Rules	*Binding Corporate Rules (BCRs) are internal rules (such as a Code of Conduct) adopted by The Legrand group of companies which define its global policy with regard to the international transfers of personal data within the same corporate group to entities located in countries which do not provide an adequate level of protection.*

4. Scope

This policy applies to all staff and 3rd parties involved in personal data processing for Raritan. Each actor must be familiar with this policy and comply with its terms.

This policy supplements our other policies relating to internet and email use. Raritan may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff and partners when adopted.

Raritan's Data Protection Officer, Julie Celma has overall responsibility for compliance with the GDPR and other data protection laws, including managing internal data protection activities, advice on data protection impact assessments; train staff and conduct internal audits.

4.1 Rights of data subjects

This policy will ensure that Raritan maintains the rights and freedoms of individuals as set out in European regulation 2016/679 on the protection of the rights and freedoms of natural persons. Said rights are described below:

1. The right to be informed:
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

.

5. Data protection risk

This policy helps to protect the rights and freedoms of data subjects and protect Raritan from data security risks including:

- **Personal data breach**. A breach of security leading to the accidental or unlawful destruction, loss alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
- **Failing to offer choice**. All individuals should be free to choose how the company uses data relating to them.
- **Reputational damage**. For example, the company could suffer if a data breach due to hacking took place.

6. Our procedures

6.1 Data inventory and data flow

Raritan will document and maintain a data inventory and data flow analysis for each activity that involves the processing of personal information. This will include the following:

1. Key business process that utilize personal information
2. Sources of personal information
3. Categories of personal information processed, including the identification of high-risk (sensitive) personal information.
4. The lawful basis for the processing

6.2 Fair and lawful processing

Raritan must process personal data fairly and adhere to "Lawful processing" in accordance with individuals' rights under GDPR.

Raritan will ensure that personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to individuals;
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the

public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

3. adequate, relevant and limited to what is necessary for relation to the purposes for which they are processed;
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
6. 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 procedural measures.

6.3 Responsibility:

Each actor that handles personal data must ensure it is handled and processed in line with this policy and data protection law. The board of directors is ultimately responsible for ensuring that Raritan meets its legal obligations

6.3.1 The Group Data Protection Officer's responsibilities:

a) to inform and advise Raritan and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;

(b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;

(d) to cooperate with the supervisory authority;

(e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

Raritan's DPR (Data Protection Representative), Rali Vellacott will assist Raritan's DPO in the above tasks as well as being the first point of contact.

6.3.2 Responsibilities of the IT Manager

- Ensure all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly

6.3.3 Responsibilities of the Marketing Manager

- Approving data protection statements attached to emails and other marketing copy
- Addressing data protection queries from clients, target audiences or media outlets
- Coordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy

6.3.4 The processing of all data must be:

- Necessary to deliver our services
- In our legitimate interests and not unduly prejudice the individual's privacy
- In most cases, this provision will apply to routine business data processing activities.

Our Terms of Business contains a Privacy Notice to clients on data protection.

The notice:

- Sets out the purposes for which we hold personal data on customers and employees
- Highlights that our work may require us to give information to third parties such as expert witnesses and other professional advisers
- Provides that individuals have rights described in 4. 1 of the policy.

(please see a sample Privacy Notice in Appendix B)

6.4 Sensitive personal data

As with all personal data Raritan will only process sensitive personal data where a lawful basis has been identified and documented. Where processing of sensitive personal data is necessary, Raritan will obtain the data subject's explicit consent and such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

6.5 Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose.

Data subjects may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the DPR & the DPO.

6.6 Your personal data

You must take reasonable steps to ensure that personal data we hold about you is accurate and updated as required. For example, if your personal circumstances change, please inform the HR representative so that they can update your records.

6.7 Data security

You must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

6.7.1 Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it.
- Printed data must be shredded when it is no longer needed
- All portable devices and media that are used to store personal data must be protected by the uses of strong encryption. Data stored on CDs or memory sticks must be encrypted and must be locked away securely when they are not being used
- Data stored on a computer must be protected by strong passwords that are changed regularly.
- Servers containing personal data must be kept in a secure location, away from general office space. Data at rest must be protected.
- Data should be regularly backed up in line with the company's backup procedures
- Data should never be saved directly to unencrypted mobile devices such as laptops, tablets or smartphones
- All servers containing sensitive data must be approved and protected by security software and strong firewall.

6.8 Data retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

6.9 Transferring data internationally

There are restrictions on international transfers of personal data. You must not transfer personal data anywhere outside the European Economic Area (EEA) without first consulting the Data Protection Officer. Said transfers must be covered by either BCR or by contractual provision when dealing with a 3rd party organisation.

6.10 Compliance with Rights of Data Subjects

6.10.1 Right to be informed

Raritan will provide concise, transparent, intelligible and easily accessible privacy notices at the point of data collection. The information supplied is determined by whether or not Raritan obtained the personal data directly from individuals. See the table below for further information on this.

Information that must be supplied?	**Data obtained directly from data subject**	**Data not obtained directly from data subject**
Identity and contact details of the controller (and where applicable, the controller's representative) and	✓	✓

the data protection officer		
Purpose of the processing and the lawful basis for the processing	✓	✓
The legitimate interests of the controller or third party, where applicable	✓	✓
Categories of personal data		✓
Any recipient or categories of recipients of the personal data	✓	✓
Details of transfers to third country and safeguards	✓	✓
Retention period or criteria used to determine the retention period	✓	✓
The existence of each of data subject's rights	✓	✓
The right to withdraw consent at any time, where relevant	✓	✓
The right to lodge a complaint with a supervisory authority	✓	✓
The source the personal data originates from and whether it came from publicly accessible sources		✓
Whether the provision of personal data part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data	✓	
The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences.	✓	✓

Where information has been indirectly received Raritan will within a reasonable period of having obtained the data (within one month) inform the data subject. If the data are used to communicate with the individual, at the latest, when the first communication takes place; or If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.

6.10.2 Right of access

Please note that under the GDPR, individuals are entitled, subject to certain exceptions, the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information – this largely corresponds to the information that should be provided in a privacy notice

If you receive a subject access request, you should refer that request immediately to the DPO or local DPO. We may ask you to help us comply with those requests.

When dealing with such request the Information must be provided without delay and at the latest within one month of receipt. You must verify the identity of the person making the request, using "reasonable means".

6.10.3 Right to rectification

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. Where the personal data in question has been disclosed to third parties, you must inform them of the rectification where possible. You must also inform the individuals about the third parties to whom the data has been disclosed where appropriate.

If you receive a rectification request, you must respond within one month. This can be extended by two months where the request for rectification is complex.

In cases where Raritan are not taking action in response to a request for rectification, the local DPO must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy

6.10.4 Right to erasure (the right to be forgotten)

The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

If you receive an erasure request, you should refer that request immediately to the DPO or local DPO. We may ask you to help us comply with those requests.

Note the right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (i.e. otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

There are some specific circumstances where the right to erasure does not apply and the request can be refused.

You can refuse to comply with a request for erasure where the personal data is processed for the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation or for the performance of a public interest task or exercise of official authority;
- for public health purposes in the public interest;
- archiving purposes in the public interest, scientific research historical research or statistical purposes; or
- the exercise or defence of legal claims.

Where the personal data in question has been disclosed to third parties, you must inform them about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

6.10.5 Right to restrict processing

A request to restrict the processing of personal data must be acted on in the following circumstances:

- Where an individual contests the accuracy of the personal data, the processing should be restrict until the accuracy of the personal data has been verified.
- Where an individual has objected to the processing (where it was necessary for the

performance of a public interest task or purpose of legitimate interests), and you are considering whether your organisation's legitimate grounds override those of the individual.
- When processing is unlawful and the individual opposes erasure and requests restriction instead.
- If you no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

You may need to review procedures to ensure you are able to determine where you may be required to restrict the processing of personal data.

If you have disclosed the personal data in question to third parties, you must inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.
You must inform individuals when you decide to lift a restriction on processing.

6.10.6 Right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.

The right to data portability only applies:

- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

If a data portability request is applicable Raritan will provide the personal data in a structured, commonly used and machine-readable form such as CSV files.

The information will be provided free of charge. A response to a request will respond without undue delay, and within one month.

6.10.7 Right to object

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

Raritan will inform individuals of their right to object "at the point of first communication" and in appropriate privacy notice.

For direct marketing activities:
- processing personal data for direct marketing purposes must stop as soon as an objection is received. There are no exemptions or grounds to refuse.
- objection to processing for direct marketing will be dealt with at any time and free of charge.

.

6.10.8 Rights related to automated decision making and profiling

Individuals have the right not to be subject to a decision when:

- it is based on automated processing; and
- it produces a legal effect or a similarly significant effect on the individual.

If applicable Raritan will ensure that individuals are able to:

- obtain human intervention;
- express their point of view; and

- obtain an explanation of the decision and challenge it.

6.11 Training

All staff will receive training on this policy. New joiners will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our policy and procedure.

Training is provided through an in-house seminar on a regular basis.

It will cover:

- The law relating to data protection
- Our data protection and related policies and procedures.

Completion of training is compulsory.

6.12 CCTV and Voice recordings

Raritan will ensure that CCTV and Voice recording is:

- Only carried out for a legitimate and justifiable reason.
- Recordings from systems will to be securely stored and access restricted to authorised personnel.
- Clear and visible notification CCTV presence will be always provided.
- All systems using voice recording will provide clear notification and the option to opt out of having your call recorded.
- CCTV recordings need to be of an appropriate quality to meet the purpose intended.
- Recording and playback functions need to provide access to recordings made in specified locations and times to comply with subject access requests from individuals in recordings or in response to police requests.
- The recording will by default be held for no more than 30 days unless Privacy Impact Assessment (PIA) and risk assessment are carried out to determine a longer retention period for a particular application.

Both voice and video recording are personal data as defined by GDPR and as such all aspects of this policy are applicable,

6.13 Sub-contractors

Raritan must have a written contract with any 3rd parties that act as data processors, GDPR defines a set of required clauses that must be in said contracts.

Contracts must set out:

- the subject matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data and categories of the data subject; and
- the obligations and rights of the controller.

Contracts must also include as a minimum the following terms, requiring the processor to:

- only act on the written instructions of the controller;
- ensure that people processing the data are subject to a duty of confidence;
- take appropriate measures to ensure the security of processing;
- only engage sub-processors with the prior consent of the controller and under a written contract;
- assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- delete or return all personal data to the controller as requested at the end of the contract;
- submit to audits and inspections by providing the controller with whatever information is needed to ensure that both parties meet their obligations under Article 28; and
- inform the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

6.14 Breach notification under GDPR

Appendix A provides a workflow for external notification process. All staff must report any suspected breach of personal data to the DPO or their local representative without delay.

7. GDPR provisions

Where not specified previously in this policy, the following provisions will be in effect on or before 25 May 2018.

Privacy Notice - transparency of data protection

Being transparent and providing accessible information to individuals about how we will use their personal data is important for our organisation. The following are details on how we collect data and what we will do with it:

What information is being collected?	
Who is collecting it?	
How is it collected?	
Why is it being collected?	
How will it be used?	
Who will it be shared with?	
Identity and contact details of any data controllers	
Details of transfers to third country and safeguards	
Retention period	

Conditions for processing

We will ensure any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented. All staff who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy notice.

Justification for personal data

We will process personal data in compliance with all six data protection principles.

We will document the additional justification for the processing of sensitive data, and will ensure any biometric and genetic data is considered sensitive.

Consent

The data that we collect is subject to active consent by the data subject. This consent can be revoked at any time.

Criminal record checks

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.

Data portability

Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done for free.

Right to be forgotten

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

Privacy by design and default

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The DPO will be responsible for conducting Privacy Impact Assessments and ensuring that all IT projects commence with a privacy plan.

When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

International data transfers

- No data may be transferred outside of the EEA without first discussing it with the data protection officer. Specific consent from the data subject must be obtained prior to transferring their data outside the EEA.

Data audit and records

- Regular data audits to manage and mitigate risks will be an ongoing requirement to ensure compliance. The data audits will be documented in record system, which contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

Reporting breaches

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

Investigate the failure and take remedial steps if necessary

Maintain a register of compliance failures

Notify the Information Commissioners Office of any compliance failures that are material either in their own right or as part of a pattern of failures

Please refer to our Compliance Failure Policy for our reporting procedure.

Monitoring

Everyone must observe this policy. The local DPR has overall responsibility for this policy. They will monitor it regularly to make sure it is being adhered to.

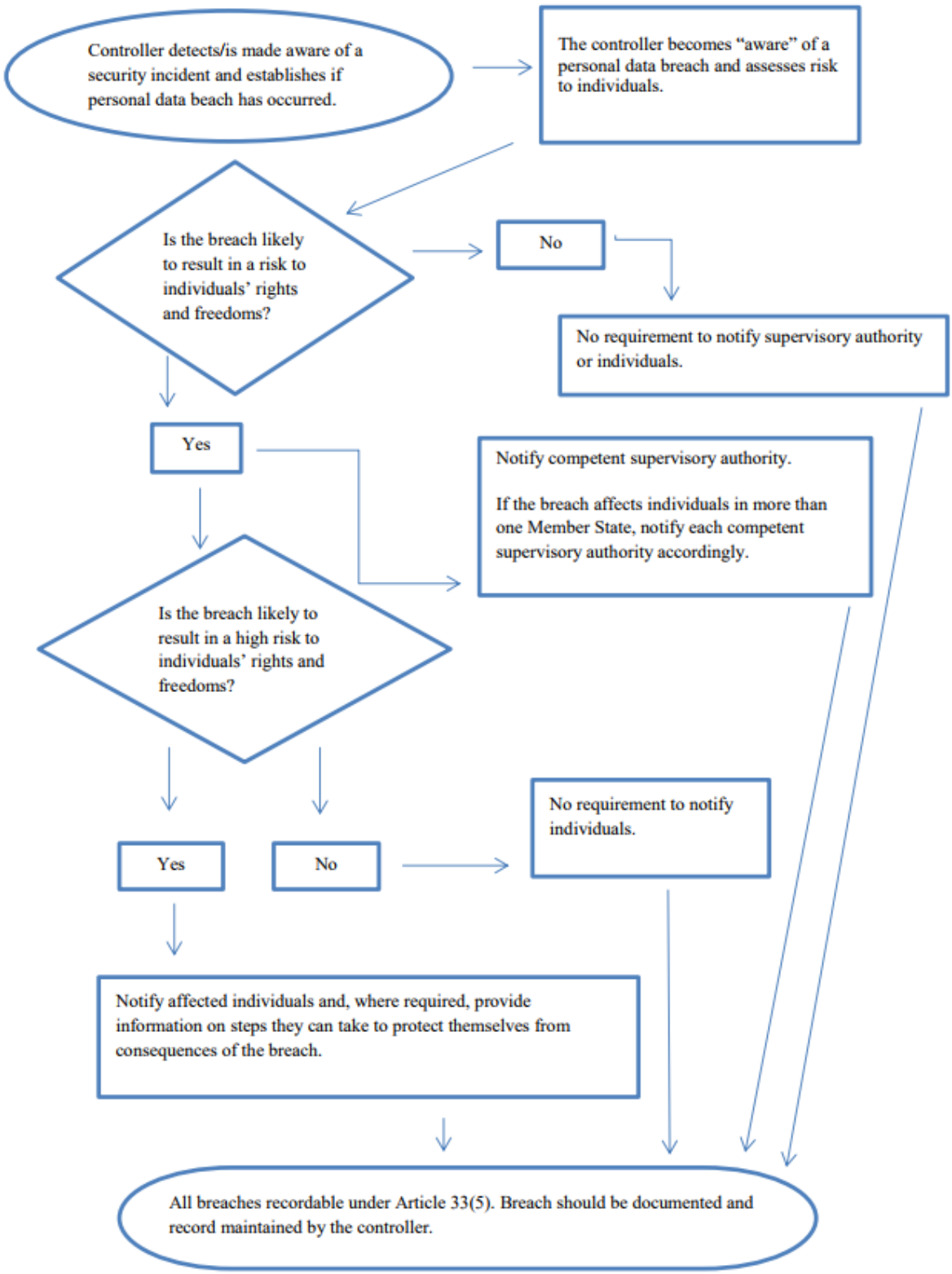
Consequences of failing to comply

We take compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPO.

8. Appendix A Notification requirements



9. Appendix B Sample Web Privacy Notice

USE OF PERSONAL DATA

Support and storage of data processing
Identity of the data controller
Nature of data collected and Purpose of the data processing
Exercise of user's rights
Conditions of the data processing
Transmission of data to third parties
Data security
Data retention
Cookies
Under 16
Modification of the Privacy Policy

Latest update: [24th of May 2018]

SUPPORT AND STORAGE OF DATA PROCESSING

This website Raritan.com is hosted via Media Temple

IDENTITY OF THE DATA CONTROLLER

The processing of personal data collected is carried out under the responsibility of Raritan Europe B.V.

Name and contact details of the controller:

For Europe:
Raritan Europe B.V.
Jan van Galenstraat 59
3115 JG Schiedam
The Netherlands

Legal information on the controller
No. Chamber of Commerce: 24256806
VAT identification number NL 803738614B01

For America:
Legrand France
128, av. du Maréchal de Lattre de Tassigny
87045 Limoges Cedex (France)
e-mail: webmaster.legrand@legrand.fr

Legal information on the controller
Limited company with capital of 54,912,550 €
No. SIRET 758 501 001 00013
APE code 2733Z
RCS Limoges 758 501 001
VAT identification number FR 94 758 501 001

NATURE OF DATA COLLECTED AND PURPOSE OF THE PROCESSING

Raritan respects the privacy of individuals, (candidate) employees and our customers. We adhere to the following principles when it comes to your personal data.

1. Processing your personal information fairly and lawfully.
2. Collecting your personal information for specified, legitimate purposes and not processing further in ways incompatible with those purposes.
3. Collecting your personal information which is relevant to and not excessive for the purposes for which it is collected and used. We may render information anonymously when feasible and

appropriate, depending on the nature of the data and the risks associated with the intended uses.
4. Maintaining your personal information accurate, and where necessary, keeping it up-to-date. We will take reasonable steps to rectify or delete Data that is inaccurate or incomplete.
5. Keeping your personal information only as long as it is necessary for the purposes for which it was collected and processed.
6. Processing your personal information in accordance with the individual's legal rights.
7. Taking appropriate technical, physical, and organizational measures to prevent unauthorized access, unlawful processing, and unauthorized or accidental loss, destruction, or damage to personal information.
8. Processing your personal information based on the following legal basis:
    - You have unambiguously given your consent; or
    - The processing is necessary for the performance of a contract to which you are party or to take steps at your request prior to entering into a contract; or
    - The processing is necessary for compliance with a legal obligation to which Raritan is subject; or
    - The processing is necessary to protect the vital interests of the data subject; or
    - The 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 is disclosed; or
    - The processing is necessary for the purposes of the legitimate interests pursued by Raritan or by the third party or parties to whom the data is disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.

Legrand and all its entities adhere to these principles.

Raritan collects personal information from all users (ie. customers, applicants, leads, etc.) for service and a personalised experience while using the various websites and pages. Raritan may collect personal information to complete various transactions, such as:

- customer/user profile creation
- marketing or product support subscriptions
- processing requests regarding quotes/resellers and other informational requests
- promotional activities (such as contests) or survey participation
- product or [professional] service orders, product activations and/or registrations
- job applications

WHICH INFORMATION WE COLLECT
When you register, and at other times, Raritan will collect personally identifiable information from you that may include your name, company name, age, address, country, zip code, e-mail address, and facts about your company's IT infrastructure as well as industry information this includes:

- customer type, job function, job title
- product and service preferences, contact preferences and job interest data
- your Raritan partner portal username and password (where applicable)
- IP address (see cookies)

USE OF DATA COLLECTED
If you provide personal information to us, either directly or through a reseller or other business partner, we will:

1. not sell or rent it to a third party without your permission. We may however use your contact information to provide you with information we believe you need to know or may find useful, such as (for example) important updates/news about our products or modifications to the Terms of Service
2. take commercially reasonable precautions to protect the information from loss, misuse and unauthorized access, disclosure, alteration and destruction
3. not use or disclose the information except:
    - as necessary to provide services or products you have ordered, such as (for example) by providing it to a transporter/carrier to deliver products you have ordered
    - in other ways described in this privacy policy or to which you have otherwise consented

- in the aggregate with other information in such a way so that your identity cannot reasonably be determined (for example, statistical compilations)
- as required by law, for example, in response to a subpoena or search warrant
- to outside auditors who have agreed to keep the information confidential
- as necessary to enforce the Terms of Service
- as necessary to protect the rights, safety, or property of Legrand its users, or others; this may include (for example) exchanging information with other organizations for fraud protection and/or risk reduction.

Your consent to processing
Your consent is important to us and as such we will take great care to always ask for your permission before processing your data. By providing us with your personal information and using the sites, you may consent to our processing your personal data and sensitive personal data for the above purposes. When providing us with your consent you will consent to our transferring your information to countries or jurisdictions which do not provide the same level of data protection as the EU. If we do make such a transfer, we will, where appropriate, put a contract in place to ensure that your information is protected. Please refer to the Data Security section.

Appointed to give consent on behalf of another user
If you provide us with information about any other person than yourself you confirm that they have appointed/instructed you to act on their behalf. The instructor has given consent to the processing of their personal data which could include personal data. The appointed person in this case will have also informed the instructor of our identity and the purposes (as set out above) for which their personal data will be processed.

We collect personal information in various ways, below you will find an overview per department.

MARKETING
Legrand including Raritan will always carefully selected third parties whom may use the information we collect to inform you (this includes by letter, fax, phone, SMS and email) about promotions, news and new products that we think may be of interest to you. By providing us with your information you consent to being contacted by these methods and for these purposes. If you do not wish to receive marketing information from us please indicate this where requested on the various webforms.

Raritan website (Searching/Browsing)
We collect certain personal Information when you visit the sites or click on the various links to learn more about our products. We collect this information to improve web user experience (ie. country selection), gather broad geographic/demographic data, activity on the various website pages and evaluate our advertising. (please refer to the cookie section)

Newsletters and promotional e-mails
We collect Personal Information when you give us consent to receive newsletters, promotional e-mails, and other information (ie. firmware updates). We solely use this information to provide you the information you request and will only retain the information for as long as you have given permission.

<u>Promotional activities:</u> We collect Personal Information from you when you enter a promotional program or activity. We use this information to administer the program or activity, to send you promotional e-mails, notify winners, and make the winners' list publicly available pursuant to applicable regulations and laws. We may also collect Personal Information from customers who volunteer to complete surveys or participate in any online polls. Information from online surveys and polls would be used to improve our products and/or services.

<u>Contact information:</u> If you contact us regarding reseller information, quotes, etc. we will keep a record of your correspondence this will include any Personal Information you will have provided us with. Unless you indicate to us that you do not wish your information stored we will use your provided information to help us provide you better service should you contact us in the future.

SALES
Orders: We collect Personal Information when you purchase products and services. We collect this information to deliver your order, to obtain payment, and to communicate with you about the status of your order.

PARTNERS

Raritan shares data necessary to facilitate purchase of our products via partners, i.e.. name, company name, email, phone and the request that was made to Raritan such as product information and project information.

AFTER SALES
Tech support: We may collect certain information when you open a ticket with our tech support department when you request technical support for Raritan products. This information is necessary to identify your systems, understand the configuration of the products, diagnose your questions, and provide solutions.

We may keep your information for a reasonable period for the purposes set out above.

DATA RETENTION
Raritan keeps personal data for as long as necessary to provide the services, support your product and fulfill the transactions you have requested, or for other essential purposes such as complying with our legal obligations.

DATA SECURITY
LEGRAND has implemented adequate physical, electronic and administrative protection measures which comply with regulations in order to protect your personal data. Though, LEGRAND wishes to draw the users' attention to potential risks in terms of data confidentiality linked to the Internet use. It is the responsibility of the users to set up or ensure the use of a personal secured computer network, as well as to ensure a correct technical configuration of the connection box connected to your Internet Service Provider and of others devices such as radio access equipment (WIFI, 4G…).

EXERCISE OF USER'S RIGHTS
You have a right of access, modification, rectification and deletion of personal information collected concerning you. You also have the right to obtain the restriction of processing. You have the right to object to processing of personal data concerning you. In this case, it will no longer be possible to access to the Application, since the way the Application operates requires the processing of your data. At your request, we can send you the personal data you give us in a structured, commonly used and machine-readable format. To exercise your right, please send your request:

By Post
Raritan Europe,
Jan van Galenstraat 59
3115 JG Schiedam
The Netherlands

LEGRAND, Service Consommateurs or Service Relations Pro,
128 avenue du Maréchal De Lattre de Tassigny,
87045 LIMOGES CEDEX,
France

By email:
webmaster.europe@raritan.com

Your request will be processed within one month of receipt. If necessary, this period can be extended by two months, in view of the complexity and the number of requests. In this case, you will be informed of this extension and its reasons within one month of receipt of the request.

No payment will be required for the exercise of your rights except in case of manifestly unfounded or excessive demand. In this case, the Legrand Group further reserves the right to not respond to your request.

If you are not satisfied with the manner in which your request was processed, we invite you contact us. In the event you remain dissatisfied with our response, we remind you that you have the right to lodge a complaint with the French data protection authority, Commission Informatique et Libertés (CNIL): https://www.cnil.fr/ or your local supervisory authority.

CONDITIONS OF THE DATA PROCESSING
The data processing take place with manual and IT instruments with the sole purpose to achieve the indicated objectives in order to ensure the data confidentiality and security.

Third-party websites [ie. Social media]
Raritan sites or services may provide links to third-party services or websites for information. By following these links you leave the Raritan website, it should be noted that Raritan does not have any control over those third party websites nor over their privacy policies which may differ from the Legrand group.

The personal information you choose to provide to or that is collected by these third parties is not covered by the Legrand Privacy Policy. Legrand encourages all of her users to review the privacy policy of any site they may interact with before consenting to processing and collection of personal information. Legrand may provide social media links that allow you to share news and/or information with your [social] networks. Your use of these links may result in the collection or sharing of information about you, depending on the feature. We encourage you to review the privacy policies and settings on the social media sites with which you interact to make sure you understand the information that may be collected, used, and shared by those sites. Legrand and Raritan are not in any way responsible for the personal information you choose to share or submit in these networks / forums.

COOKIES
When accessing our application, cookies are stored on your device (computer, cellphone, tablet computer), subject to the choice you have made and that you can change at any time by managing your settings (see "Accept or reject cookies").

Placed on your terminal when you visit a website, a cookie is a small text file containing information about your browsing (pages views, date and time of the consultation…), whose main purpose is to enhance your visit and allow you to receive targeted services.

Type of cookies
Using cookies enables us to provide you with certain features and provides us with information regarding website visits. We measure the number of page views, the number of visits, the different actions performed by visitors on our site, the geolocation of our visitors and the number of times visitors return to our site. For this purpose, we use Google Analytics as well as the Marketo Munchkin Cookie.

Google Analytics
This website uses as well Google Analytics, a web analytics service provided by Google, Inc. ("Google"). Google Analytics uses "cookies", which are text files placed on your computer, to help the website analyse how users use the site. The information generated by the cookie about your use of the website will be transmitted to and stored by Google on servers in the United States. In case IP-anonymisation is activated on this website, your IP address will be truncated within the area of Member States of the European Union or other parties to the Agreement on the European Economic Area. Only in exceptional cases the whole IP address will be first transferred to a Google server in the USA and truncated there. IP-anonymisation is active on this website.

Google will use this information on behalf of the operator of this website for the purpose of evaluating your use of the website, compiling reports on website activity for website operators and providing them other services relating to website activity and internet usage.

The IP-address that your Browser conveys within the scope of Google Analytics will not be associated with any other data held by Google. You may refuse the use of cookies by selecting the appropriate settings on your browser, however please note that if you do this you may not be able to use the full functionality of this website. You can also opt-out from being tracked by Google Analytics with effect for the future by downloading and installing Google Analytics Opt-out Browser Add-on for your current web browser: http://tools.google.com/dlpage/gaoptout

Marketo Munchkin Cookie
Raritan uses a third party marketing automation software company called Marketo for various marketing activities related to the Raritan and Legrand brand (ie. Emailers). We use their cookies for information on email open rates and click through rates, we also use this to track activity on the Raritan website. For more information on Marketo's privacy and cookie policy, please visit Marketo's website and read their privacy policy: http://www.marketo.com/trust/legal/privacy

How it works and what type of information the cookie logs/captures: Marketo embeds a Munchkin Javascript snippet on your sites. When visitors come to a site, a cookie is placed in the visitor's web browser (if there wasn't already one) and this sends messages to our servers about that visitor's web activity. This behaviour is very functional, very similar to other web tracking scripts such as Google

Analytics. The cookie is a 1st party cookie, and only visible to Marketo.

Information gathered by the Munchkin Cookie :
Page Visits
Link Clicks
IP Address
Referrer
cookie ID

Accept or reject cookies
You can set your browser to store cookies in your terminal or reject them, either routinely, depending on where they originate from, or to inform you each time a cookie is stored in your terminal, so you can decide whether to accept or reject them.

However, deleting all cookies used by the browser, including those used by other applications or websites, may lead to some settings or information being altered or lost, making it difficult or even impossible to browse the application.

If you want to delete any cookies that are already on your computer or to stop cookies from automatically being accepted you should refer to your browser instructions by clicking "Help" in your browser menu. More information on how to set up your cookie settings is available on this website: www.AboutCookies.org.

UNDER SIXTEEN
The minors aren't the intended audience of the Application. Access to the Application is though not reserved to the adults since the contents of the Application are not prohibited for the minors under 16.

The Application does not knowingly collect or use any personal information from children under 16. If information is collected concerning a minor, the minor's legal representative has the possibility to contact the Service Relations Pro of LEGRAND in order to rectify, modify or delete this information (cf section "Rights of the users").

END OF DOCUMENT